З усього сказаного потрібно зробити висновок про те, що тестування (пентест) на проникнення є одним з пріоритетних напрямків в інформаційній безпеці. Воно дозволяє отримати об'єктивну оцінку того, наскільки легко здійснити несанкціонований доступ до комп'ютерної системи, а також поглянути на саму систему з точки зору зловмисника, а саме – зрозуміти, яким способом можна скомпрометувати обрану систему і які шкідливі дії на неї можна зробити.

Одержано 17.04.2018

УДК 343.1+004

Єлизавета Георгіївна БЄЛЯЄВА,
курсант групи Ф4-202 ХНУВС
Науковий керівник: професор кафедри кібербезпеки
факультету № 4 ХНУВС кандидат технічних наук, доцент Носов В. В.

ПОРІВНЯЛЬНИЙ АНАЛІЗ СПОСОБІВ ІНСТАЛЯЦІЇ СПЕЦІАЛІЗОВАНОЇ ОПЕРАЦІЙНОЇ СИСТЕМИ KALILINUX

В останній час дистрибутив операційної системи (ОС) KaliLinux стає одною із основних платформ тестування безпеки комп'ютерних мереж та проведення розслідувань кіберінцидентів. Даний дистрибутив містить множину інструментів, які орієнтовані на експертів з комп'ютерної безпеки. Він представляє собою ядро та набір базових утиліт, програм і налаштувань (за замовчуванням), які потрібні для тестування безпеки, а не для забезпечення нормальної роботи звичайного користувача.

Дистрибутив KaliLinux у діяльності спеціальних підрозділів поліції використовується, в тому числі, для збору інформації при розслідуванні і попередженні злочинів. У поточному дистрибутиві передбачено понад 90 різних інструментів збору інформації, які можна розділити на інструменти, що збирають інформацію з жорстких дисків комп'ютера (DFF, Guymager, інші), з локальної мережі (acccheck, arp-scan, інші) та з глобальної мережі Інтернет (Maltego, DNSRecon, інші). Також їх можна класифікувати за іншими критеріями.

До основних методів інсталяції відносяться установка: на віртуальну машину; на USB-флеш-накопичувач або зовнішній жорсткий диск; в якості другої операційної системи; в хмару. В кожного з цих методів є свої переваги та недоліки в залежності від задач використання KaliLinux.

Перевагами інсталяції KaliLinux у віртуальну машину є те, що сама інсталяція не є надто складною; основна ОС повністю ізольована від додаткової; відрізняється вищою продуктивністю порівняно з флеш-накопичувачами, а також гарантована повна безпека. До недоліків відносяться:нездатність деяких процесорів працювати з віртуалізацією; неможливість безпосереднього використання відео-карт та мережевих карт (якщо вони не USB), як наслідок відбувається певна втрата продуктивності.

Інсталяція KaliLinux з використанням USB-флеш-накопичувача або зовнішнього диску вирізняється легкістю транспортування системи, ізольованістю від основної ОС, також тим, що може завантажуватися на будь-якому комп'ютері. Недоліком даного способу є уповільнення роботи ОС (особливо при інтенсивному навантаженні на постійний запам'ятовуючий пристрій), наприклад, при оновленні пакетів.

Для досягнення найвищої продуктивності використовується інсталяція в якості другої ОС на внутрішній жорсткий диск, але при помилкових діях можна повністю стерти дані з основної ОС(випадково видалити цілі диски).

Для використання меншої кількості ресурсів, отримання простого доступу до системи з розмежованими рівнями доступу використовують інсталяцію у хмару, але в цьому випадку можливість виконання повного спектру задач значно зменшиться.

Таким чином, вибір способу інсталяції ОС KaliLinux залежить від поточних задач. Наприклад, доцільно встановлювати KaliLinux в якості другої ОС на мобільному комп'ютері при виїзді фахівця спеціального підрозділу поліції на місце події для пошуку і фіксації цифрових слідів.

Одержано 17.04.2018

УДК 004.056.53

Єлизавета Георгіївна БЄЛЯЄВА,
курсант групи Ф4-202 ХНУВС
Науковий керівник: викладач кафедри кібербезпеки
факультету № 4 ХНУВС кандидат технічних наук Світличний В. А.

МЕТОДИ ТА ЗАСОБИ ВИЯВЛЕННЯ ЕЛЕКТРОННИХ ПРИСТРОЇВ ПЕРЕХОПЛЕННЯ АКУСТИЧНОЇ ІНФОРМАЦІЇ

З початку інформаційної ери, тоді, як діє принцип – хто володіє інформацією, той володіє світом, охочих заволодіти інформацією стає все більше. Дійсно, інформація у сучасному світі – це стратегічний ресурс, спотворення чи викривлення якого може призвести до серйозних наслідків. Виявлення електронних пристроїв перехоплення інформації є одним з важливих напрямів діяльності національної поліції України для забезпечення інформаційної безпеки державних та недержавних підприємств, установ і організацій.

В загальному випадку, мовна інформація існує у вигляді акустичних хвиль, які створюються за допомогою голосового апарату людини та складається з мовних сигналів. Енергія мовного сигналу зосереджена в діапазоні 300–4000 Гц.

Під впливом акустичних коливань в приміщення, в якому міститься джерело мовного сигналу, виникають вібраційні коливання.

Проблема захисту конфіденційної мовної інформації вирішується у комплексі з використанням різних заходів, в тому числі й з використанням технічних засобів. Для захисту акустичної (мовної) інформації використовуються пасивні і активні методи, а також заходи з використанням певних засобів.

Деякі елементи допоміжних технічних засобів системи, у тому числі трансформатори, котушки індуктивності, електромагніти вторинного електрогодинника, дзвінків телефонних апаратів і т.п., мають властивість змінювати свої параметри (місткість, індуктивність, опір) під дією акустичного поля, створюваного джерелом мовного сигналу. Зміна параметрів призводить або до появи на цих елементах електрорушійної сили, або до модуляції струмів, що протікають по цих елементах відповідно до змін відповідного акустичного поля. Окрім вказаних елементів, можуть містити безпосередньо акустоелектричні перетворювачі. До таких належать: деякі типи датчиків охоронної і пожежної сигналізації, гучномовці ретрансляційної мережі, тобто, всі пристрої, які мають «мікрофонний ефект».

Нейтралізувати витік інформації можна двома поширеними способами: перший спосіб пасивний, полягає в установці спеціальних фільтрів на всі розетки в приміщенні. Дані фільтри будуть перешкоджати поширенню сигналів понад 50 Гц., тим самим блокувати роботу пристроїв, які працюють на високих частотах і перехопленню інформативних сигналів. Інший спосіб активний, полягає в постановці шумових перешкод на кожну фазу мережі в діапазоні частот, що використовуються апаратурою перехоплення. Прилади, що дозволяють реалізувати дану перешкоду, називаються мережними генераторами шуму, вони встановлюються на кожну фазу мережі, заведену в приміщення (включно освітлювальну).

Реалізація організаційних методів – це також важлива задача і в конкретних умовах досягається за допомогою різноманітних технічних засобів. Найбільший ефект досягається, коли сили й засоби, що забезпечують досягнення цілей і рішення завдань захисту акустичної інформації, утворюють комплексну систему. Крім того, ефективність обраних заходів щодо захисту інформації в значній мірі залежить від уміння і практичних навичок відповідних фахівців, й тому велика увага повинна приділятися практичним заняттям, на яких будуть розглядатися основні питання захисту акустичної інформації.

Одержано 17.04.2018

УДК 004.056.53

Ксенія Олександрівна КРАТАСЮК,
курсант групи Ф4-202 ХНУВС
Науковий керівник: викладач кафедри кібербезпеки
факультету № 4 ХНУВС кандидат технічних наук Світличний В. А.

ОСОБЛИВОСТІ КРИПТОВАЛЮТИ

Звичні для нас гроші випускаються в обіг центральними банками різних країн. На їх вартість впливають рішення урядів, економіка країн, міжнародна торгівля. Криптографічна валюта – це принципово новий інструмент взаєморозрахунків. Для генерації монет, або майнінгу, необхідно виробляти певний математичний алгоритм обчислень. Кожна криптоодиниця являє собою послідовність блоків, а кожен з блоків – складну математичну формулу. Для створення нової монети необхідно згенерувати нову ланцюжок блоків транзакцій. Таким чином криптовалюта – це цифрова (віртуальна) валюта, одиниця якої – монета, яка захищена від підробки, тобто криптовалюта по суті – це зашифрована інформація, скопіювати яку неможливо. Криптовалюта емітується безпосередньо в мережі і ніяк не пов'язана з будь-якою валютою або з державною валютною системою.

Це суттєва відмінність від звичайних грошей, які перш, ніж з'явитися на рахунку в електронному вигляді, повинні бути спочатку внесені на рахунок у грошовому еквіваленті. Наприклад, через банк або платіжний термінал. Тобто для звичайної валюти електронний вигляд – лише одна з форм представлення.

На даний момент у світі кількість видів криптовалют вже наближається до тисячі і ринок продовжує рости. Біткоін – це перша і найвідоміша з безлічі інших віртуальних електронних валют. Термін «біткоін» запозичений з англійської мови (bitcoin) і утворився шляхом злиття двох слів: bit (мінімальна одиниця комп'ютерної пам'яті) і coin (монета). Біткоін кваліфікують як віртуальну валюту, грошовий сурогат, електронну послугу, електронну інформацію, нематеріальну цінність, приватні гроші, віртуальний товар тощо.

Біткоін функціонує без будь-якого контролюючого органу або центрального банку; обробка транзакцій і емісія здійснюються колективно учасниками мережі, дозволяє проводити будь-які операції анонімно, без ідентифікації користувача. Біткоін має відкритий вихідний код; ніхто не володіє і не контролює біткоіни, але всі можуть стати учасниками мережі. Мережа біткоін заснована на так званому «блокчейні» (ланцюжку блоків) і являє собою публічний реєстр, який зберігає дані про всі транзакції системи. Усі транзакції захищені електронними підписами користувачів – учасників мережі, які видобувають біткоін і/або проводять з ними будь-які операції.

Для розуміння функціонування криптовалют, перш за все потрібно ознайомитись з поняттям «Блокчейн» (Blockchain), Blockchain – це публічна база всіх транзакцій, які коли-небудь робились в межах певної системи. Це, так званий, ланцюжок блоків транзакцій, що побудований за певними правилами із сформованих блоків транзакцій. Вперше термін з'явився як назва розподіленої бази даних, реалізованої в саме у криптовалюті біткойн. По суті, блокчейн – це децентралізований реєстр інформації, копія якого є у всіх учасників системи, і кожна його зміна залишається в базі назавжди. Змінити щось заднім числом неможливо – для цього доведеться одночасно поміняти всі наступні записи у всіх учасників системи. Для такої операції не вистачить тих обчислювальних потужностей, які сьогодні є у людства. Учасники підключені до мережі та для переказу коштів використовують адреси, а не прізвища. Достовірність адреси перевіряється за допомогою публічних ключів шифрування. При цьому особи платника і одержувача залишаються в секреті.