Звичайно на відміну від навісних замків краще – накладний, але в цьому є свої мінуси, тому що якщо їх накладають або встановлюють в середину дверей і це призводить до того що приходиться посилювати внутрішню частину дверей, а це призводить до того, що вони стають занадто тяжкими і частіше ламаються та ремонт обходиться дорожче.

Але зауважимо, що потрібно надати більшу перевагу врізаним замкам, тому що головна особливість замку цього типу – це кріплення його всередині дверного полотна, що робить його більш естетичним зсередини і, на відміну від навісних замків, більш надійним від в злому.

Злодіям для відкривання замків потрібні відмички різних видів, які допомагають відкрити різні класів та типи замків. Звичайно 1 та 2 клас замку злодій відкриє занадто швидко, тому такі замки потрібно встановити на міжкімнатні двері, а на вхідні краще всього підійде 3 та 4 клас, який навіть самий досвідчений фахівець не зможе справитися менш ніж за 30 хвилин.

Для того щоб протидіяти в злому вашого майна, потрібно всього на всього збільшити точність виготовлення механізму секретності та встановити секретність зі складним профілем замкової шпарини, та системою автентичності ключа.

Крім відмичок існують інші способи відкривання замків, наприклад руйнація замкової щілини шляхом хімічної руйнації пружин. Щоб нейтралізувати загрози цієї проблеми необхідно застосувати:

а) захист накладок, які механічно перекривають доступ до замкової шпарини циліндрового механізму;

б) встановити циліндр, у якому сумарна довжина штифтової пари перевищує глибину камори в корпусі циліндрового механізму;

в) використання циліндрових механізмів, в яких серцевина блокується обертання стопорними елементами різного типу.

Один з методів силового деблокування відноситься ствердіння корпусу (фрезування), при якому створюються умови з нейтралізації окремих деталей, що блокують від обертання серцевини.

Також потрібно спостерігати за візуалізацією коду ключа, ще краще всього мати з собою ключ дублікат, який врятує вас від зламу чи пропажі ключа, також по можливості міняти свою серцевину замка кожних пів року.

Якщо встановити захисні накладки, які закривають доступ до торцевої частини механізму секретності, його вибиття суттєво ускладниться.

Виходячи зі специфіки розглянутих вище методів запобігання в злому механізму дверей та замків секретності та акцентування уваги на необхідність системного підходу до питання захисту приміщення, при якому оцінка стійкості від злому має враховувати показники кожного елементу: механізму секретності, замка, дверей тощо. Рекомендується проводити постійний моніторинг ситуації з означеним питанням безпеки.

Одержано 17.04.2018

УДК 004.9

Данило Олексійович КУЛІКОВ,
курсант групи Ф4-202 ХНУВС
Науковий керівник: викладач кафедри кібербезпеки факультету № 4 ХНУВС кандидат технічних наук Світличний В. А.

ПЕНТЕСТ ЯК ПРІОРИТЕТНИЙ НАПРЯМОК В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

У ситуації, що склалася в наш час, популярним стає пентест, іншими ж словами тестування на проникнення.

Пентест – це новий метод оцінки безпеки комп'ютерних систем або мереж засобами моделювання атаки зловмисника. Сам процес включає в себе активний аналіз системи на наявність потенційних вразливостей, які можуть спровокувати некоректну роботу цільової системи, або ж в результаті повну відмову в обслуговуванні. Важливо виділити мету самого пентеста – це оцінка можливості його здійснення і прогноз економічних втрат в результаті успішного здійснення атаки. Результатом є звіт, який містить в собі всі знайдені вразливості системи безпеки, а також може містити рекомендації щодо їх усунення. Тобто, можна зробити висновок, що випробування на проникнення є частиною аудиту безпеки.

Слід виділити кілька різних методик випробувань на проникнення. Основними відмінностями є наявність інформації про досліджувану систему. Існує чотири вида систем: відкриті, закриті, напівзакриті та цільові.

При перевірці закритої системи атакуючий не має гадки відомостей про пристрій, що атакується. Завданням такого виду перевірки є збір необхідної інформації про розташування цільової системи, її інфраструктури.

У відкритих системах доступна повна інформація про цільовій системі, а в напівзакритих системах доступна часткова інформація. Розглянемо цільові системи, до них відносяться комп'ютерні системи з доступом з мережі Інтернет. Випробування на проникнення повинно проводитися до запуску цільової системи в масове використання. Це дає певний рівень гарантії, що будь-який атакуючий не зможе завдати шкоди, прямої або непрямої, роботі досліджуваної системи.

Тест на проникнення дозволяє досить швидко оцінити реальну захищеність обраних інформаційних активів від несанкціонованого доступу, моделюючи найбільш поширені атаки. Основною відмінною особливістю тесту на проникнення в порівнянні з традиційним аудитом інформаційної безпеки є:

– велика деталізація знайдених вразливостей;

– більш точна оцінка ризиків ІБ (грунтується на результатах реалізації знайдених вразливостей);

– оцінка більшої кількості процесів ІБ, ніж при інструментальному аудиті, включаючи оцінку процесів (наприклад, управління інцидентами, моніторинг і т.д.), об'єктивна оцінка яких не може бути отримана іншими засобами (інструментальний аудит, анкетування і інтерв'ювання і т.д.);

– детальне опрацювання знайдених вразливостей, що дозволяє отримати більш об'єктивну оцінку процесів забезпечення інформаційної безпеки організації.

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.