

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 БСЛЯЄВА,

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 KALI LINUX

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 БСЛЯЄВА,

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.