4. Зачко О. Б. Управління безпекою на стадії планування проектів з масовим перебуванням людей з врахуванням категорії складності / О. Б. Зачко, Д. С. Кобилкін, Р. Р. Головатий // Вісник НТУ «ХПІ». Серія: Стратегічне управління, управління портфелями, програмами та проектами. – Х. : НТУ «ХПІ», 2018. – № 2 (1278). – С. 53–58. – Бібліогр.: 17 назв. – ISSN 2311–4738.

5. Купчак М. І., Смотр О. О., Купчак М. Я. Тенденції та проблеми впровадження інформаційних технологій в управління підрозділами університету. Вісник Львівського державного університету безпеки життєдіяльності. 2013. № 7. С. 28–32.

6. Рак Ю. П. Формування проектів методом візуалізації інформації для підвищення стану безпеки торгово-розважальних центрів / 123 Ю. П. Рак, Р. Р. Головатий // Управління проектами у розвитку суспільства: зб. тез доповідей XII Міжнар. конф. – Київ: КНУБА, 2015. – С. 226 – 228

СКАНЕРИ ВРАЗЛИВОСТІ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Балацька В.С., Шабатура М.М.
Львівський державний університет безпеки життєдіяльності

Summary. The increasing volume of attacks on the Internet has increased the demand for sophisticated tools for vulnerability analysis, intrusion detection, forensic investigations, and possible responses. Current hacker tools and technologies warrant reengineering to address cyber crime and homeland security. The creation of network scanners is necessary to secure the information infrastructure by gathering network topology, intelligence, internal/external vulnerability analysis, and penetration testing.

Keywords: vulnerability scanner, security, cyber crime, "back door", network scanners.

Сканери вразливості – це комплексні рішення, які можуть являти собою як апаратні, так і програмні засоби, призначені для постійного сканування стану комп'ютерної мережі, на предмет дії вірусів або підозрілих процесів. Їх основним завданням є оцінка безпеки процесів і пошук вразливостей та їх усунення.

Vulnerability scanner або сканер вразливості, дає адміністратору можливість пошуку існуючих в мережі «дірок» або «бекдор», за допомогою яких, хакери і шахраї можуть отримати доступ до мережі компанії і конфіденційних даних. Крім цього, до складу сканерів входять засоби для сканування запущених служб і процесорів, а також сканери портів.

Виходячи з цього, можна виділити такі функції сканерів вразливостей:

- пошук вразливостей і їх аналіз;
- перевірка всіх ресурсів у мережі, пристроїв, операційної системи, портів, додатків, процесів і т.п.;
- створення звітів, у яких вказується вразливість, шлях її поширення і характер.

В основі сканера лежать два механізми [1]. Перший механізм називається – зондування. Даний механізм є не дуже швидкий, але найбільш ефективний інструмент активного аналізу. Суть його полягає у тому, що він сам запускає атаки, і стежить за тим, де ці атаки можуть пройти. Під час зондування, підтверджуються можливі припущення і можливості проходження атак на певних напрямках.

Інший механізм – сканування. У цьому випадку інструмент працює швидко, але виробляється тільки поверхневий аналіз мережі, по найчастішим і можливим «діркам» в безпеці мережі. Відмінність другого способу в тому, що він не підтверджує наявність уразливості, а тільки повідомляє адміністратора про її можливості, ґрунтуючись на непрямих ознаках. Наприклад, відбувається сканування портів, визначаються їх заголовки і потім вони порівнюються з еталонними таблицями і правилами. У разі розбіжності значень, сканер повідомляє про знаходження потенційної уразливості, які адміністратор повинен перевірити більш надійними способами.

Основні принципи роботи сканерів вразливостей:

- збір всієї інформації в мережі, ідентифікація всіх служб, пристроїв і процесів;
- пошук потенційних вразливостей;
- використання спеціалізованих методів і моделювання атак, для підтвердження уразливості (існує не у всіх мережевих сканерах).

На сьогоднішній день найбільш поширеними є такі сканери: Xspider, Nessus, Shadow Security Scanner.

Xspider. Як заявляється розробник, їх рішення здатне виявити третину всіх можливих вразливостей, так званих «zero day». Основною перевагою даного сканера, є можливість виявлення максимального числа «дірок» в системі безпеки, до того, як їх зможуть виявити хакери. Даний сканер не вимагає додаткового програмного забезпечення. Після проведення аналізу, він формує повний звіт зі знайденими уразливими і можливими способами їх усунення. XSpider [2] створювався в першу чергу експертами з інформаційної безпеки, яким був необхідний професійний інструмент найвищої якості. Відрізняється безкомпромісною якістю роботи, без якого користь від застосування сканера безпеки стає сумнівною, незалежно від наявності інших плюсів. Характеризується розумною ціною і легкістю володіння, оскільки інформаційна безпека покликана запобігати втратам, а не збільшувати їх. Однаково зручний у використанні для компанії будь-якого масштабу (від одиниць до десятків тисяч обслуговуючих вузлів з'єднання). Універсальність XSpider є те, що він хоч і працює під управлінням Microsoft Windows, також він перевіряє всі можливі вразливості незалежно від програмної і апаратної платформи вузлів: починаючи від робочих станцій під Windows і закінчуючи мережевими пристроями Cisco (не виключаючи, звичайно, *nix, Solaris, Novell, AS400 і т.п.).

Nessus. Даний сканер почав свою роботу, ще з 1998 року, компанія Tenable Network Security, почала займатися розробкою свого сканера враз-

ливостей, завдяки чому має великий досвід і далеко попереду в своїй сфері. Багато років їх сканер є комерційним ПЗ. Ключовою особливістю сканера Nessus [3], є можливість розширювати функціонал за допомогою різноманітних плагінів. Таким чином, потужні тести, а саме тести на проникнення або інші, не встановлюються разом з головним модулем, а при необхідності підключаються окремо. Всі плагіни можна розділити на 42 категорії. Це означає, що, наприклад, для проведення пінтеста (тесту на проникнення), не обов'язково запускати повну перевірку, а можна виділити тільки тести з певної категорії або вибрати режим тестування вручну. Крім цього, Nessus має свою спеціальну скриптову мова, так що, адміністратори можуть самі писати необхідні їм тести.

Shadow Security Scanner. Сканер мережевої безпеки який завдяки унікальним методам дозволить надійно перевірити сайт або мережу на наявність дір і дозволить надійно захистити мережу від проникнення хакерів. При скануванні системи, програма робить аналіз даних, виявляє уразливі місця, можливі помилки у налаштуванні сервера і запропонує можливі шляхи виправлення недоліків та вразливих місць у системі, підкаже, звідки можна завантажити патч або оновлене програмне забезпечення. Вміє автоматично (Fix-It) виправляти знайдені помилки у безпеці одним натисканням на кнопку в меню Fix-It.

Shadow Security Scanner [4] сканує не тільки машини на яких стоять операційні системи Windows, але так само різні операційні системи Unix (Linux, * BSD, Solaris, etc) роутери, файрволи та системні пристрої. У нього входить аудит таких модулів як TCP / IP, UDP, FTP, DNS, SMTP, POP3, HTTP, CGI, NetBIOS, Registry, Users accounts, Password checks, Services, LDAP, DoS атаки, і багато іншого.

Висновок: використовувати такого роду засоби треба. Але хочу зауважити, що не варто вважати їх панацеєю від усіх бід. Вони ні в якому разі не замінюють фахівців в області безпеки. Вони всього лише автоматизують їх роботу, допомагаючи швидко перевірити сотні вузлів, в т.ч. і знаходяться на інших територіях. Вони допоможуть виявити практично всі відомі уразливості і порекомендувати заходи, їх усувають, автоматизують цей процес, а з урахуванням можливості опису своїх власних перевірок, допоможуть ефективно застосовувати їх в мережі будь-якої організації, з огляду на саме специфіку роботи.

Література:

1. Як працює сканер безпеки [Електронний ресурс] – Режим доступу: http://citforum.ru/internet/securities/scaner.shtml, вільний;

2. Сканер уязвимостей XSpider 7 [Електронний ресурс] – Режим доступу: http://www.ixbt.com/soft/xspider7.shtml#int, вільний;

3. NESSUS vulnerability assessment [Електронний ресурс] – Режим доступу: https://www.tenable.com/products/nessus, вільний;

4. Shadow Security Scanner [Електронний ресурс] – Режим доступу: http://www.safety-lab.com/en/products/securityscanner.htm, вільний.