“strong” primes needed for RSA? RSA Laboratories Seminar Series // Seminars Proceedings, 1999. 11. Байденко П. В., Кудін А. М. Ефективність застосування алгоритмів факторизації до модулів криптосистеми RSA // X Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених “Теоретичні і прикладні проблеми фізики, математики та інформатики” 19–20 квітня 2012 р. – Збірка тез доповідей учасників. – К., 2012. – С.253–254. 12. Ишмухаметов Ш.Т. Методы факторизации натуральных чисел. LAP LAMBERT Academic Publishing. – 2014. – 256 с. 13. Ишмухаметов Ш. Т., Шарифуллина Ф. Ф. О распределении полупростых чисел // Изв. вузов. матем. 2014. – №8. – С.53–59. 14. Hildebrand A. On the number of positive integers ≤ x and free of prime factors> y // Journal of Number Theory. v.22. Issue 3. 1986. – P.289–307.

УДК 004.451, 004. 492

Я. Я. Стефінко, А. З. Піскозуб
Національний університет “Львівська політехніка”,
кафедра безпеки інформаційних технологій,
кафедра захисту інформації

ВИКОРИСТАННЯ ВІДКРИТИХ ОПЕРАЦІЙНИХ СИСТЕМ ДЛЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ В НАВЧАЛЬНИХ ЦІЛЯХ

Наведено інформацію про методологію тестів на проникнення, його методів і способів реалізації. Проаналізовано сучасні безкоштовні та з відкритим вихідним кодом програми. Розглянуто приклад тестування на проникнення в академічній сфері в навчальних цілях на базі Kali Linux і Metasploitable 2 Linux. Ці перевірки і методи показують проактивні методи захисту та повинні допомогти поліпшити безпеку комп'ютерних систем і корпоративних мереж.

Ключові слова: Kali Linux, Metasploitable, пентест, проникнення, вразливість, Metasploit Framework, PTES, тест на проникнення, безпека, проактивний захист, корпоративні мережі.

USING KALI LINUX AND METASPLOITABLE FOR PENETRATION TESTING FOR STUDYING PURPOSES

This paper comprises information about penetration testing methodology, its methods and ways of implementation. The current free and open-source software has been analyzed. It has been done the example of penetration testing in academic field for studying purposes on the base of Kali Linux and Metasploitable2 Linux. This tests and techniques purpose proactive methods of defense and must help to improve security of computer systems and corporate networks.

Key words: Kali Linux, Metasploitable, pentest, penetration, vulnerability, Metasploit Framework, PTES, pentest, security, proactive defense, corporate networks.

Вступ

Сучасні комп’ютерні системи і мережі зазнають тисяч різних атак як ззовні, так і зсередини. Тому актуальним сьогодні є питання різнобічного підходу до питання захищеності. Саме тут виникає потреба оцінювання захищеності системи до зламу та запобігання його руйнівним наслідкам. Тести на проникнення є складовою повного аудиту безпеки.

Найчастіше такі тести проводять у таких випадках: перед введенням в експлуатацію нового сервісу, після внесення значних змін в IT-інфраструктуру підприємства, періодично з частотою, зазначеною в нормативних документах підприємства, але, як правило, не рідше 1 разу на рік для оцінювання реальних загроз і вразливостей.

Тестування на проникнення та його можливості

Тест на проникнення (далі – пентест) дає змогу моделювати несанкціонований доступ в інформаційні системи, а також інші дії, які допомагають порушити нормальне функціонування систем і бізнес-процесів. По суті, це метод оцінювання захищеності інформаційних систем та/або інформації та об'єктів, де вона зберігається або обробляється від несанкціонованого використання.

Пентест виглядає як генеральна репетиція дій “зломщиків”. Сьогодні ця послуга стає все популярнішою і критично необхідною в області інформаційної безпеки у всьому світі. Сенс подібних робіт полягає в санкціонованій спробі обійти існуючий комплекс засобів захисту інформаційної системи. Під час тестування аудитор грає роль зловмисника або “зломщика”, перед яким стоїть завдання порушити інформаційну безпеку мережі замовника. Тестувальника ще називають етичним хакером через те, що під час цього тестування він повинен дотримуватись угоди про здійснення пентесту. Цю угоду пентестер і замовник повинні підписати заздалегідь, щоб не допустити витоку інформації про стан захисту на конкретному підприємстві.

Об'єктами тестів на проникнення є різноманітні компоненти інформаційної інфраструктури: активне мережеве обладнання, сервери, робочі станції, сервіси, інформаційні системи, бази даних. Завдання пентестера – виявити в них вразливості і з'ясувати можливість їх експлуатації, після чого ліквідувати ці вразливості. Проте до тестування на проникнення потрібно обов’язково підходити з огляду етичного хакінгу [1].

Тести на проникнення необхідно проводити регулярно, оскільки постійно з'являються нові вразливості, розробляються нові експлоїти, змінюється інфраструктура та умови, в якій функціонують інформаційні системи.

У межах етичного хакінгу аудитори здійснюють повний аналіз всіх деталей досліджуваного об'єкта, вибирають відповідні сценарії атак, враховуючи людський фактор, можливо, розробляють унікальне для кожного конкретного випадку програмне забезпечення чи скрипти для спроби проникнення до інформаційної системи.

Зазвичай в пентестах використовують допрацьовані методики Національного інституту стандартів і технології США (NIST) Draft Guideline on Network Security Testing і Open-Source Security Testing Methodology (OSSTM). Вибирають об'єкти дослідження, задають модель порушника і вибирають режим тестування на основі рівня початкових знань виконавця про систему, що тестується (Black Box або White Box) і рівня інформованості замовника про випробування (режим Black Hat або White Hat).

Важко сказати про найактуальнішу чи популярну методику пентесту. До того ж жодна методика (за винятком OWASP) детально не може бути застосована у конкретному проекті. Провідні спеціалісти часто застосовують елементи OSSTMM, OISSG. Зараз набуває популярності відкритий стандарт PTES (Penetration Testing Execution Standard), але його всеосяжність є і його слабким місцем. Для Web-додатків найпридатнішою є методика OWASP (Open Web Application Security Project). OWASP TOP 10 – це проект для збільшення обізнаності про безпеку додатків за допомогою визначення найкритичніших ризиків, що загрожують організаціям. На проект Топ-10 посилається безліч стандартів, інструментів і організацій, зокрема MITRE, PCI DSS, DISA, FTC та ін.

Кожна методика має свої переваги і недоліки. Деякі методики роблять наголос на технічній складовій тесту, інші описують організацію самого процесу тестування. Методики, як правило, описують загальні принципи проведення тесту і можуть бути використані як довідковий посібник або мінімальний стандарт.

При проведенні тесту на проникнення важливо чітко регламентувати дії сторін, виділити узгоджені тимчасові інтервали для проведення активних дій, визначити етапність, ті чи інші обмеження, погоджувати дії під час переходу від етапу до етапу. Без виконання зазначених умов є

ризик порушення платіжних та інформаційних технологічних процесів, сервісів, реалізованих на базі об'єктів інформаційної інфраструктури, які піддаються дослідженню. Крім того, необхідно послідовно документувати отримані результати і на їх основі формувати пропозиції щодо виправлення виявлених проблем. Адже проведення тесту не є самоціллю – важливо надалі доопрацювати результати тесту і усунути виявлені вразливості.

Особливу увагу в методології проведення тестів на проникнення звертають на оцінку виявлених вразливостей і ранжуванню їх за ступенем критичності. Класичні вразливості – це слабкі паролі, неоновлення операційних систем чи прикладного програмного забезпечення (ПЗ), помилки у програмуванні прикладних систем, особливо веб-орієнтованих, відкриті без необхідності порти на граничних мережевих пристроях.

Під час проведення пентесту важливо чітко регламентувати дії сторін, виділити узгоджені тимчасові інтервали для проведення активних дій, визначити етапність, обмеження, погоджувати дії, переходячи від етапу до етапу. Крім того, необхідно послідовно документувати отримані результати і на їх основі формувати пропозиції щодо виправлення виявлених недоліків. Адже проведення тесту не є самоціллю – важливо опрацювати результати тесту й усунути виявлені вразливості.

Актуальні інструменти для пентесту

Kali Linux [4] – це орієнтований на платформі Linux Debian арсенал для тестування на проникнення, який створили для відпрацювання саме етичного хакінгу.

В основу роботи Kali покладено використання методики пентесту, що складається з 10 етапів, якими є: визначення меж тестування (Target Scoping), збирання інформації про цільову систему (Information Gathering), виявлення працюючих цільових хостів (Target Discovery), виявлення працюючих сервісів на цільових хостах (Enumerating Target), визначення вразливостей на цільових хостах (Vulnerability Mapping), соціальна інженерія (Social Engineering), злам цільових систем (Target Exploitation), підвищення привілеїв на цільових системах (Privilege Escalation), збереження доступу після зламу цільових систем (Maintaining Access) і документація та звітність (Documentation and Reporting) [1].

Практично для кожного з цих етапів характерні свої програми з набору утиліт Kali Linux:

- Узгодження із замовником умов тестування та бажаного результату – підписання умов застосування. Збирання інформації: пасивне та активне. Для пасивного застосовують: GHDB (пошукову машину Google), Nmap (сканер портів чи навіть більше), Wireshark, Maltego; для активного – утиліти driftnet, dnsmap, arpspoof та ін. Сьогодні неможливо переоцінити можливості Maltego. Вона збирає інформацію з різних БД і подає її у дуже зручному вигляді. Працюючі хости визначаємо: ping, arping, hping3, fping та ін. Потім застосовують Nmap із його розширеними опціями [3].
- Для визначення вразливостей на цільових хостах фахівці зазвичай застосовують такі сканери, як Nessus, Nexpose, OpenVAS, w3af та ін.
- Соціальна інженерія не є обов’язковою складовою пентесту, хоча інколи вона буває визначальною частиною тестування. Найвживанішим у цьому випадку інструментом з набору Kali є SET [3].
- Злам цільових систем дає змогу застосувати експлоїти для виявлених вразливостей та отримати доступ до цільового хоста: Metasploit Framework [2], SQLmap тощо.
- На етапах підвищення привілеїв на цільових системах та збереження доступу після їх зламу цільових систем пентестер намагається не лише підвищити свої привілеї до суперкористувача (root), але й витерти “сліди” свого перебування на цільовій системі та залишити собі лаз (backdoor).
- Документація та звітність є невід’ємною частиною етичного хакінгу та останнім етапом, на якому формуються детальний звіт про виконані роботи та отримані результати.

Metasploitable 2 Linux – операційна система, спеціально спроектована на максимальну вразливість для тестування, тести експлоїтів і навчання новачків. Віртуальна машина Metasploitable – це навмисно уразлива версія Ubuntu Linux, призначена для випробувань засобів безпеки та демонстрації поширених вразливостей. Версія 2 цієї віртуальної машини вільно доступна для усіх користувачів Інтернету. Ця віртуальна машина сумісна з VMWare, VirtualBox та іншими платформами загальної віртуалізації.

На відміну від інших вразливих віртуальних машин, Metasploitable фокусується на вразливостях в операційній системі Linux і мережевих сервісах загалом [5].

У таблиці наведено результат роботи утиліти nmap із додатковими ключами при скануванні Metasploitable. Практично кожен з цих відкритих портів є точкою для входу в систему за правильного використання сучасних утиліт.

Сканування мережевих портів

*root@kali:~# **nmap –p0-65535 192.168.99.131***	*1099/tcp open rmiregistry*
Starting Nmap 5.61TEST4 (http://nmap.org) at 2012-05-31 21:14 PDT	*1524/tcp open ingreslock*
Nmap scan report for 192.168.99.131	*2049/tcp open nfs*
Host is up (0.00028s latency).	*2121/tcp open ccproxy-ftp*
Not shown: 65506 closed ports	*3306/tcp open mysql*
PORT STATE SERVICE	*3632/tcp open distccd*
21/tcp open ftp	*5432/tcp open postgresql*
22/tcp open ssh	*5900/tcp open vnc*
23/tcp open telnet	*6000/tcp open X11*
25/tcp open smtp	*6667/tcp open irc*
53/tcp open domain	*6697/tcp open unknown*
80/tcp open http	*8009/tcp open ajp13*
111/tcp open rpcbind	*8180/tcp open unknown*
139/tcp open netbios-ssn	*8787/tcp open unknown*
445/tcp open microsoft-ds	*39292/tcp open unknown*
512/tcp open exec	*43729/tcp open unknown*
513/tcp open login	*44813/tcp open unknown*
514/tcp open shell	*55852/tcp open unknown*
	MAC Address: 00:0C:29:9A:52:C1 (VMware)

До складу надвразливих застосунків у Metasploitable входять:

- mutillidae (NOWASP Mutillidae 2.1.19)
- dvwa (Damn Vulnerable Web Application)
- phpMyAdmin
- tikiwiki (TWiki)
- tikiwiki-old
- dav (WebDav)

Вразливості веб: Mutillidae

The Mutillidae – це веб-застосунок (NOWASP (Mutillidae)), який містить усі вразливості з набору OWASP Top Ten, такі як HTML-5 web storage, forms caching, і click-jacking. На відміну від DVWA, Mutillidae дає користувачу змогу змінювати “Security Level” від 0 (повністю небезпечно) до 5 (безпечно). Якщо застосунок пошкоджений ін’єкціями коду чи іншими діями користувача, то натиснувши “Reset DB”, застосунок відновиться до оригінального вигляду. Ця програма дасть змогу випробувати всі сучасні атаки на веб-додатки чи сайти в інтернеті.

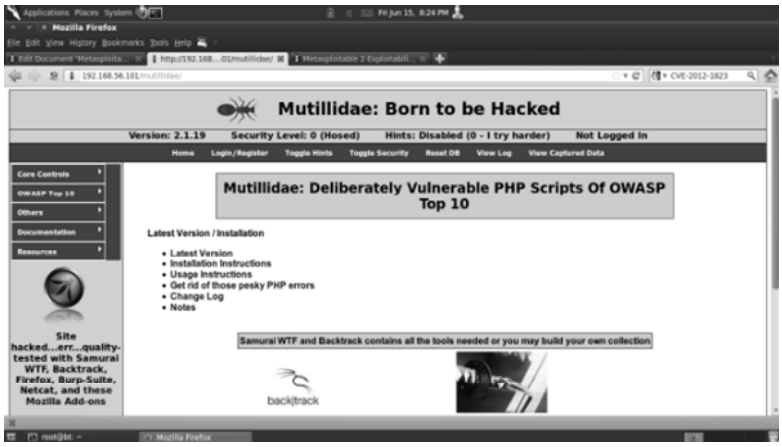

*Рис. 1. Робоче вікно **Mutillidae***

DVWA

Damn Vulnerable Web App (DVWA) – це “дуже вразливий веб-додаток” з PHP/MySQL Головні цілі: стати основним додатком для професіоналів у сфері безпеки, випробовувати їх знання і вміння, допомагати веб-розробникам, викладачам і студентам вивчати безпеку веб-додатків на реальному прикладі у навчальних середовищах.

Default username = admin

Default password = password

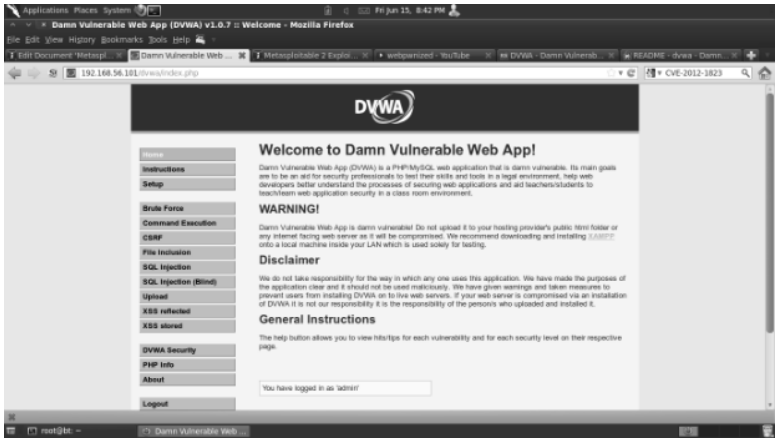

*Рис. 2. Робоче вікно **DVWA***

Metasploitable 2 Linux містить вразливі веб-сервіси (DVWA, Mutillidae), бази даних, слабкі паролі, backdoors, можливості розкриття інформації та інші неприємні речі, що вже повинні бути усунуті в найсучасніших та постійно оновлюваних ОС та сервісах. Це зроблено для зручного і наочного прикладу, як це не потрібно робити.

Застосування вищезгаданого ВВПЗ та навчально-методичний аспект

Для навчання студентів чи будь-яких інших ІТ-спеціалістів ми наводили два такі приклади пентесту: Kali > Metasploitable2, Kali > Windows XP, Kali > > Windows 7, причому всі ці операційні системи є віртуальними машинами на кафедральному сервері. Дослідження проводили в навчально-методичних лабораторіях кафедр безпеки інформаційних технологій та кафедри захисту інформації з використанням сервера vSphere ESXi. На сервері було попередньо встановлено різноманітні ОС (Kali linux, Metasploitable, Windows XP, Windows 7), які були предметом тестування на проникнення.

Подібне застосування цих сучасних інструментів в навчальних цілях здійснюється вперше у межах нашого університету, а можливо навіть у межах інших ВНЗ м. Львова. Ці дослідження дадуть змогу розробити курси для навчання студентів у лабораторіях зазначених кафедр. Вони здійснювались для підвищення фахового рівня студентів, ознайомлення їх з найновішими досягненнями в ІТ-галузі, а саме у сфері безпеки інформаційних та комунікаційних систем.

Тестування допомагає вивчити та випробувати всі сучасні інструменти з пакета Kali Linux та просканувати всі можливі дірки у захисті Metasploitable. Крім цього, застосувавши їх, ми можемо проаналізувати знайдені вразливості, відкриті порти, запущені сервіси і, відповідно, створювати різні надбудови над основним захистом нашої ОС чи комп’ютерної мережі. Це дасть нам змогу підняти загальний рівень захищеності систем.

Висновки

Як показує практика, більшість виявлених вразливостей пов'язана з несвоєчасним оновленням ПЗ і засобів захисту, використанням попередньо встановлених параметрів настроювання ПЗ та мережевого обладнання, недотриманням політики безпеки, помилками в ПЗ, доступних з Інтернету сервісів і т.д.

Методи тестування на проникнення постійно удосконалюються і, на жаль, використовуються не лише в оборонних, але і в наступальних цілях.

Формування фахівців у сфері інформаційної безпеки, які володіють сучасними засобами як захисту, так і зламу комп'ютерних систем, дає змогу підвищити обороноздатність країни, адже кібервійна практично завжди супроводжує будь-які військові дії.

1. Піскозуб А.З. Використання тестування на проникнення в комп'ютерні мережі та системи для підняття їх рівня захищеності // Матеріали третьої міжнародної науково-практичної конференції FOSS Lviv 2013,. – Львів,2013. 2. Kennedy D., O'Gorman J. Metasploit. The penetration tester's guide. – No starch press, San Francisco, 2011. 3. Pritchett W., Smet D. Kali Linux Cookbook – Birmingham-Mumbai, Puckt Publishing, 2013. 4. Kali Linux. https://kali.org 5. Metasploitable 2. https://community.rapid7.com/docs/DOC-1875.

УДК 004.032.026

П. В. Тимощук
Національний університет "Львівська політехніка",
кафедра систем автоматизованого проектування

АНАЛІЗ МОДЕЛІ ШВИДКІСНОЇ АНАЛОГОВОЇ НЕЙРОННОЇ СХЕМИ ІДЕНТИФІКАЦІЇ НАЙБІЛЬШИХ ЗА ЗНАЧЕННЯМИ З МНОЖИНИ СИГНАЛІВ

Проаналізовано моделі неперервного часу швидкісної аналогової нейронної схеми, придатної для ідентифікації *K* найбільших серед *N* невідомих сигналів, де $1 \le K < N$, які можна розрізняти, із скінченними значеннями. Модель описується рівнянням стану з розривною правою частиною і вихідним рівнянням. Аналізуються існування та єдиність встановлених режимів, збіжність траєкторій змінної станів і час збіжності до KWTA-режиму. Порівняно модель з іншими близькими аналогами. Згідно з отриманими результатами, модель володіє вищою швидкістю збіжності до KWTA-режиму, ніж інші аналоги.

Ключові слова: модель неперервного часу, аналогова нейронна схема, розривна права частина, встановлений режим, час збіжності, KWTA-режим.

MODEL ANALYSIS OF FAST ANALOGUE NEURAL CIRCUIT OF LARGEST VALUE SIGNAL SET IDENTIFICATION

An analysis of continuous-time model of high speed analogue *K*-winners-take-all (KWTA) neural circuit which is capable of identifying the *K* largest of unknown finite value *N* distinct inputs, where $1 \le K < N$ is presented. The model is described by a state equation with discontinuous right-hand side and by an output equation. Existence and uniqueness of the steady-states, convergence of state-variable trajectories and convergence time to the KWTA operation are analyzed. The model comparison with other close analogs is given. According to obtained results, the model possesses a higher convergence speed to the KWTA operation than other comparable analogs.

Key words: continuous-time model, analogue neural circuit, discontinuous right-hand side, steady-state, convergence time, KWTA operation.

Вступ

Схеми типу "K-winners-take all" (KWTA), як відомо, забезпечують вибір K найбільших з множини N вхідних сигналів, де $1 \le K < N$ – позитивне ціле число [1]. У частковому випадку, коли