Данченко, Т. Ю. Олєйнікова, Г. О. Заспа // Вісник Черкаського державного технологічного університету : зб. наук. пр. – Черкаси : ЧДТУ, 2004. – № 2. – С. 157-159.

3. *Белощицкий А. А. Структура методологии проектно-векторного управления образовательными средами / А. А. Белощицкий // Управління розвитком складних систем : зб. наук. пр. – К. : КНУБА, 2011. – № 7. – С. 121-125.*
4. *Дерев'янчук А. Й. Загальний методичний підхід до створення навчальних комп'ютерних 3D моделей військово-технічного призначення / А. Й. Дерев'янчук, Д. Р. Москаленко // Сучасні інформаційні технології у сфері безпеки та оборони : зб. наук. пр. – К. : Національний університет оборони України імені Івана Черняховського, 2014 – № 3. – С. 82-88.*
5. *Гумен О. М. Графічні інформаційні технології у підготовці фахівців технологічних спеціальностей / О. М. Гумен, С. Є. Лясковська, Є. В. Мартин // Теорія і методика електронного навчання : зб. нак. пр. – Кривий Ріг : Криворізький національний університет, 2013 – Вип. IV. – С. 65-68.*
6. *Рак Ю. П. Формально-логічні моделі проектування комп'ютерного тренажера з відпрацювання тактичних навиків у керівника ліквідації пожежі / Ю. П. Рак, О. Б. Зачко, Т. Є. Рак // Вісник Національного університету "Львівська політехніка". – 2010. – № 688 : Комп'ютерні системи та мережі. – С. 197–203.*
7. *Зачко О.Б. Формирование информационной инфраструктуры высшего учебного заведения: проектный поход / О.Б. Зачко, Ю.П. Рак, Т.Є. Рак // Новые информационные технологии в образовании для всех / монография. – К. : Академпериодика, 2012. – С. 153-166.*

УДК 004.451, 004. 492

Ярослав Стефінко, Андріян Піскозуб, Роман Банах
Національний університет "Львівська політехніка"

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ У НАВЧАЛЬНИХ ЛАБОРАТОРІЯХ З ЗАСТОСУВАННЯМ КОНТЕЙНЕРИЗАЦІЇ

Ця стаття містить інформацію про загрози в комп'ютерних мережах і системах, і тестування на проникнення як один з шляхів їх

захисту. Наймогутнішими інструментами для цієї цілі є операційна система Kali Linux і вбудовані інструменти. Навички етичного хакінгу є надзвичайно важливими для сучасного спеціаліста у сфері інформаційної безпеки. Запропоновано методи практичного впровадження тестування на проникнення з застосуванням технології контейнеризації в навчальні курси. Представлені пропозиції впровадження Docker в курси по захисту інформації. Проаналізовано та запропоновано практичне вирішення проблем тестувань безпеки в лабораторіях кафедр університету.

Ключові слова: проактивний захист, тест на проникнення, контейнер, вразливості, зловмисник, захищеність, віртуалізація, тестування безпеки.

This article contains information about threats to computer networks and systems, and penetration testing as a one of the ways of protection. Powerful tools for this purpose is the operating system Kali Linux and embedded tools. Ethical hacking skills are essential for a modern specialist in the field of information security. The methods of practical implementation of penetration testing using technology containerization in training courses are suggested. Docker implementation approach into courses of information security are presented. Analyzed and proposed practical problems of safety testing in laboratories of university departments.

Keywords: proactive protection, penetration test, container, vulnerability, the attacker, security, virtualization, security testing.

Вступ. У світі інформаційних технологій комп'ютерні мережі і системи стають невід’ємним інструментом в житті сучасної людини, і все більшу роль при цьому відіграють аспекти інформаційної безпеки. Разом з тим, кіберзлочинність зростає, кількість вразливих операційних систем (ОС) та іншого програмного забезпечення (ПЗ) також невпинно росте. Зловмисники - кібер-злочинці, з одного боку та хакери-активісти чи кібер-військові з іншого боку, постійно поповнюють свій арсенал новими програмами, вірусами, троянами тощо. Слідом за цим неминуче з'являються нові методи і способи для захисту комп'ютерних систем. Важливим є вчасно виявити і закрити вразливість в операційних системах чи ПЗ. Тому дана проблематика є надзвичайно актуальною в сучасному світі, зокрема в українських реаліях. З навчальної точки зору, підготовка спеціалістів у сфері інформаційної безпеки є

необхідною загалом для інформаційної безпеки держави. Так як будь-які знання потребують практичних навичок, запропоновано навчати етичного хакінгу студентів, щоб закріпити їх знання у сфері інформаційної безпеки.

Технологія тестування на проникнення (етичного хакінгу) в даний час не є новинкою і сьогодні рясніє спрощеними графічними інтерфейсами для користувача. Незважаючи на простоту у використанні, вони часто виявляються дуже обмеженими і не пропонують надто інформативний досвід для своїх користувачів. Ще одним недоліком є те, що багато з цих рішень оцінки безпеки розроблені тільки для ідентифікації та автоматизації експлуатації у найбільш очевидних і традиційних випадках вразливостей. Для будь-якого іншого практичного прикладу уразливості, тестувальнику безпеки (етичному хакеру) потрібно покладатися на свої власні сценарії та інструменти оцінки. Часто потрібно проаналізувати ціль тестування, виконати розробку скриптів чи ПЗ, та вже після цього виявити конкретну вразливість в операційних системах чи програмах. Саме цими важливими аспектами сучасної кібербезпеки повинні володіти студенти, випускники та інші спеціалісти у сфері інформаційної безпеки.

Тенденції тестування на проникнення. Тест на проникнення (пентест) дозволяє моделювати несанкціонований доступ в інформаційні системи, а також інші дії, які дозволяють порушити нормальне функціонування систем і бізнес-процесів. По суті, це метод оцінки захищеності інформаційних систем та/або інформації, та об'єктів, де вона зберігається або обробляється від несанкціонованого використання [2].

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 часто стає ключовим елементом в повному аудиті безпеки організації, де циркулює секретна інформація чи інформація з обмеженим доступом. Також пентест став одним з вимог для міжнародних сертифікацій щодо впровадження електронних платіжних систем чи сертифікацій банківських установ.

Тести 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 ПЗ чи скрипти (bash, python, ruby) для спроби проникнення до інформаційної системи.

Тестування на проникнення має три основних різновиди. Найбільш реалістичним, звичайно, вважають Black Hat, адже він дозволяє симулювати атаки і проникнення зловмисника ззовні без знань про систему. Хоча, останні дослідження також показують, що краще тестувати з усіма необхідними знаннями (White Hat) і постаратись виявити якомога більше слабких місць в системі та вразливостей ПЗ.

В основу роботи операційної системи Kali Linux покладено використання добре відомої методики пентесту, що складається з 10 етапів, якими є: визначення меж тестування (Target Scoping), збирання інформації про цільову систему (Information Gathering), виявлення працюючих хостів (Target Discovery), виявлення працюючих сервісів (Enumerating Target), визначення вразливостей (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].

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 тестування на проникнення, проаналізувати вразливості і усунути їх в порядку критичності. Важливим аспектом також є так званий ROI (return of investment), що показує наскільки дані тестування ефективні та допомагають заощадити майбутні витрати на можливі витоки інформації чи кібератаки.

Етичний хакінг для студентів і практика. В курсах для спеціальностей кафедри безпеки інформаційних систем та кафедри захисту інформації надзвичайно цікавим і доцільним буде застосування всіх без винятку технік етичного хакінгу. На даний момент вже є достатньо теоретичної бази та практична частина не надто розвинута. Саме дане дослідження повинно мати практичне застосування в розробці практичних і лабораторних робіт для навчання тестування на проникнення. Реальні практичні навички спеціалістів у сфері інформаційної безпеки можна розвинути тільки при використанні найсучаснішого програмного та апаратного забезпечення. Це дозволить більше заглибитись в технічні деталі тестувань та сприятиме розвитку навичок

дослідника чи розробника у студентів, що працюють з сучасними системами, алгоритмами та міжнародними методиками.

Середовище для тестувань безпеки буде представлене на прикладі спеціалізованої операційної системи Kali Linux. Kali - це дистрибутив взятий з Debian, і він упакований з утилітами, орієнтованими виключно на вирішення технічних проблем безпеки і тестування на проникнення. Таким чином, для ефективного тестування безпеки необхідно також мати вразливу операційну систему чи ПЗ. Для прикладу це може бути будь-який Linux server зі стандартним набором серверного ПЗ, так як LAMP server. Також в якості вразливого сервера можна розглянути Metasploitable 2 Linux – образ Linux, навмисно створений з великою кількістю вразливостей.

Так як студенти повинні проводити багато досліджень та кожен повинен отримати індивідуальні результати та напрацювання, ми пропонуємо використовувати щоразу нові віртуальні образи систем. Адже кожен повинен отримати чистий образ для своїх власних дослідів. Для цілей тестувань часто використовували системи для віртуалізації, такі як VirtualBox чи VMWare. Проте з розвитком технології контейнеризації це питання починає вирішуватись значно легше та ефективніше. У цьому нам допомагає нова технологія Docker, яка запозичила більшість функціональності з давно відомої технології LXC для Linux.

Docker — open-source інструментарій для управління ізольованими Linux-контейнерами, який вільно поширюється з ліцензією Apache. Він доповнює технологію віртуалізації LXC більш високорівневим API, що дозволяє маніпулювати контейнерами на рівні ізоляції окремих процесів. Зокрема, Docker дозволяє, не переймаючись вмістом контейнера, запускати довільні процеси в режимі ізоляції, потім переносити і клонувати сформовані для даних процесів контейнери на інші сервери. При цьому він надає інтерфейс для створення, обслуговування і підтримки контейнерів.

Docker надає API (Application Programming Interface) для управління зображення, а також можливість використання віддаленого реєстру для спільного використання контейнерів. Ця схема вигідна обом розробникам, тестувальникам безпеки і системним адміністраторам, зважаючи на наступні переваги:

- швидке розгортання додатків чи ОС;
- транспортабельність між серверами;
- управління версіями і повторне використання компонентів [8];
- спільне використання та віддалений репозиторій;

• спрощене обслуговування.

Таким чином, дане дослідження рекомендує специфічні налаштування лабораторії з застосуванням контейнеризації Docker для покращення ефективності роботи студентів на практичних та лабораторних роботах. Основною перевагою буде простота та швидкість розгортання нових операційних систем з готових docker образів.

Впровадження в курси. В теперішніх умовах, ми бачимо, як щоденно виявляються нові вразливості у всесвітньо відомих і широко використовуваних протоколах чи системах (Bash shellshock, SSL heartbleed etc.). Тому жодну систему чи протокол зараз не можна вважати цілком і абсолютно захищеними. В кожної сучасної компанії чи фінансової установи виникає необхідність проведень пентестів, які у поєднанні з різними скриптами дозволить сповна використати усі можливості ОС Kali Linux чи інші хакерські утиліти. В підготовці комп'ютерної лабораторії для тестування на проникнення особливу роль відіграє технологія віртуалізації і контейнеризації. Отож зараз docker і його підпроекти взагалі є ключовими інструментами для здійснення ефективних тестів на проникнення та для виявлення нових вразливостей, адже вони дозволяють заглибитись в найдрібніші деталі певних операційних систем і не витрачати час на розгортання великих віртуальних машин. Наприклад, студент розгортає влсну міні лабораторію на окремому ПК і робить всі необхідні тести для виконання лабораторної роботи. Після цього все документує і подає звіт викладачу.

Отже, для прикладу наведемо дві прості команди з інтерфейсу docker:

#docker pull kalilinux/kali-linux-docker

#docker run -t -i kalilinux/kali-linux-docker /bin/bash

Перша з них, завантажує готовий офіційний образ Kali Linux з публічного репозиторію Docker Hub. Друга – стартує контейнер на базі цього образу.

Також існує можливість управління цілим кластером контейнерів на одному чи кількох серверах за допомогою інструментів Docker Compose і Docker Swarm.

Висновки. Запровадження контейнеризації в навчальні програми дозволить навчати студентів на сучасних інструментах з корпоративного сегменту та дасть їм всі необхідні практичні навички, що дуже необхідні для сучасного фахівця з інформаційної безпеки. Отже, дані практичні дослідження і пропозиції пропонуються для використання в навчальних курсах для студентів кафедр захисту інформації та кафедри безпеки інформаційних систем ІКТА.

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

важливим є питання своєчасного виявлення вразливостей в захищених чи стратегічно важливих для держави системах з допомогою періодичного проведення тестування на проникнення.

Література

1. *Піскозуб А.З. —Використання тестування на проникнення в комп'ютерні мережі та системи для піднятя їх рівня захищеності" // Матеріали третьої міжнародної науково-практичної конференції FOSS Lviv 2013 – Львів, 2013.*
2. *Стефінко Я.Я.,Піскозуб А.З. "Використання відкритих операційних систем для тестування на проникнення в навчальних цілях" // Вісник НУ —Львівська політехніка": "Комп'ютерні системи та мережі". – 2014. – № 806. – С.258-263.*
3. *Стефінко Я.Я., Піскозуб А.З., Банах Р.І. / "Тестування на проникнення з Metasploit і shell скриптами" // Вісник НУ —Львівська політехніка": —Серія: Автоматика, вимірювання та керування : збірник наукових праць. – 2015. – № 821. – С. 90–93.*
4. *Y.Stefinko, A.Piskozub, R.Banakh —Manual and automated penetration testing. Benefits and drawbacks. Modern tendency" // Матеріали Міжнародної конференції —Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії— TCSET 2016 – Львів-Славсько, 2016. – с.488-492. IEEE doi: 10.1109/TCSET.2016.7452095*
5. *J. Andress, Ryan Linn. Coding for Penetration Testers. Elsiever - London, 2012, 321c.*
6. *M. Bishop —About Penetration Testing". - IEEE Security & Privacy, December 2007, p.84-87.*
7. *A.Grattafiori —Understanding and Hardening Linux Containers" // NCC Group Whitepaper April 20, 2016 – Version 1.0.*
8. *A.Mouat —Using Docker. Developing and Deploying Software with Containers"- O'Reilly Media- 2015, - 354c.*
9. *Anthony Bettini —Vulnerability exploitation in docker container environments", FLAWCHECK Inc., Presented at Black Hat Europe, - 2015.*