КОМПАНІЯ «E-TRADE HUB LTD.»
МІЖНАРОДНИЙ ІНСТИТУТ ЕКОЛОГІЧНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ БЕЗПЕКИ СПІЛЬНОТИ ЄВРОПИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ХАРЧОВИХ ТЕХНОЛОГІЙ
ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ НТУУ «КПІ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА
ТОВ «ІТЦ ХАЙ-ТЕК БЮРО»
ЦЕНТР ЕКОЛОГО-РЕСУРСНОГО ВІДНОВЛЕННЯ ДОНБАСУ

Друга міжнародна

науково-практична конференція

«Сучасні тенденції розвитку інформаційних систем і телекомунікаційних технологій»

19 грудня 2019 р.

Київ НУХТ 2019

УДК 004:621.39

Наукові праці Другої міжнар. наук.-практ. конф. «Сучасні тенденції розвитку інформаційних систем і телекомунікаційних технологій», 19 грудня 2019 р. (Київ, Україна). – К. : НУХТ, 2019. – 332 с.

У матеріалах конференції наведено доповіді за напрямами:

- світові тенденції в розробленні інформаційних систем і телекомунікаційних технологій;
- міжнародні стандарти у галузі інформаційних і телекомунікаційних технологій та кіберзахисту;
- розвиток освіти і науки в галузі інформаційних і телекомунікаційних технологій та кіберзахисту;
- інтернет речей та розвиток його технологій для безпечного суспільства;
- моделювання та симуляція стихійних лих, надзвичайних ситуацій і реагування на них;
- досвід використання інформаційних технологій, безпілотних літальних апаратів і роботів для моніторингу навколишнього середовища, попередження й ліквідації надзвичайних ситуацій природного і техногенного походження;
- неурядові та громадські організації у сфері цивільного захисту.

Матеріали конференції будуть корисні науковим та інженерно-технічним працівникам, студентам ВЗО та всім, хто цікавиться сучасними інформаційними системами та телекомунікаційними технологіями.

Подано в авторській редакції.

ISBN 978-83-956296-0-0

УДК 004.4

АНАЛІЗ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ ЗА ДОПОМОГОЮ МЕТОДУ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

Олексюк І. О.
Національний університет харчових технологій, Київ, Україна
E-mail: ilya.oleksiuk@gmail.com

Information System Security Analysis Using Penetration Testing Method

Information is one of the most important organization assets. For an organization, information is valuable and should be appropriately protected. Security is to combine systems, operations and internal controls to ensure integrity and confidentiality of data and operation procedures in an organization.Penetration testing, also called pen testing or ethical hacking, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit. Penetration testing can be automated with software applications or performed manually. The primary goal of a pen test is to identify weak spots in an organization's security posture, as well as measure the compliance of its security policy, test the staff's awareness of security issues and determine whether — and how — the organization would be subject to security disasters.

Тест на проникнення — метод оцінювання захищеності комп'ютерної системи чи мережі шляхом часткового моделювання дій зовнішніх зловмисників з проникнення у неї (які не мають авторизованих засобів доступу до системи) і внутрішніх зловмисників (які мають певний рівень санкціонованого доступу). Цей процес включає активний аналіз системи з виявлення будь-якої потенційної вразливості, що може виникати внаслідок неправильної конфігурації системи, відомих і невідомих дефектів апаратних засобів та програмного забезпечення, чи оперативне відставання в процедурних чи технічних контрзаходах. Цей аналіз проводиться з позиції потенційного нападника і може включати активне використання вразливостей.
Проблеми безпеки, що були виявлені в ході тесту на проникнення, представляються власнику системи. Ефективний тест на проникнення поєднає цю інформацію з точною оцінкою потенційного впливу на організацію і окреслити межі технічних і процедурних контрзаходів для зменшення ризиків.

Типи тестів на проникнення:

- **Соціальна інженерія** — Тестування з підключенням «людського контингенту», здатність чітко виявляти і отримувати конфіденційні дані та іншу інформацію через Інтернет чи телефон (до цієї групи можуть відноситися співробітники організації чи будь-які інші уповноважені особи, які присутні в мережі організації);
- **Веб-додаток** (Web Pentesting) — Використовується для виявлення вразливості в безпеці та інших проблем в декількох варіантах веб-додатків і сервісів, які розміщені на боці клієнта чи сервера;
- **Мережева служба.** (Network Pentesting) — Тестування проникнення в

мережу для виявлення можливості доступу зловмисників чи інших неавторизованих об’єктів;

- **Клієнтська частина —** Тест використовується для тестування додатків, встановлених на клієнтському сайті / додатку;
- **Віддалене підключення** — Тестування vpn чи аналогічного об’єкта, який може забезпечити доступ до підключеної системи;
- **Бездротові мережі** — Тест призначений для бездротових додатків і сервісів, включаючи їх різні компоненти та функції (маршрутизатори, фільтраційні пакети, шифрування, дешифрування і т. д.);
- **Тестування Системи автоматичного контролю та збору інформації** (SCADA Pentesting).

Процес тестування на проникнення можна розділити на 7 етапів:

1. Етап попередніх заходів. Обговорюється об’єм робіт та отримується дозвіл на їх проведення.
2. Розвідка. Відбувається збір усієї можливої інформації про цільову систему (ip адреси серверів, версії програмного забезпечення, відкриті порти і тд.)
3. Моделювання загрози та ідентифікація вразливих місць. Після успішної розвідки, даних має бути достатньо для моделювання загроз та розуміння векторів атаки на цільову систему.
4. Експлуатація вразливості системи.
5. Фаза після експлуатації. На цьому етапі доступ до системи отримано та потрібно повернути її початкового стану.
6. Написання звітності. Необхідно перерахувати знайдені вразливості, описати кроки для відтворення, класифікувати за рівнема ризику а також дати рекомендації щодо усунення
7. Усунення вразливості та повторне тестування

Рейтинг OWASP (The Open Web Application Security Project) TOP 10 описує найкритичніші веб інформаційних систем, а саме:

- **Ін’єкції (Injections**). Вразливості пов’язані, наприклад, з впровадженням SQL, NoSQL, OS і LDAP, виникають, коли неперевірені дані відправляються інтерпретатора в складі команди або запиту. Шкідливі дані можуть змусити інтерпретатор виконати непередбачені команди або звернутися до даних без проходження відповідної авторизації.
- **Недоліки аутентифікації**. Функції додатків, пов’язані з аутентифікацією і управлінням сесіями, часто некоректно реалізуються, дозволяючи зловмисникам скомпрометувати паролі, ключі або сесійні токени, а також експлуатувати інші помилки реалізації для тимчасового або постійного перехоплення облікових записів користувачів.
- **Розголошення конфіденційних даних.** Багато веб-додатки та API мають поганий захист критичних фінансових, медичних або персональних даних. Зловмисники можуть викрасти або змінити ці дані, а потім здійснити шахрайські дії з кредитними картами або

персональними даними. Конфіденційні дані вимагають додаткових заходів захисту, наприклад їх шифрування при зберіганні або передачі, а також спеціальних запобіжних заходів при роботі з браузером.

- **Зовнішні XML (XXE).** Старі або погано налаштовані XML-процесори обробляють посилання на зовнішні суті всередині документів. Ці сутності можуть бути використані для доступу до внутрішнім файлів через обробники URI файлів, загальні папки, сканування портів, віддалене виконання коду і відмову в обслуговуванні.
- **Недоліки контролю доступу.** Дії, дозволені аутентифицироваться користувачам, часто некоректно контролюються. Зловмисники можуть скористатися цими недоліками і отримати несанкціонований доступ до облікових записів інших користувачів або конфіденційної інформації, а також змінити призначені для користувача дані або права доступу.
- **Некоректна налаштування параметрів безпеки.** Некоректне налаштування безпеки є поширеною помилкою. Це відбувається через використання стандартних параметрів безпеки, неповної або специфічною настройки, відкритого хмарного зберігання, некоректних HTTP-заголовків і докладних повідомлень про помилки, що містять критичні дані. Всі ОС, фреймворки, бібліотеки і додатки повинні бути не тільки налаштовані належним чином, а й своєчасно коректуватися і оновлюватися.
- **Міжсайтове виконання сценаріїв (XSS).**XSS має місце, коли додаток додає неперевірені дані на нову веб-сторінку без їх відповідної перевірки або перетворення, або коли оновлює відкриту сторінку через API браузера, використовуючи надані вам дані, що містять HTML- або JavaScript-код. За допомогою XSS зловмисники можуть виконувати сценарії в браузері жертви, що дозволяють їм перехоплювати призначені для користувача сесії, підміняти сторінки сайту або перенаправляти користувачів на шкідливі сайти.
- **Небезпечна десеріалізація.** Небезпечна десеріалізація часто призводить до віддаленого виконання коду. Помилки десеріалізації, що не приводять до віддаленого виконання коду, можуть бути використані для атак з повторним відтворенням, впровадженням і підвищенням привілеїв.
- **Використання компонентів з відомими вразливостями.** Компоненти, такі як бібліотеки, фреймворки і програмні модулі, запускаються з привілеями програми. Експлуатація уразливого компонента може призвести до втрати даних або перехоплення контролю над сервером. Використання додатками і API компонентів з відомими уразливими може отримати несанкціонований додатки і призвести до серйозних наслідків.
- **Недоліки журналирования і моніторингу.** Недоліки журналирования і моніторингу, а також відсутність або неефективне використання системи реагування на інциденти, дозволяє зловмисникам розвинути атаку, приховати свою присутність і

проникнути в інші системи, а також змінити, витягти або знищити дані. Проникнення в систему зазвичай виявляють тільки через 200 днів і, як правило, сторонні дослідники, а не в рамках внутрішніх перевірок або моніторингу.

Penetration Testing — дозволена імітаційна кібератака на комп'ютерну систему, яка виконується для оцінки безпеки. Таке тестування є ефективним, тому має бути присутнім в циклі розробки програмного забезпечення.

Література

1. Топ-10 OWASP-2017. 10 найбільш критичних загроз безпеки веб-додатків. – 2017. – URL : https://www.owasp.org/images/9/96/OWASP_Top_10-2017-ru.pdf.
2. Pentest (penetration testing) [Електрон. ресурс] // SearchSecurity. – 2018. – URL : https://searchsecurity.techtarget.com/definition/penetration-testing.