УДК 004.77 (045)

А. О. Блоха

МОДУЛЬ ДЛЯ МОДЕЛЮВАННЯ АТАК

Вінницький національний технічний університет

Анотація

В цій доповіді проведено ознайомлення з відомими методами атак, їх векторів направленості. Налаштування та проведення деяких атак, що були створені власними силами, та атак, що проводяться за допомогою програмного забезпечення.

Ключові слова: атака, кібербезпека, проведення атак, Nmap, WireShark.

Abstract

In this report, familiarization with well-known methods of attacks and their directionality vectors was carried out. Setting up and running some homegrown and software-based attacks.

Keywords: *attack, cyber security, conducting attacks, Nmap, WireShark.*

Вступ

У світі швидкого технологічного розвитку зростає потреба у захисті комп'ютерних систем від різних видів кібератак. З кожним роком злочинні елементи знаходять нові способи, якими можуть завдати шкоди електронним пристроям та інформаційним системам, що утримують важливу інформацію. Щоб відстояти вірогідність таких атак, необхідно розробляти та вдосконалювати методи захисту і тестування комп'ютерних систем. Один із способів тестування імітує кібератаки на власній системі.

Метою роботи є ознайомитись з існуючими атаками та з принципами створення та проведення атак на інформаційно-комунікаційну систему.

Результати дослідження

Тема атак на інформаційно-комунікаційну систему (ІКС) включає в себе розгляд різних типів атак, їх принципів, методів та наслідків. Атаки на ІКС можуть бути спрямовані на отримання несанкціонованого доступу до конфіденційної інформації, порушення нормального функціонування системи або зловживання правами доступу[1].

Основні типи атак на ІКС включають:

– Соціальний інжиніринг: це метод маніпуляції людьми з метою отримання невідповідної інформації або зловживання їх довір'ям. Приклади включають фішинг, вимагання паролів, використання соціальних схем та імітацію авторитетних осіб.

– Шкідливе програмне забезпечення: це шкідливі програми, розроблені з метою завдати шкоди комп'ютерним системам. Шкідливе програмне забезпечення можуть включати в себе віруси, черв'яки, троянські програми, шпигунське програмне забезпечення та інші типи шкідливого коду.

– Атаки на мережу: такі атаки спрямовані на порушення мережевої інфраструктури або перехоплення комунікації. Приклади включають DoS (забій служби), DDoS (розподілене забій служби), MITM (перехоплення посередником) та атаки на бездротові мережі [2].

– Витік інформації: ці атаки спрямовані на незаконне отримання чутливої інформації. Це може включати витоки даних, порушення безпеки баз даних, крадіжку ідентифікаторів та інші методи отримання невідповідної інформації [3].

Принципи створення та проведення атак на ІКС можуть варіюватись в залежності від типу атаки, мети та цільової системи. Однак, деякі загальні принципи включають:

– Розвідка: перед проведенням атаки зловмисник зазвичай здійснює докладне дослідження цільової системи або організації. Це може включати збір інформації про інфраструктуру, вразливості, слабкі місця та цільові особи.

– Використання вразливостей: зловмисник шукає і використовує вразливості в програмному забезпеченні або конфігурації системи для отримання несанкціонованого доступу.

– Ескалація привілеїв: після отримання початкового доступу зловмисник може використовувати

додаткові методи, щоб отримати більше привілеїв або розширити свої можливості в системі [4].

– Збереження доступу: після успішної атаки зловмисник зазвичай намагається зберегти доступ до системи або створити засіб для подальшого вторгнення.

Атаки на ІКС можуть мати серйозні наслідки, такі як втрата конфіденційної інформації, порушення приватності, пошкодження репутації, фінансові втрати або навіть вплив на критичну інфраструктуру. Тому захист інформаційних систем від атак є критично важливим завданням, і він включає в себе застосування заходів безпеки, моніторинг, виявлення та відповідь на інциденти.

Завдання на побудову модуля генерації атак полягає в такому.

Аналізі вимог: визначити потреби та вимоги до модуля моделювання атак, включаючи підтримку різних типів атак, гнучкість в налаштуванні параметрів атак, збереження та аналіз результатів.

Розробка атак: розробити бібліотеку атак, яка включатиме різні типи атак, такі як соціальний інжиніринг, використання шкідливого програмного забезпечення, атаки на мережу, витік інформації, тощо. Кожна атака повинна мати налаштовуванні параметри для різних сценаріїв та рівнів складності.

Інтеграція з кіберполігоном: створення механізмів взаємодії, які дозволяють запускати атаки та отримувати результати.

Конфігурація атак: вибір типу атаки, налаштування параметрів, обрання цільової системи або мережі, імітацію реальних вразливостей та дій зловмисників.

Виконанні моделювання: реалізувати процес моделювання атак, який дозволяє запускати атаки на інформаційно-комунікаційну систему, відслідковувати прогрес та результати атаки, а також зберігати дані для подальшого аналізу.

Висновки

В ході дослідження було встановлено, що проведення різних видів атак мають різні цілі, що дозволять дослідити існуючі вразливості при побудові інформаційно-комунікаційної системи. Завдяки цій роботі було досліджено декілька моделей атак та вектори їх направленості. Було визначено, що основними цілями для атак є персональна інформація, інформація про структуру мережі та отримання несанкціонованого доступу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. 10 поширенних типів кібератак. Електронній ресурс [URL]. — https://thekernel.ua/10-poshyrenykh-typiv-kiberatak/.

2. DDoS Attacks: Understanding, Effects, and Protection. Електронній ресурс [URL]. — https://solutions-cloud.net/cybersecurity/ddos-attacks-understanding-effects-and-protection/?gclid=Cj0KCQjwjryjBhD0ARIsAMLvnF-_KJH_kKx0obljHSOmSlgbcsJPkWcRCt2J1j3mOZ2OKX4hJ-Ff6saAuI2EALw_wcB

3. Витік інформації. Електронній ресурс [URL]. — https://ukr.detective-ua.com/vitik-inform/3. Metasploit: The Penetration Tester's Guide.

4. Privilege escalation. Електронній ресурс [URL]. — https://www.ibm.com/docs/en/aix/7.1?topic=database-privilege-escalation

Блоха Андріан Олександрович — студент групи 1БС-21МС, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: EnixSquad10@gmail.com

Войтович Олеся Петрівна — кандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет

Andrian Oleksandrovych Blokha — *student of group 1BS-21MS, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: EnixSquad10@gmail.com*

Voytovych Olesya Petrivna — Candidate of Technical Sciences, Associate Professor of the Department of Information Protection, Vinnytsia National Technical University