Петляк Н.С., асистент
Хмельницький національний університет

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ІМІТАЦІЇ АТАК МЕТОЮ АНАЛІЗУ ТРАФІКУ

Імітація атак та аналіз мережевого трафіку є елементами забезпечення кібербезпеки, які дозволяють виявляти вразливості, тестувати достовірність систем захисту та покращувати стійкість інфраструктури до реальних загроз. Проведення тестування та імітація атак сприяють виявленню слабких місць у мережевих і веб-системах, вдосконаленню політик безпеки та підготовці персоналу до реагування на кібератаки. Усе це дозволяє підвищити рівень захисту інформаційно-комп'ютерних систем та мінімізувати ризики несанкціонованого доступу (НСД), витоку даних і фінансових втрат.

Аналіз та розвідка мережі спрямовані на збір інформації про відкриті порти, запущені служби та операційні системи, що дозволяє зловмиснику визначити потенційні цілі для подальших атак. Для реалізації таких атак використовуються Nmap, Masscan, Angry IP Scanner. Nmap дозволяє виконувати активне сканування мережі, визначати відкриті порти та запущені служби, тоді як Masscan відрізняється високою швидкістю сканування. Для тестування систем виявлення атак можна налаштувати розширене сканування з використанням різних режимів, наприклад, TCP SYN-сканування або сканування без встановлення з'єднання.

Атаки на автентифікацію та паролі базуються на методах підбору паролів, використанні словників або викраденні хешів з метою отримання НСД. Якщо така атака вдається, то зловмисник може заволодіти обліковими записами користувачів чи адміністраторів, що відкриває йому шлях до управління системою або мережею. Використовуються інструменти Hydra, Medusa, John the Ripper, Hashcat та Mimikatz. Hydra та Medusa дозволяють здійснювати перебір паролів у режимі brute-force або словникової атаки для мережевих сервісів, таких як SSH, FTP та RDP. Для тестування можна використовувати реальні або синтетичні паролі, а також обмежувати частоту запитів, щоб оцінити достовірність системи захисту.

Виявлення вразливостей та їх експлуатація передбачає пошук вразливих місць у програмному забезпеченні (ПЗ) та використання спеціальних скриптів або експлойтів для їх використання. Це може призвести до виконання довільного коду на сервері, отримання привілейованого доступу або крадіжки конфіденційних даних. Основними інструментами є Metasploit, SQLmap, Nikto, OpenVAS та Burp Suite. Metasploit надає широкий вибір експлойтів для тестування мережевих систем, а SQLmap автоматично знаходить SQL-ін'єкції у веб-додатках. Для тестування можна використовувати симуляцію реальних атак на вразливі сервери у контрольованому середовищі.

Атаки типу "людина посередині" базуються на перехопленні трафіку між двома сторонами, що дозволяє зловмиснику змінювати або перенаправляти дані без відома жертв. Основні інструменти для реалізації цих атак – Ettercap, Bettercap, MITMf та Wireshark. Ettercap дозволяє виконувати отруєння ARP-кешу для перехоплення трафіку, а Bettercap підтримує інтеграцію з атаками на HTTPS-з'єднання. Для тестування можна використовувати емуляцію підміни DNS-запитів або перехоплення HTTP-трафіку.

DoS- та DDoS-атаки спрямовані на перевантаження сервера або мережевого пристрою великою кількістю запитів, що призводить до його недоступності для легітимних користувачів. Використовуються LOIC, HOIC, Slowloris, Hping3 та UFONet. Slowloris атакує сервер шляхом підтримки великої кількості відкритих підключень, а Hping3 дозволяє генерувати спеціалізовані пакети для перевантаження мережевої інфраструктури. Для тестування можна використовувати контрольовані атаки на тестові сервери з обмеженою частотою запитів.

Атаки на веб-додатки використовують методи SQL-ін'єкцій, XSS та CSRF для отримання контролю над веб-сайтами або даними їхніх користувачів. Найпоширенішими інструментами є Burp Suite, OWASP ZAP, SQLmap та BeEF. OWASP ZAP дозволяє автоматично знаходити вразливості у веб-додатках, а BeEF спеціалізується на XSS-атаках. Для тестування варто використовувати середовища, такі як DVWA або OWASP Mutillidae, що містять вразливі веб-додатки.

Однак, більшість програм поширюються під відкритими ліцензіями, такими як GPL, MIT або Apache, що дозволяє їх використання у навчальних цілях, дослідженнях та тестуванні безпеки за умови отримання дозволу власника мережі. Наприклад, Nmap, Wireshark, Metasploit та Aircrack-ng мають ліцензію GPL, яка передбачає можливість використання для освітніх і наукових досліджень, тоді як Burp Suite Community Edition має обмежений функціонал і доступний лише для некомерційного використання. Важливо дотримуватися законодавчих норм, оскільки несанкціоноване тестування або втручання в роботу комп'ютерних мереж може суперечити нормативно-правовим актам, що передбачають відповідальність за подібні дії.

Список використаних джерел:

1. NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment. National Institute of Standards and Technology (NIST). URL: https://csrc.nist.gov/publications/detail/sp/800-115/final (дата звернення: 11.03.2025).