УДК 510.635:004.891(045)

А.І. Вавіленкова, д.т.н.
Національна академія Служби безпеки України, Київ

МОНІТОРИНГ МЕРЕЖ З МЕТОЮ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ

Сьогодні для організації захисту комп'ютерних мереж від кіберзагроз здійснюється багато превентивних заходів, серед яких постійний моніторинг мережі та сканування портів [1]. Одним із програмних засобів, що дозволяє здійснювати тестування на проникнення – Kali Linux.

Обмін даними в мережі відбувається між двома процесами за певним протоколом. Для встановлення зв'язку потрібні: номер протоколу; дві IP-адреси (адреса хоста-відправника та адреса хоста-одержувача) для побудови маршруту між ними; два номери портів (порт процесу –відправника та порт отримувача).

В комп'ютерних мережах порт є кінцевою точкою зв'язку в операційній системі. В програмному забезпеченні це логічна конструкція, яка ідентифікує конкретний процес або вид послуг [2].

Мережевий протокол задає загальні правила взаємодії різноманітних програм, мережевих вузлів чи систем і створює таким чином єдиний простір передачі. Для того, щоб прийняти і обробити відповідним чином повідомлення, їм необхідно знати, як сформовані повідомлення і що вони означають. Прикладами використання різних форматів повідомлень в різних протоколах можуть бути встановлення з'єднання з віддаленою машиною, відправлення повідомлень електронною поштою, передача файлів.

Коли клієнт і сервер починають використовувати TCP, створюється віртуальний канал. Дані по цьому каналу можуть одночасно передаватися в обох напрямках. Один прикладний процес пише дані в TCP-порт, вони проходять по мережі, а інших прикладний процес читає їх зі свого TCP-порту. Для того, щоб клієнт міг звертатися до необхідного йому серверу, він повинен знати номер порту, за яким сервер очікує звернення до нього .

Nmap («Network Mapper») – це утиліта з відкритим вихідним кодом для дослідження мережі та перевірки безпеки, розроблена для швидкого сканування великих мереж.

Вихідні дані ***Nmap*** – це список просканованих цілей з додатковою інформацією щодо кожної з них залежно від заданих опцій. Ключовою інформацією є «таблиця важливих портів» [3].

Найпоширеніші дії, що можна здійснити за допомогою утиліти ***Nmap***:

- здійснити сканування визначених IP-адрес: **nmap 172.27.157.151**;
- здійснити сканування цілей, список яких знаходиться у файлі *.txt, наприклад, **nmap –iL targets.txt;**
- реалізувати метод сканування TCP портів, якщо порт відкритий і прослуховується, то результат виконання буде успішним, тобто з'єднання буде встановлене, у протилежному випадку вказаний порт є закритим або доступ до нього заблоковано засобами захисту, виконується за допомогою ключа **nmap –sT 192.168.1.17;**
- реалізувати метод напіввідкритого сканування, оскільки повне TCP-з'єднання з портом сканування не встановлюється **nmap –sS 192.168.1.2;**
- реалізувати Ping-сканування для отримання інформації про активні хости в сканованій мережі **nmap –sn 192.168.1.17;**
- визначити операційну систему віддаленого хосту **nmap –O 192.168.1.17.**

У доповнення до таблиці важливих портів ***Nmap*** може надавати подальшу інформацію про цілі: перетворені DNS імена, припущення про операційну систему, типи пристроїв і MAC адреси.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Юхименко П. Глобалізація та політика національної безпеки. – підручник. – 2021. – 402 с.

2. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок, Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с.

3. Вавіленкова А.І., Душкевич В.С., Лозниця Р.А. Види налаштувань безпеки комп'ютера: Proceedings of the V International Scientific and Practical Conference «Formation of perceptions of the structure of scientific methodology», 30-31 січня, 2023, – Відень, Австрія: InterSci. – 2023. – С. 47–50.