Савчук А. В., магістрант гр. КБм-21-1,
Єфіменко А. А., канд. техн. наук, доцент, зав. кафедри КІ та КБ,
Вакалюк Т. А., д-р пед. наук, професор, професор кафедри ІПЗ
Державний університет «Житомирська політехніка»

РІЗНОВИДИ АТАК НА МЕРЕЖУ ТА СПОСОБИ ЗАХИСТУ

Розвиток технологій не стоїть на місці і стрімко йде вгору. Не кожна людина в даний період розвитку встигає дізнатися та ознайомитись з інформацією про власну безпеку в мережі. Проте зловмисники не стоять на місці, а також вигадують, знаходять помилки в обладнаннях чи коді, і користуються цим в своїх цілях. На сьогоднішній день існує дуже багато різних атак, які здійснюють хакери для того, щоб дізнатися ту чи іншу інформацію, зламати сайти, заволодіти мережею тощо. Для того, щоб захиститися від різних типів атак, потрібно знати, як вони працюють. На великих підприємствах захистом мережі займаються адміністратори. Розглянемо детально деякі типи атак, щоб знати, як правильно і надійно від них захищатися.

Rogue DHCP Server – це атака, що спрямована на DHCP сервера. Порушник вичерпує всі адреси, що пропонує справжній сервер, а далі видає себе за сервер і пропонує IP-адреси та інші мережеві налаштування всім іншим користувачам у мережі. Тобто зловмисник впроваджує в мережі свій зловмисний сервер [1]. Цей сервер має змогу відповідати на запити клієнтів на виявлення DHCP.

У випадку, коли користувач отримує дані зловмисного сервера, це може порушити доступ до мережі, спричиняючи DoS. У результаті, зловмисник отримує весь трафік від клієнта і перенаправляє на шлюз по замовчування. Такі атаки залишаються впродовж довгого часу непомітними, тому що клієнт вважає, що все працює правильно. Зловмисник за допомогою даних маніпуляцій намагається отримати дані користувачів мережі.

DHCP starvation – це атака, за допомогою якої порушники посилають багато підроблених пакетів DISCOVER, доки DHCP сервер не втратить всі IP-адреси. Тобто, якщо клієнт захоче отримати IP-адресу, в нього нічого не вийде, так як буде відмовлено в доступі. Крім того, порушник може створити свій DHCP сервер для того, щоб надавати свої IP-адреси для перехоплення трафіку клієнта. Для того, щоб перехопити всі IP-адреси, порушник надсилає сотні пакетів DHCP DISCOVER, використовуючи підроблені MAC-адреси [2].

MAC-spoofing – це атака, при якій порушник обходить перевірку аутентифікації для порушення працездатності мережі. Використовується для того, щоб дізнатися про дані, програми, паролі та IP-адреси кінцевого хоста [3].

ARP Spoofing – це атака, при якій зловмисник надсилає підроблені ARP пакети через локальну мережу для того, щоб зв'язати свою MAC адресу з IP-адресою справжнього користувача мережі. Коли зв'язок налаштовується, зловмисник починає отримувати, а також модифікувати передачу даних. ARP атаки відбуються лише в локальних мережах [3].

DOS – це атака, за допомогою якої злочинець намагається зробити цільовий пристрій недоступним для користувачів, перезавантажуючи або заповнюючи пристрій запитами, поки неможливо буде обробити звичайний трафік, що призводить до відмови в обслуговуванні інших користувачів. Основною різницею DOS і DDOS атаки є те, що перша виконується з використанням одного комп'ютера, а друга – із залученням великої кількості робочих станцій [4]. Отже, як бачимо, в сучасному світі існує багато атак на робочі станції, пристрої та на мережі, які тим чи іншим чином впливають на її працездатність.

Тобто для того, щоб налагодити робочу мережу та налаштувати її працездатність, потрібно її захищати від порушників, які будуть намагатися заволодіти інформацією. Із розвитком атак розвивався і захист мереж. Більшість атак, які здійснювали порушники, мали пагубний характер, так як могли виводити мережі з ладу на достатньо довгий термін, несанкціоноване заволодіння приватною інформацію тощо.

На великих підприємствах на даний час досить розвинена система захисту. Майже всі атаки відбиваються і не мають великого впливу на мережі. Проте кожний день зловмисники розвивають свої способи атаки і тому потрібно також розробляти нові методи захисту від них. Розглянемо способи захисту від атак, які були розглянуті вище.

Rogue DHCP Server – простим та ефективним способом захисту є вмикання DHCP snooping на комутаторах. Існує 2 типи портів: довірений (до якого підключається DHCP сервер) та недовірений (порти для всіх інших підключень, за якими DHCP сервера не може бути і за яким може бути зловмисник, який намагається атакувати даний сервер) [5].

Налаштування DHCP snooping необхідно, щоб показати, що пакети DHCP offer та acknowledgment повинні проходити через довірений порт (trusted), і не допускати проходження даних пакетів через недостовірні (untrusted) порти. Після налаштування запити від справжніх клієнтів будуть перенаправлятися на довірені порти.

DHCP starvation: кращим способом захисту від даної атаки буде обмеження кількості доступних IP адрес, що може дати DHCP сервер. Також необхідно налаштувати збереження в комутаторі MAC адреси в конфігураційному файлі. Це необхідно для того, щоб DHCP сервер міг видавати користувачу мережі IP адресу, прив'язану до MAC адреси користувача. Якщо це мережа чи підмережа якогось підприємства, до якого не мають доступу інші користувачі, то необхідно налаштувати кількість безпечних MAC адрес, налаштувати кількість DHCP пакетів на порт, і в випадку їх перевищення автоматично виключати його на деякий час [5].

MAC-spoofing: кращим захистом від даної атаки є запис в таблицю комутатора MAC адресу користувача, який підключений за даним портом. Тобто, якщо MAC адреса за даним портом зміниться, то користувач буде недоступний.

ARP Spoofing: у випадку цієї атаки потрібно використовувати інструмент Dynamic ARP Inspection. Суть його роботи полягає в тому, що він вибирає, які пакети пропускати, а які відкинути, тобто повністю захищає мережу від атаки.

DOS: від даної атаки існує ряд захистів. Можна налаштовувати комутатори так, щоб вони визначали тип невідомого трафіку і не пропускали його. Також можна обмежити пропускну швидкість до сервера. Також можна виділити сервер, який зможе обробляти інформацію і буде працювати.

Отже, як можна побачити, що як розвиваються атаки, так розвивається і захист. В наш час будь-яка мережа повинна бути захищена, щоб працювати.

Список використаних джерел

1. Rogue DHCP Server Attack [Електронний ресурс] - Rogue DHCP Server Attack | Rogue DHCP | Info-savvy.com
2. What is a DHCP Starvation Attack? [Електронний ресурс] - What is a DHCP Starvation Attack? | CBT Nuggets
3. MAC Spoofing Attack: All You Need to Know in 6 Important points [Електронний ресурс] - MAC Spoofing Attack: All You Need to Know in 6 Important points (jigsawacademy.com)
4. What is a denial of service attack [Електронний ресурс] - What is a denial of service attack (DoS) ? - Palo Alto Networks
5. Защищаем сеть L2 комутаторами [Електронний ресурс] - Защищаем сеть L2 коммутаторами / Хабр (habr.com)