ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ДАННЫХ НА КАНАЛЬНОМ УРОВНЕ НА ОСНОВЕ ОБОРУДОВАНИЯ HUAWEI

А.К. Матюшенко, П.А. Снигирь

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Среди техник MITRE ATT&CK, использующих уязвимости канального уровня, известна такая техника, как Adversary in the Middle Attack (AiTM) с идентификатором T1557 [1]. Используя данную технику, нарушитель может осуществлять прослушивание сети, манипуляции с передаваемыми данными или реализовывать другие кибератаки. В соответствии с субтехникой 1557.002 [2] нарушитель, используя протокол канального уровня ARP (Address Resolution Protocol), может осуществлять кибератаку типа ARP-spoofing (ARP Cache Poisoning), то есть отравлять кэш протокола, чтобы позиционировать себя между двумя или более сетевыми устройствами.

Основным методом предотвращения ARP-spoofing в сетях является настройка функции ARP Anti-spoofing на коммутаторах. Минимальные настройки безопасности включают в себя строгое распознавание ARP, фиксированный ARP для предотвращения изменения записей поддельными ARP-пакетами и настройку отбрасывания ARP-пакетов.

Для анализа уязвимостей ARP-протокола была создана локальная сеть в виртуальной лаборатории PNETLab, которая предоставляет возможность моделирования локальных сетей на базе устройств различных производителей в режиме реального времени. Элементами созданной модели локальной сети являются:

– маршрутизатор Huawei серии NE40E;

– коммутатор Huawei серии CE6800;

– компьютер нарушителя с ОС Linux;

– компьютер пользователя с ОС Linux.

Для обеспечения безопасности от кибератак на канальном уровне предлагается настроить коммутатор, используя следующие команды [3]:

1. Настройка строгого распознавания ARP (команда arp learning strict).

2. Настройка фиксированного ARP (команда arp anti-attack entry-check fixed-mac enable).

3. Настройка безвозмездного отбрасывания ARP-пакетов (команда arp anti-attack gratuitous-arp drop).

В дальнейшем в смоделированной локальной сети в виртуальной лаборатории PNETLab планируется реализовать кибератаки на канальном уровне с целью тестирования правильности работы функции ARP Anti-Spoofing коммутатора Huawei серии CE6800.

Список литературы

1. Adversary-in-the-Middle [Электронный ресурс]. Режим доступа: https://attack.mitre.org/techniques/T1557/. – Дата доступа: 06.05.2024.

2. Adversary-in-the-Middle: ARP Cache Poisoning [Электронный ресурс]. Режим доступа: https://attack.mitre.org/techniques/T1557/002/. – Дата доступа: 06.05.2024.

3. Настройка безопасности ARP [Электронный ресурс]. Режим доступа: https://support.huawei.com/enterprise/ru/doc/EDOC1100112933/2fd242a8/configuring-arp-security-arp-anti-spoofing. – Дата доступа: 06.05.2024.