Глава 1

Атаки на сети уровня L2

1.1 ARP-Spoofing

ARP-spoofing [1] — разновидность сетевой атаки типа MITM, применяемая в сетях с использованием протокола ARP. В основном применяется в сетях Ethernet. Атака основана на недостатках протокола ARP.

Злоумышленник выбирает машину или машины жертвы Первым шагом в планировании и реализации атаки ARP Spoofing является выбор цели. Это может быть конкретная конечная точка в сети, группа конечных точек или сетевое устройство, такое как маршрутизатор. Маршрутизаторы являются привлекательными целями, поскольку успешное отравление ARP маршрутизатора может нарушить трафик для всей подсети. Злоумышленник запускает инструменты и начинает атаку Всем зло-

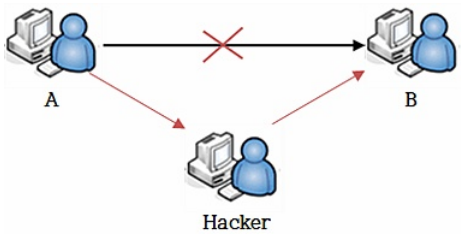

Рис. 1.1: MITM

умышленникам, желающим выполнить отравление ARP, легко доступен широкий спектр инструментов. После запуска выбранного инструмента и настройки соответствующих параметров злоумышленник начинает атаку. Он может незамедлительно начать рассылку сообщений ARP или дождаться получения запроса. Злоумышленник выполняет определенные действия с некорректно направленным трафиком После повреждения

кэша ARP на устройстве (устройствах) жертвы злоумышленник обычно выполняет какие-то действия с некорректно направленным трафиком. Он может просматривать или изменять его, либо создать «черную дыру», чтобы данные никогда не доходили до адресата. Выбор действий зависит от мотивов злоумышленника. Пример реализация ARP-спуфинга на Python:

```
import socket
import time

interface = "wlan0"  # Прослушиваемый сетевой интерфейс
mac = b"\xbb\xbb\xbb\xbb\xbb\xbb"  # Наш MAC-адрес, он же bb:bb:bb:bb:bb:bb

gateway_ip = socket.inet_aton("192.168.1.1")  # IP-адрес шлюза
gateway_mac = b"\xaa\xaa\xaa\xaa\xaa\xaa"  # MAC-адрес шлюза

victim_ip = socket.inet_aton("192.168.1.2")  # IP-адрес жертвы
victim_mac = b"\xcc\xcc\xcc\xcc\xcc\xcc"  # MAC-адрес жертвы

connect = socket.socket(socket.PF_PACKET, socket.SOCK_RAW, socket.htons(0x0800))
connect.bind((interface, socket.htons(0x0800)));
}
```

Список литературы

[1] Андрей Бирюков. *Информационная безопасность: защита и нападение*. Litres, 2022.