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-

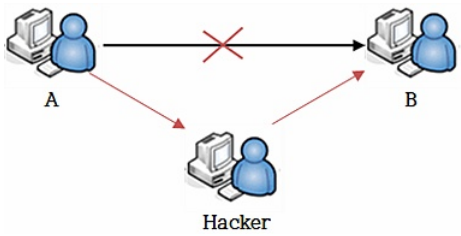

Рис. 1.1: MITM

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.

1.2 VLAN-hopping

VLAN-hopping [1] - эксплойт компьютерной безопасности, метод атаки сетевых ресурсов в виртуальной локальной сети. Основная концепция всех атак с переключением VLAN заключается в том, что атакующий хост в VLAN получает доступ к трафику в других VLAN, которые обычно недоступны. Существует два основных метода переключения VLAN: подмена коммутатора и двойная маркировка. Оба вектора атаки могут быть устранены при правильной конфигурации порта коммутатора. Ата-

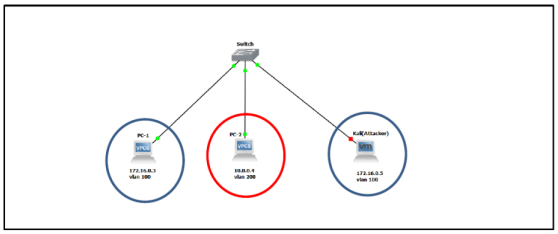

Рис. 1.2: VLAN-hopping

ка VLAN hopping может осуществляться следующим образом: если сетевой свитч установлен в режим авто-транка, злоумышленник меняет настройки так, что возникает «нужда» в постоянном канале связи (транке). То есть, на данном транковом порту становится разрешен доступ ко всем VLAN'ам.

Список литературы

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