

Основы администрирования сетевых устройств

Лекция 5 — Обеспечение
безопасности сетевых устройств

- Сетевой безопасностью называются действия, направленные на защиту работоспособности и целостности сети и данных.
- Важным фактором при первоначальном конфигурировании и администрировании сетевых устройств является обеспечение функции безопасности, включающих контроль доступа , конфиденциальность и сохранность данных пользователя;
- Раздел сетевой безопасности очень обширен, подготовка специалистов занимает много времени и требует большого количества ресурсов. В данной лекции рассмотрим базовые подходы к администрированию сетевых устройств с точки зрения безопасности.

- Говоря о сетевой безопасности часто используют модель КЦД (Конфиденциальность, Целостность, Доступность) по отношению к информации;
- Рассмотрим базовые способы и методы обеспечения безопасности сетевых устройств и информации передаваемой через такие устройства.

- В первую очередь стоит учитывать организацию доступа к устройствам. Устройства должны находиться в помещении в котором отсутствует физический доступ к устройству для третьих лиц, с этой проблемой сталкиваются т.е. устройства которые установлены непосредственно у абонента, в общественных местах и т.д.;
- Наиболее массовой проблемой безопасности является использование удаленного доступа, который открывает широкие возможности для злоумышленников.

При работе с сетевыми устройствами можно выделить основные методы защиты:

- Доступ по логину и паролю – тип контролируемого доступа, рекомендуется использовать сложные пароли не сохраняемые на бумажных или цифровых носителях (исключение – цифровая подпись);
- Ограничение доступа по IP или MAC адресу;
- Ограничение списка доступных сетевых портов;
- Отключение сетевых сервисов (ping, traceroute и т.п.);
- Шифрование конфигурационного файла;
- Динамический (fail2ban) и статический брандмауэр;
- Списки контроля доступа (ACL);
- Деление сети на сегменты и т.д.

- Надежный контроль доступа к устройству является одной из основных задач администрирования, однако этого недостаточно для обеспечения безопасности передаваемой информации;
- Существует множество сетевых атак, которые позволяют перехватить информации, скомпрометировать передачу или осуществить отказ в обслуживании.

- Для обеспечения наиболее полной картины безопасности сети необходимо представлять и понимать принципы работы всех используемых интерфейсов и протоколов, включая уязвимости среды передачи и характерные недостатки оборудования (т.н. Backdoors);
- Выявление уязвимости крупных сетей(устройств) это долгий и ресурсоемкий процесс, рассмотрим наиболее распространенную сетевую атаку и методы борьбы с ней.

- Злоумышленники часто применяют концепцию **MITM** (англ. Men In The Middle – «человек посередине») с применением атаки ARP-spoofing;
- В данном методе используется уязвимость протокола ARP, которая позволяет подменять MAC адреса в сети коммутации L2 модифицируя схему обмена информацией между передающей и приемной стороной.

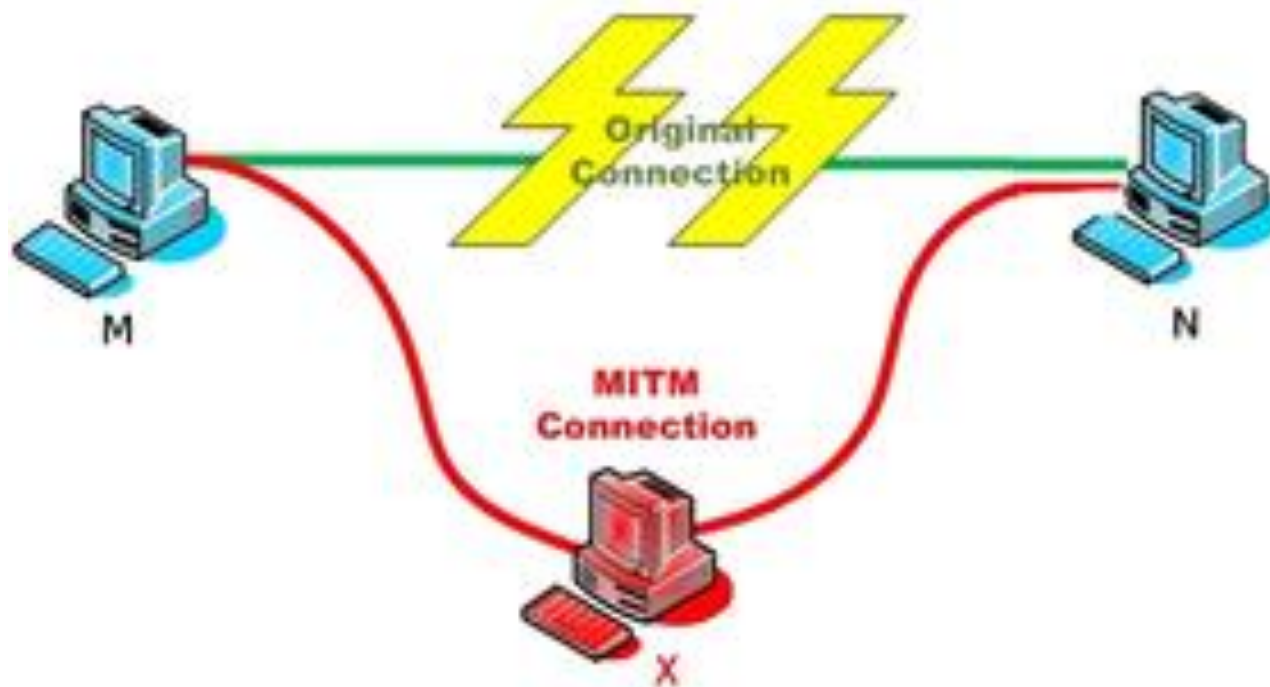


Рис. 1 Схема MITM соединения

- Злоумышленник подключается «в разрыв» соединения двух хостов, если включен форвардинг пакетов то хосты «жертвы» думают, что общаются напрямую;
- Это происходит за счет того, что злоумышленник постоянно генерирует поддельный ARP ответ содержащий не оригинальную связку IP-MAC. ПК жертвы обновляет ARP таблицу и за указанным IP отправляет пакеты на MAC адрес злоумышленника.

- Злоумышленник подключается «в разрыв» соединения двух хостов, если включен форвардинг пакетов то хосты «жертвы» думают, что общаются напрямую;
- Это происходит за счет того, что злоумышленник постоянно генерирует поддельный ARP ответ содержащий не оригинальную связку IP-MAC. ПК жертвы обновляет ARP таблицу и за указанным IP отправляет пакеты на MAC адрес злоумышленника. Уязвимость протокола заключается в том, что он принимает ответы ARP в любой момент времени.

Существует множество методов защиты:

- Закрыть все возможные пути подключения к локальной сети (в частности беспроводные сети должны быть защищены);
- Настроить статический тип записей для протокола ARP (по умолчанию записи динамические);
- Использовать механизмы защиты IpGuard и подобные.

- Среди общих рекомендаций также присутствуют вопросы использования шифрования как при организации доступа к устройству, так и при обмене данными по сети;
- Например, протоколы **HTTP** и **TELNET** не имеют шифрования, перехваченный пакет данных может быть прочитан и использован злоумышленником. Альтернативными являются протоколы **HTTPS** и **SSH** использующие шифрование устойчивое к взлому, в этом случае даже если пакет был перехвачен, на его расшифровку потребуется большое количество времени и вычислительных ресурсов;
- Также рекомендуется программно запрещать использование уязвимых протоколов пользователю.

- Среди общих рекомендаций также присутствуют вопросы использования шифрования как при организации доступа к устройству, так и при обмене данными по сети;
- Например, протоколы **HTTP** и **TELNET** не имеют шифрования, перехваченный пакет данных может быть прочитан и использован злоумышленником. Альтернативными являются протоколы **HTTPS** и **SSH** использующие шифрование устойчивое к взлому, в этом случае даже если пакет был перехвачен, на его расшифровку потребуется большое количество времени и вычислительных ресурсов;
- Также рекомендуется программно запрещать использование уязвимых протоколов пользователю.

К общим мерам обеспечения безопасности информации можно добавить:

- Использование антивирусного ПО;
- Применение политик доступа;
- Использование виртуальных туннелей с шифрованием (VPN);
- Защита электронной почты;
- Безопасность веб-ресурсов;
- Анализ поведения сетевого трафика;
- Защита программного обеспечения и т.д.

- Список литературы:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов 4-е изд. — СПб.: Питер, 2010. — 944 с.: ил

- **Материалы для самостоятельной подготовки:**

Тема	Источник
Фильтрация трафика	[1, с. 600-603]
Трансляция сетевого адреса	[1, с. 616-619]
Сетевая безопасность	[1, с. 828-847]
Сетевые экраны	[1, с. 875-882]
Протоколы защищенного канала. IpSec, VPN	[1, с. 887-903]

Спасибо за внимание!

Лекция 5 — «Обеспечение безопасности
сетевых устройств»

Версия документа 1.0

Стенин А.В.

av.stenin@yandex.ru