06.09.2025 Лекция 1. Классификация угроз безопасности в протоколах межсетевого взаимодействия

Существует множество видов классификации угроз безопасности, реализуемых с использованием протоколов межсетевого взаимодействия. Наиболее интересной представляется классификация по уровням стека протоколов TCP/IP, который включает канальный, сетевой, транспортный и прикладной уровни.



Стек протоколов TCP/IP

* Канальный уровень - подготавливает фреймы для передачи по локальной среде
* Сетевой уровень - производит маршрутизацию IP-пакетов для межсетевого взаимодействия
* Транспортный уровень - осуществляет сегментацию, передачу и сборку сегментов
* Прикладной уровень - обеспечивает работу сетевых приложений и их протоколов

Угрозы на канальном уровне

* Подслушивание – Сбор информации без ее подмены. Нарушает конфиденциальность.
* Перехват сообщений – Исходное сообщение подменяется другим. Нарушает конфиденциальность и целостность.
* Подмена хоста – Один хост выступает от имени другого. Нарушает конфиденциальность и целостность.
* Dos-атаки – “Отказ в обслуживании”, например, через широковещательный шторм. Нарушает доступность.

Угрозы на сетевом уровне

На сетевом уровне в стеке протоколов TCP/IP производится маршрутизация IP-пакетов, позволяющая осуществлять межсетевое взаимодействие независимо от физических, конструктивных и технологических особенностей различных технологий канального уровня.

Основные атаки:

* Подслушивание
* Перехват
* Подмена объекта
* Отказ в обслуживании
* Навязывание ложного маршрута
* Подмена IP-адреса

Транспортный уровень

На транспортном уровне производится сегментация, передача и сборка сегментов, содержащих информацию с прикладного уровня.

Передача может осуществляться:

- С установкой виртуального соединения (TCP)

- Без установления соединения (UDP)

Угрозы на транспортном уровне:

* SYN-flooding – скрытый отказ в обслуживании, вызванный штормом запросов на установление TCP-соединений.
* Пакеты с нестандартными атрибутами – Явный отказ в обслуживании: “Land”, “TearDrop”, “Bonk”, “Nuke”, “UDP-boomb”, “Ping Death”.
* Подмена доверенного объекта – Передача от имени доверенного объекта с присвоением его прав доступа.
* Сканирование портов – Сетевая разведка для определения открытых портов и функционирующих сетевых служб.

Прикладной уровень

На прикладном уровне работает большинство сетевых приложений, имеющих собственные протоколы обмена информацией:

* HTTP – для веб-браузеров
* FTP – для передачи файлов
* SMTP -для электронной почти
* SSH -для защищенного удаленного доступа
* DNS – для разрешения доменных имен
* И многое другое

Угрозы на прикладном уровне (часть 1)

Парольные атаки – направлены на конкретные приложения или учетные записи пользователя, реализуемые с использованием сетей.

Атаки на серверы – атаки на DHCP и DNS-серверы, нарушающие их нормальное функционирование

Уязвимости протоколов – атаки, использующие уязвимости протоколов прикладного уровня: FTP, HTTP, POP, Telnet и других

Угрозы на прикладном уровне (часть 2)

Вредоносные программы – атаки программно-математического воздействия с использованием вредоносных программ, распространяемых по сети:

* Сетевые и почтовые черви
* Файловые вирусы
* Троянские программы

Уязвимости ПО – Атаки, эксплуатирующие уязвимости системного и прикладного программного обеспечения

Не декларированные возможности – атаки, использующие не декларированные возможности системного и прикладного программного обеспечения.

Технологии Защиты канального уровня

VLAN и VPN: Основы Защиты

Технологии защиты канального уровня, такие как VLAN (виртуальная локальная сеть) и VPN (виртуальная частная сеть), играет ключевую роль в обеспечении безопасности данных. VPN может работать на разных уровнях стека TCP/IP, но особое внимание уделяется канальному уровню. VLAN же реализуется исключительно на втором уровне.

В данном обзоре мы рассмотрим протоколы VPN канального уровня и более подробно остановимся на технологии VLAN, которая позволяет создавать логически изолированные сети на одном физическом оборудовании.

VPN Канального уровня

Технология VPN на втором уровне модели OSI обеспечивает инкапсуляцию и шифрование трафика канального уровня, позволяя безопасно передавать данные по сетям общего пользования. Это предотвращает несанкционированные доступ третьих лиц к передаваемой информации.

К протоколам формирования защищенного канала на втором уровне обычно относят PPTP, L2TP. Однако эти технологии считаются морально устаревшими из-за уязвимостей в шифровании и архитектуре.

Устаревшие протоколы VPN

* PPTP (Point-to-Point Tunneling Protocol)
* Использует GRE и TCP-порт1723. Применяет MPPE с устаревшим алгоритмом RSA RC4. Имеет серьезные недостатки безопасности, не рекомендуется к использованию.
* L2TP (Layer-2 Tunneling Protocol)
* Преемник PPTP, инкапсулирует PPP внутри UDP на порт 1701. Для конфиденциальности и целостности данных зависит от IPsec. L2TP/IPsec добавляет ненужные уровни инкапсуляции и плохо работает за NAT.
* Современные операционные системы поддерживают IPsec VPN на основе IKEv2, что делает устаревшие протоколы неактуальными.

Для защиты канального уровня VPN тоже может активно использоваться, если не используются IP адреса.

Также существует защита канала передачи данных по WI-FI. Все устройства WI-FI поддерживают протоколы канального уровня для конфиденциальности и целостности. Изначально использовался протокол WEP (до 2004), потом WPA (после 2004), WPA3 (заменил PSK на PAKE, обеспечивает дополнительную защиту от слабых паролей и предлагает PFS).

MACSEC – защита Ethernet. Создает безопасное соединение точка – точка в сети, являясь аналогов WPA для WI-FI. Для обмена ключами аутентификации использует протокол MKA. Защищает IP-трафик, ARP, IPV6 и DHCP.