Домашнее задание к уроку №5 Сети, маршрутизация. Часть 2.

Группа: Cyb07-onl

Студент: Парфимович Алексей

1. Дополнить каждый уровень модели OSI примерами реализаций и атак.

Модель OSI сотоит из 7 уровней (Физический Канал Сети Транспортирует Сессии Представляя Приложения):

1. Physical Layer (Физический уровень) отвечает за передачу сырых битов по физической среде (кабель, радиоволны и т.д.). Определяет электрические, механические, процедурные и функциональные характеристики соединения.
Примеры реализации:
аппартная реализация Ethernet, USB, Bluetooth, Wifi, кабели, концентраторы (хабы).
Примеры атак:
a) Помехи и подавление сигнала (Jamming) - намеренное создание радиопомех в беспроводных сетях (Wi-Fi, Bluetooth, сотовая связь) с целью нарушения связи, DoS.
Защита: Использование защищённых частот, переключение каналов, обнаружение джеммеров.
b) Подмена оборудования (Hardware Tampering) - установка злоумышленного оборудования в сеть, например поддельного хаба, сплиттера или "жучка" для перехвата, модификация или блокировка трафика.
Защита: Контроль доступа к серверным и сетевым шкафам, инвентаризация оборудования.

2. Data Link Layer (Канальный уровень) обеспечивает надёжную передачу данных между двумя узлами в пределах одной сети. Осуществляет управление доступом к среде через MAC-адреса, обнаружение и исправление ошибок.
Примеры реализации:
программная реализация Ethernet, PPP, WiFi (IEEE 802.11), коммутаторы (switches).
Примеры атак:
a) MAC-флудинг (MAC Flooding) – отправка огромного количества кадров с поддельными MAC-адресами на коммутатор с целью переполнить таблицу MAC-адресов (CAM-таблицу) коммутатора. Коммутатор перестаёт "понимать", куда отправлять кадры, и начинает работать как хаб — рассылает весь трафик на все порты, что позволяет выполнить перехват трафика.
Защита: Port Security — ограничение количества MAC-адресов на порту, Блокировка неизвестных MAC-адресов, Использование управляемых коммутаторов с защитными функциями.
b) Атаки через VLAN Hopping что бы обойти изоляцию между VLAN и получить доступ к трафику другой VLAN, например:
Switch spoofing: Атакующий имитирует работу коммутатора и использует протокол DTP (Dynamic Trunking Protocol), чтобы установить trunk-соединение и получить доступ ко всем VLAN.
Double tagging: Отправка кадра с двумя VLAN-тегами (IEEE 802.1Q), чтобы обмануть коммутатор.
Защита: Отключить DTP на портах пользователей (switchport nonegotiate), Не использовать VLAN 1 для пользовательского трафика, явное назначать порты как access/trunk, добавить фильтрацию тегированных кадров на access-портах.

3. Network Layer (Сетевой уровень) отвечает за маршрутизацию данных между разными сетями. Определяет логические адреса (например, IP-адреса) и выбирает оптимальный путь доставки пакетов.
Примеры реализации:
протоколы IP (IPv4, IPv6), ICMP, маршрутизаторы (routers).
Примеры атак:
a) Атаки на маршрутизацию, например:
- Route Injection: объявление ложных маршрутов (например, через BGP), чтобы перенаправить трафик через свой узел для перехвата, анализа или блокировки трафика (например, между странами или провайдерами).
- BGP Hijacking: Подделка обновлений маршрутизации (через протоколы внутренней маршрутизации RIP, OSPF) для изменения топологии сети.
Защита: BGPsec, RPKI (Resource Public Key Infrastructure), мониторинг маршрутов. Аутентификация в OSPF (MD5/SHA), отключение RIP в пользу более безопасных протоколов.
b) Фрагментация и атаки на сборку пакетов, например Teardrop-атака - отправка перекрывающихся фрагментов IP-пакетов с некорректными смещениями, при этом старые ОС не могли корректно собрать такие пакеты что приводило к сбою ядра ОС.
Защита: Корректная реализация обработки фрагментов, фильтрация подозрительных пакетов.

4. Transport Layer (Транспортный уровень) обеспечивает надёжную передачу данных между конечными точками (хостами). Управляет сегментацией, сборкой, контролем ошибок, потоком и повторной передачей.
Примеры реализации:
протоколы TCP (надёжный, с установлением соединения), UDP (быстрый, без установления соединения).
Примеры атак:
a) UDP-flood: Массовая отправка UDP-пакетов на случайные порты цели (т.к. UDP — без установления соединения, легко подделать источник) - сервер начинает генерировать ICMP-сообщения "Port Unreachable", что нагружает CPU и сеть. Часто используется в амплификационных DDoS-атаках (например, через DNS, NTP, SSDP).
Защита: Rate limiting. Фильтрация на пограничных маршрутизаторах. Отключение ненужных UDP-сервисов.
b) Атака "Land" (Local Area Network Denial): Отправка TCP-пакета, в котором IP-адрес источника и назначения одинаковы, а также порт источника = порту назначения. В уязвимых системах (старые Windows, Cisco IOS) это вызывало зацикливание или сбой.
Защита: Фильтрация пакетов с одинаковыми IP источника и назначения на границе сети.

5. Session Layer (Сеансовый уровень) управляет установлением, поддержанием и завершением сеансов связи между приложениями. Обеспечивает синхронизацию и восстановление сеанса при сбое.
Примеры реализации:
протоколы NetBIOS, RPC (gRPC), PPTP.
Примеры атак:
Некоторые специализированные протоколы работают на этом уровне и имеют свои уязвимости:

a) NetBIOS / SMB (частично): Устаревшие реализации позволяли перехватывать сессии в Windows-сетях, например атака SMB Relay — перенаправление аутентификационных данных на другой сервер.

b) RPC (Remote Procedure Call): Уязвимости в реализации могут позволить подмену сессии или выполнение кода, например уязвимости в MS-RPC (использовались в червях типа Blaster).

c) PPTP (Point-to-Point Tunneling Protocol): Несмотря на то, что это протокол туннелирования, он управляет сессиями и Известен слабым шифрованием и уязвимостями в установке сессии, плэтому лучше использовать современную замену: IPsec, OpenVPN, WireGuard.

Общие меры защиты:

- Шифрование всего сессионного трафика (TLS/SSL).
- Безопасная генерация и хранение идентификаторов сессий.
- Автоматическое завершение неактивных сессий.
- Многофакторная аутентификация (MFA) — даже при угоне сессии доступ может быть ограничен.
- Мониторинг аномалий (вход с нового устройства/IP во время активной сессии).

6. Presentation Layer (Уровень представления) отвечает за формат данных, шифрование, сжатие и преобразование данных для прикладного уровня. Обеспечивает совместимость между разными системами.

Примеры реализации:

протоколы SSL/TLS, MIME, JPEG, MPEG.

Примеры атак:

Атаки через сжатие данных (Compression Attacks)

a) CRIME (Compression Ratio Info-leak Made Easy): Использует сжатие TLS/SPDY, чтобы определить содержимое зашифрованных cookie. Злоумышленник отправляет множество запросов с известными данными и анализирует размер сжатого трафика → выводит секрет (например, session cookie).

b) BREACH (Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext): Аналогична CRIME, но работает на уровне HTTP-сжатия (gzip/deflate), даже если TLS не использует сжатие. Эффективна против веб-приложений, отражающих введённые данные в ответ (например, поиск).

Защита: Отключение сжатия в TLS. Для BREACH: добавление случайного "padding" в ответы, ограничение отражения пользовательских данных, CSRF-токены.

7. Application Layer (Прикладной уровень) обеспечивает интерфейс между пользовательскими приложениями и сетью. Предоставляет сетевые службы напрямую конечному пользователю.

Примеры реализации:

протоколы HTTP, FTP, SMTP, DNS, Telnet.

Примеры атак:

Атаки на DNS (Domain Name System)

a) DNS Spoofing / Cache Poisoning: Подмена DNS-записей в кэше резолвера для перенаправления пользователей на фишинговый сайт.

Защита: DNSSEC, обновление ПО DNS-серверов.

b) DNS Amplification (DDoS): Использование открытых DNS-резолверов для амплификационной DDoS-атаки.

Защита: закрытие рекурсивных резолверов от публичного доступа.

2. Выполнить конвертацию IPv4 в IPv6

Прямого конвертирования IPv4-адреса в IPv6-адрес для получения эквивалентного глобального IPv6-адреса не существует, потому что IPv4 и IPv6 — это разные протоколы с разными адресными пространствами.
Но для обеспечения совместимости существуют специальные форматы представления IPv4-адреса внутри IPv6. Наиболее распространённый способ - **IPv4-mapped IPv6 address**. Этот формат используется в сокетах ОС (например, в Linux) для представления IPv4-адреса в IPv6-форме.

Формат **IPv4-mapped IPv6**: ::ffff:a.b.c.d

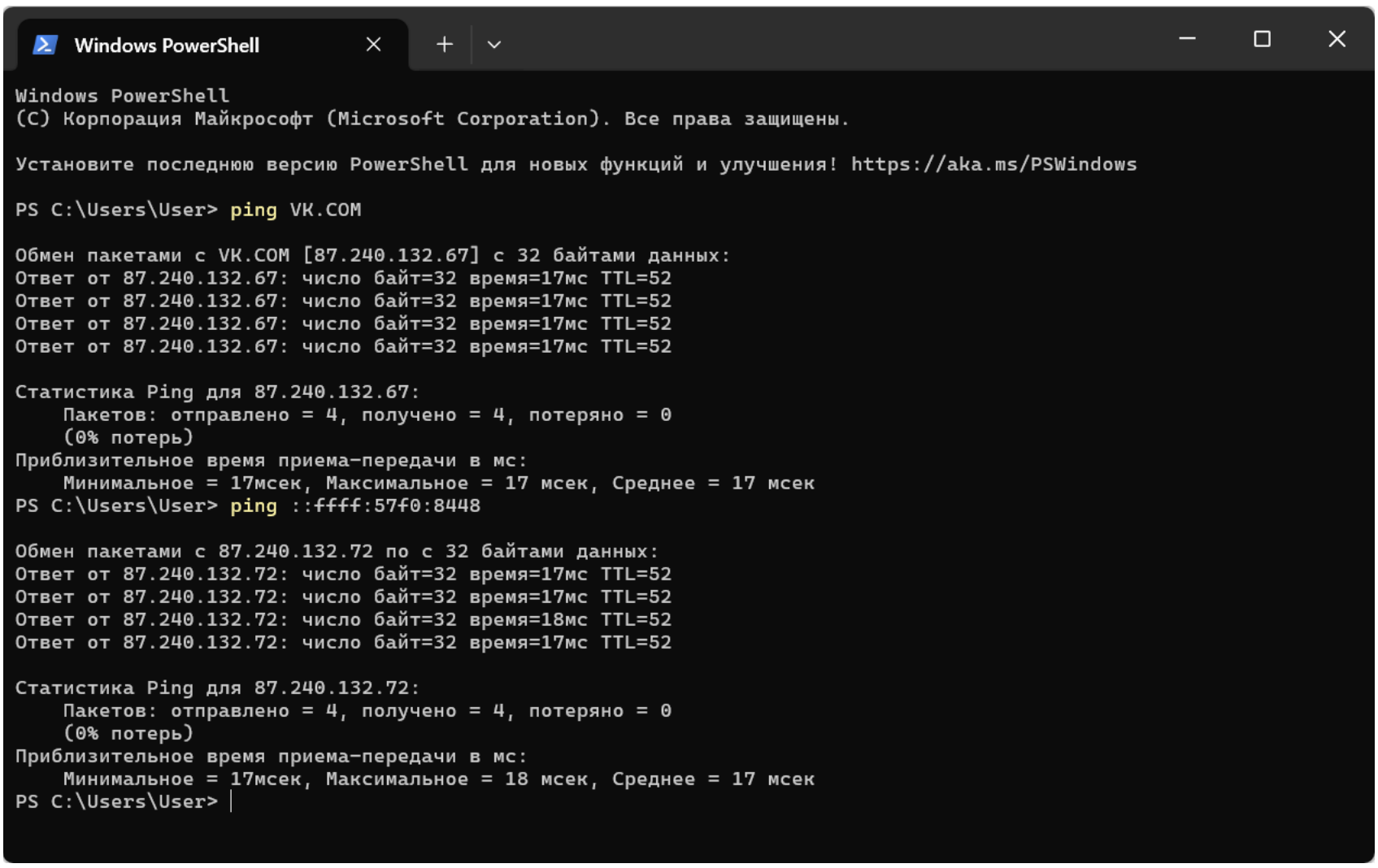
в полной шестнадцатеричной записи: 0000:0000:0000:0000:0000:ffff:aabb:ccdd

где a.b.c.d — обычный IPv4-адрес.

Пример для представления адреса IPv4 к сайту VK.COM в формате IPv6:

IPv4: 87.240.132.72
IPv6: ::ffff:87.240.132.72
IPv6 в hex:
Для перевода IPv4 в hex для mapped-адреса разобьем IPv4 на 4 октета и переведем каждый из них в hex:
87 - 57
240 - f0
132 - 84
72 - 48

Соберем последние 32 бита: 57f0:8448
Полный mapped-адрес: ::ffff:57f0:8448



3. Включит 3-й сетевой интерфейс в PfSense, настроить локальную сеть LAN2, подключить в эту сеть BM Ubuntu.

В VirtualBox для BM PfSense создаем две внутрение сети - internal_lan1 и internal_lan2:

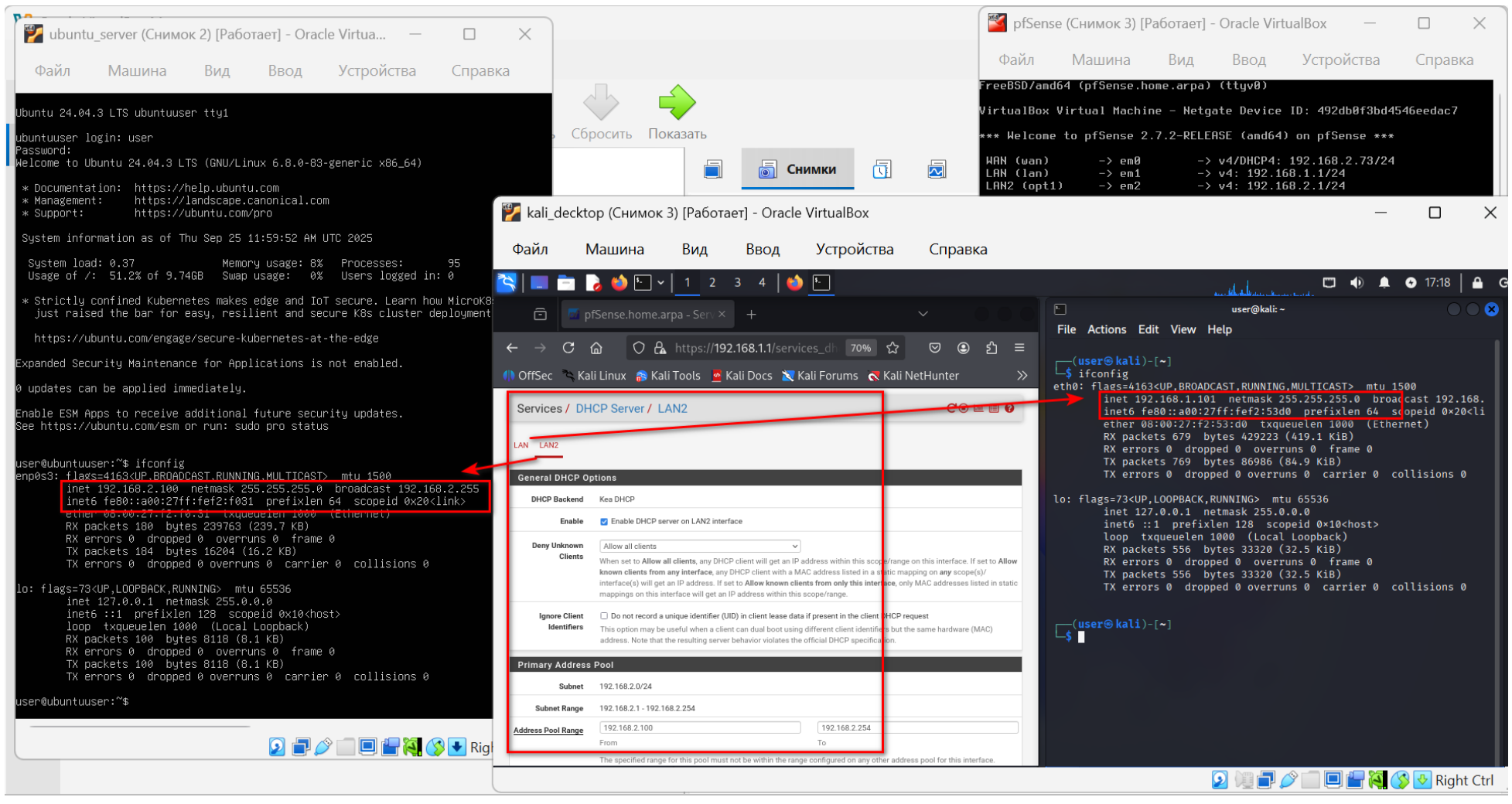
- сеть internal_lan1 назначаем для BM Kali и Metasploitable,
- сеть internal_lan2 назначаем для BM Ubuntu_server и Windows_server

В запущенной BM PfSense включаем интерфейсы em1 и em2 и конфигурируем их:

- для LAN, назначаем подсеть 192.168.1.0/24, адрес шлюза 192.168.1.1
- для LAN2, назначаем подсеть 192.168.2.0/24, адрес шлюза 192.168.2.1

В Web-консоли PfSense включаем и настраиваем DHCP сервера для сетей LAN и LAN2

После запуска BM Ubuntu и Kali присходит автоматическое назначение IP адресов из соответствующих диапазонов для каждой подсети:



3. В CiscoPacketTracer собрать локальную сеть

Из 4-х компьютеров (PC1_1, PC1_2, PC2_1, PC2_2) подключенных по сети ethernet к коммутатору switch1, который так же подключен к отдельно стоящему маршрутизатору router0.

В коммутаторе switch1 сконфигурированы порты и созданы VLAN10 и VLAN20:
- порт FastEthernet 0/1 - как trunk для подключения к маршрутизатору
- порты FastEthernet 0/2 и 0/3 - как access vlan 10 для подключения компьютеров PC1_1 и PC1_2
- порты FastEthernet 0/4 и 0/5 - как access vlan 20 для подключения компьютеров PC2_1 и PC2_2

В маршрутизаторе router0 сконфигурирован порт, настроен DHCP, созданы access-lists и правила:
- порт GigabitEthernet 0/0/1.10 – с адресом 192.168.10.0/24 для подключения vlan 10
- порт GigabitEthernet 0/0/1.20 – с адресом 192.168.20.0/24 для подключения vlan 20
- создан access-list icmp-rules в который добавлены правила:
    1. разрешает запросы icmp echo-reply из vlan20 в vlan10
    2. запрещает все запросы icmp из vlan10 в vlan20
    3. разрешает остальной IP-трафик между vlan