Лабораторная работа №9

Гусева, Булатов, Гришин

Задание 1.

1. pmap 135/tcp loc-srv #DCE endpoint resolution

epmap 135/udp loc-srv #DCE endpoint resolution

Порт 135 используется функцией отображения конечных точек RPC (Remote Procedure Call - удалённый вызов процедур), реализованной во многих технологиях Windows (например, приложения COM/DCOM, DFS, журналы событий, формирование очередей сообщений и Microsoft Outlook)

Так же, сюда относится и 445 порт.

- svchost.exe

1. http 80/tcp www www-http #World Wide Web

Общепринятый протокол интернет-связи, протокол передачи гипертекста (HTTP). Это порт, с которого компьютер отправляет и получает сообщения и сообщения на основе веб-клиента от веб-сервера и используется для отправки и получения страниц или данных HTML.

Так же, 443 порт является для http.

1. smtp 25/tcp mail #Simple Mail Transfer Protocol

протокол передачи почты.

У протокола две главные задачи:

* Проверка корректности настроек системы и предоставление «разрешения» на отправку email-сообщения для определенного устройства.
* Отправка исходящего сообщения на заданный адрес электронной почты и подтверждение успешной доставки. Если сообщение доставить не удается, отправитель получает соответствующее извещение.

Теоретически SMTP умеет работать с практически любыми протоколами так называемого транспортного уровня, включая TCP, UDP и другие. Еще на заре развития протокола за ним закрепили два номера порта:

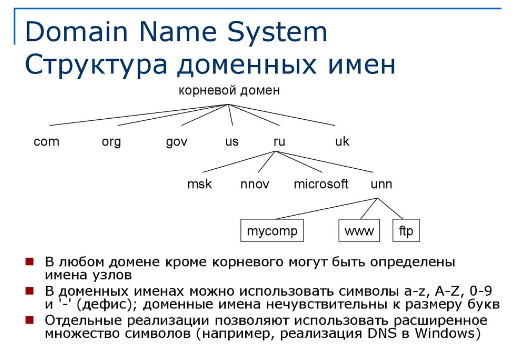
- Первый — это порт 25, посредством которого почта передается между почтовыми серверами.

- Второй — порт 587, благодаря которому почта передается от почтового клиента на сервер.

1. domain 53/tcp #Domain Name Server

domain 53/udp #Domain Name Server

Использует протокол управления передачей данных (TCP), который является одним из основных протоколов в сетях TCP/IP. TCP является протоколом с установлением соединения и требует квитирования для установки сквозной связи.



1. wsd 5357/tcp #Web Services on devices

Web Services for Devices или Web Services on Devices (WSD) - это API Microsoft, позволяющий программировать подключения к устройствам с поддержкой веб-служб, таким как принтеры, сканеры и файлообменники. Такие устройства соответствуют профилю Devices Profile for Web Services (DPWS). Это расширяемая структура, которая служит заменой старых сетевых функций Windows и общей основой для обеспечения доступа к новым API-интерфейсам устройств.

1. ws-discovery 3702/udp #WS-Discovery

ws-discovery 3702/tcp #WS-Discovery/

WS-Discovery представляет собой многоадресный протокол, который можно использовать для обнаружения других устройств, которые обмениваются данными через определенный протокол или интерфейс. Так, он применяется для обнаружения и обмена данными посредством SOAP с использованием пакетов UDP, поэтому иногда WS-Discovery называют SOAP-over-UDP.

- [svchost.exe]

1. ipsec-msft 4500/tcp #Microsoft IPsec NAT-T

ipsec-msft 4500/udp #Microsoft IPsec NAT-T /

- [svchost.exe]

NAT Traversal (NAT-T) — протокол, который инкапсулирует трафик VPN-соединения, работающего по таким протоколам как IPSec или PPTP, создавая пакеты UDP. Исходящие пакеты UDP пересылаются маршрутизатором, реализующим NAT Traversal через Интернет без всякого учёта их содержимого. Для этого NAT-T помещает дополнительный заголовок UDP перед пакетом IPSec, чтобы он во всей сети обрабатывался как обычный пакет UDP и хост получателя не проводил никаких проверок целостности.

1. ssdp 1900/tcp

ssdp 1900/udp

- [svchost.exe]

Simple Service Discovery Protocol (SSDP) - это сетевой протокол на основе пакета протоколов Интернета для рекламы и обнаружения сетевых услуг и информации о присутствии.

1. isakmp 500/udp ike #Internet Key Exchange

- [svchost.exe]

Internet Key Exchange (IKE) — безопасный протокол управления ключами, используемый для того, чтобы создать безопасный канал аутентификации связи между двумя устройствами.

IKE делает следующее:

* Согласование и управление IKE параметрами IPsec
* Аутентификация защищенного обмена ключами
* Обеспечивает аутентификацию взаимного равноправного узла с помощью общих секретов (а не паролей) и открытых ключей
* Обеспечивает защиту идентификации (в основном режиме)
* Применяет методы Diffie-Hellman и является необязательным в IPsec (общие ключи можно встроить вручную в конечных точках).

1. netbios-ssn 139/tcp nbsession #NETBIOS Session Service

NetBIOS session service (NBSS) - это метод соединения двух компьютеров для передачи больших сообщений или интенсивного трафика данных. Служба сеансов etBIOS (NBSS) - это метод соединения двух компьютеров для передачи больших сообщений или интенсивного трафика данных. Поскольку служба сеансов NetBIOS участвует в генерации и пересылке трафика, используется порт TCP 139. Служба сеансов NetBIOS в основном используется для принтеров и файловых служб по сети

Система с реализацией NBSS имеет следующие характеристики:

* Восстановление ошибок: Приложениям разрешено управлять сетями и предоставлять функции обнаружения и восстановления ошибок.
* Службы эталонной модели OSI: Транспортные и сеансовые службы эталонной модели взаимосвязи открытых систем (OSI) очень близки к тем, которые используются в NetBIOS. Однако NetBIOS не следует формату и шаблону модели OSI для передачи сообщений.
* Именование NBSS: Имена для NBSS имеют длину 16 байт с некоторыми специфическими ограничениями на значения байтов

Задание 2.

Входе выполнения задания были изучены способы подключения к ssh серверу через putty:

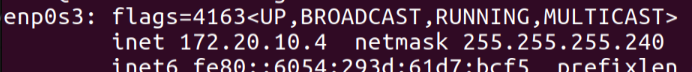
* С основной машины на виртуальную

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Начальные слушатели.

Установив необходимые инструменты (sudo apt install net-tools), и введя команду ifconfig узнаем ip виртуальной машины

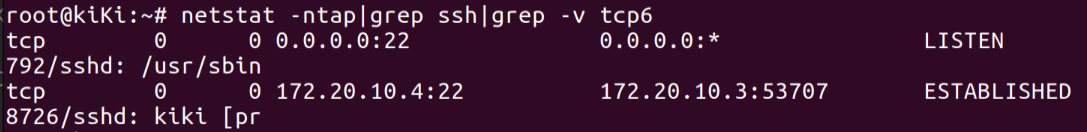


Подключившись с помощью Putty на виртуальную машину

В результате выполнения задания было произведено подключение к виртуальной машине через Putty, войдём в терминал

Изображение выглядит как текст, электроника, снимок экрана, дисплей

Автоматически созданное описание

Проверим подключение командой netstat -ntap|grep ssh|grep -v tcp6 

Появился Established

В процессах появились процессы, один для входящего соединения, второй для сокета



Ещё один процесс используется для связи с терминалом

Продублируем сессию :

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

По прежнему один прослушивающий сокет

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

На каждое входящее соединение создается по 2 процесса

1 – использует сокет , 2 – для связи с терминалом