**Активный анализ, сканер nmap.**

1. Назначение хостнейма
2. Настройка сети

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 1 хостнейм и адрес сети

Изменяем имя машины на фамилию и назначаем адрес в соответствии с нашей сетью

Сканировать Множество IP Адресов:

*Изображение выглядит как текст

Автоматически созданное описание*

Рисунок 2 сканирование множество

Такое сканирование выведет данные о конкретных указанных адресах

Сканировать Подсеть:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 3 сканирование всей подсети

Такое сканирование выведет информацию о всей подсети  
Также можно использовать команду nmap 172.16.27.0/24

Сканировать Диапазон IP Адресов (172.16.27.0 — 172.16.27.40):

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 4 сканирование диапазона адресов

Такое сканирование выведет информацию об адресах указанного диапазона

Сканировать сеть в поиске Активных Хостов:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 5 сканирование в поиске активных хостов

Такое сканирование выведет информацию об активных хостах указанного адреса подсети

Сканирование списка хостов/сетей из Файла:

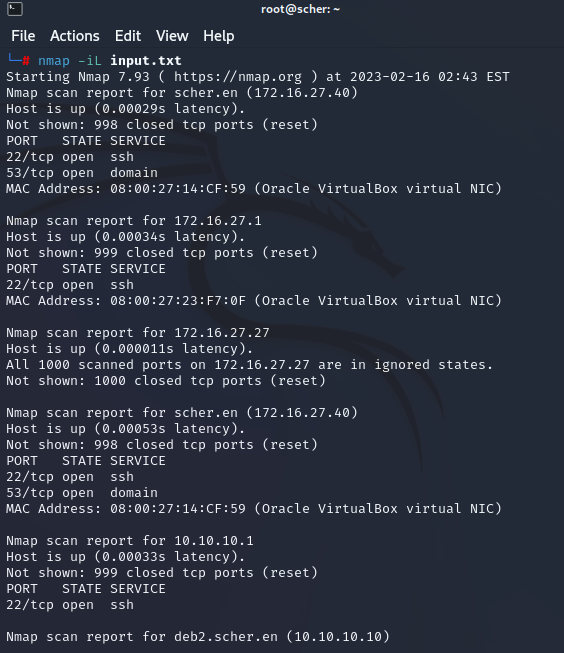


Рисунок 6 сканирование списка хостов/сетей и файла

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 7 продолжение сканирование списка хостов/сетей их файла

Такое сканирование выводит данные из файла, в котором хранятся списки хостов/сетей, указанные в различных форматах

Исключить Цели из сканирования Nmap-ом:Изображение выглядит как текст

Автоматически созданное описание

Рисунок 8 исключение цели из сканирования

Такое исключение выводит информацию обо всех указанных хостах, кроме того, что помечен на исключение

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 9 исключения списка хостов из файла

Такое исключение выводит информацию обо всех указанных хостах, кроме того, что помечен на исключение в файле

Сканировать Один Порт:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 10 сканирование одного порта

Такое сканирование выведен информацию об одном указанном порте (к примеру, 53 (домен))

Сканировать Несколько Портов:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 11 сканирование нескольких портов

Такое сканирование выведен информацию о нескольких указанных портах (к примеру, 22(ssh) 53 (домен))

Сканировать Диапазон Портов:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 12 сканирование диапазона портов

Такое сканирование выведен информацию о портах указанных в диапазоне. У данного хоста нашел только 22(ssh) и 53 (домен)

Сканировать Все Порты:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 13 сканирование всех портов

Такое сканирование выведет информацию обо всех найденных портах у конкретного хоста

Сканировать несколько самых Распространенных Портов:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 14 сканирование самых распространенных портов

Такое сканирование выведет информацию о некоторых самых распространенных портах, в зависимости от указанного количества

Сканирование протоколов IP

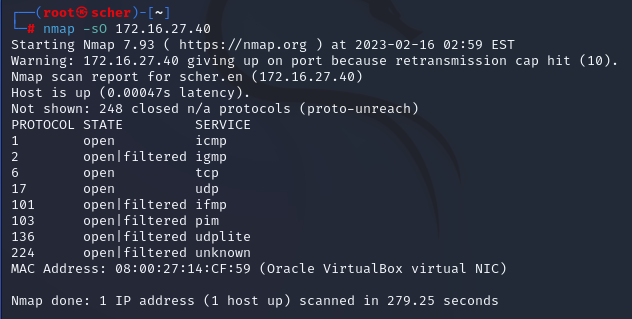


Рисунок 15 сканирование IP протоколов

Такое сканирование определит какие IP протоколы (TCP, UDP, ICMP, и т.д.) поддерживает сканируемый хост

В момент проведения сканирования методами TCP Connect, TCP ACK, TCP SIN TCP Null, Fin Xmas, на сканируемом хосте запустить сниффер, и выделить из захвата пакеты подтверждающие факт сканирования, приложить скрины в отчет, данные захвата сохранить, для демонстрации преподавателю (tcpdump or whireshark)

Сканировать все TCP Порты:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 16 сканирование всех tcp портов

Такое сканирование выведет все tcp порты сканируемого хоста

Изображение выглядит как текст

Автоматически созданное описание

*Рисунок 17 tcpdump L-SRV*

С помощью команды tcpdump -I enp0s8 произведем сниффинг и заметим, что кто-то сканирует наши порты

**ТСР пакеты с какими флагами отправляются с Kali на сканируемый хост?**

**-** множественные попытки установить соединение посредством отправления пакетов с флагом SYN

**Какие флаги установлены в ответных ТСР пакетах сканируемого хоста, о чем говорят флаги установленные в этих пакетах, с каких портов они отправлены?**

**-** сканируемый хост пытается оборвать (закрыть) соединение, посылая в ответ флаги RST

Порт сканирующей машины (источника) 56386, порт сканируемой машины (назначения) 1720

Сканировать все UDP Порты:Изображение выглядит как текст

Автоматически созданное описание

Рисунок 18 сканирование всех udp портов

Такое сканирование выведет все udp порты сканируемого хоста

Объединение сканирования разных портов:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 19 объединенное сканирование разных портов

Такое сканирование выведет все запрошенные порты различных протоколов базирующихся на udp, tcp сканируемого хоста

Активировать Быстрый Режим сканирования:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 20 активация быстрого сканирования

Название само за себя говорит

Включить Определение ОС:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 21 сканирование определяющее ОС

Такое сканирование определит операционную систему сканируемого хоста

Включить Определение Версии Сервисов:Изображение выглядит как текст

Автоматически созданное описание

Рисунок 22 сканирование определения версии сервисов

Такое сканирование определит текущие версии сервисов имеющихся на сканируемом хосте

ACK-сканирование

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 23 ACK сканирование

Такое сканирование поможет узнать защищен ли какими-либо пакетными фильтрами ли фаерволом

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 24 tcpdump L-SRV

**ТСР пакеты с какими флагами отправляются с Kali на сканируемый хост?**

**-** отправляют флаги с пустым значение, поскольку метод этого сканирования заключается в отправке ACK пакетов на сканируемых порт.

**Какие флаги установлены в ответных ТСР пакетах сканируемого хоста, о чем говорят флаги установленные в этих пакетах, с каких портов они отправлены?**

**-** в ответ приходят флаги RST, что говорит о том, что порт классифицируется как не фильтруемый

Порт сканирующей машины (источника) 54745, порт сканируемой машины (назначения) imap2

TCP Window

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 25 сканирование tcp window

В результате такого сканирование по значениям поля Initial Window пришедшего в ответ, можно определить открытые порты

TCP Null сканирование:Изображение выглядит как текст

Автоматически созданное описание

Рисунок 26 сканирование tcp null

Такое сканирование заключаются в отправке пакетов с отключенными флагами в заголовке

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 27 tcpdump L-SRV

**ТСР пакеты с какими флагами отправляются с Kali на сканируемый хост?**

**-** при сканировании TCP Null у отправленных TCP-пакетов нет установленных флагов.

**Какие флаги установлены в ответных ТСР пакетах сканируемого хоста, о чем говорят флаги установленные в этих пакетах, с каких портов они отправлены?**

**-** Если порт closed, цель должна ответить RST (согласно RFC)  
Порт сканирующей машины (источника) 46328, порт сканируемой машины (назначения) 8087

TCP Fin сканирование:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 28 FIN сканирование

При таком сканировании отправляется пакет с установленным флагом FIN, который используется для корректного закрытия соединения

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 29 tcpdump L-SRV

**ТСР пакеты с какими флагами отправляются с Kali на сканируемый хост?**

**-** вместо отправки полностью пустого TCP-пакета он отправляет пакет с установленным флагом FIN

**Какие флаги установлены в ответных ТСР пакетах сканируемого хоста, о чем говорят флаги установленные в этих пакетах, с каких портов они отправлены?**

**-** цель должна ответить RST для closed портов, в соответствии с RFC.  
Порт сканирующей машины (источника) 43749, порт сканируемой машины (назначения) 6543

TCP Xmas сканирование:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 30 xmas сканирование

При таком сканировании используются TCP-пакеты с установленными флагами PSH, URG и FIN

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 31 tcpdump L-SRV

**ТСР пакеты с какими флагами отправляются с Kali на сканируемый хост?**

**-** используются TCP-пакеты с установленными флагами PSH, URG и FIN

**Какие флаги установлены в ответных ТСР пакетах сканируемого хоста, о чем говорят флаги установленные в этих пакетах, с каких портов они отправлены?**

**-** ожидает пакеты RST для closed портов в соответствии с RFC  
Порт сканирующей машины (источника) 56127, порт сканируемой машины (назначения) 5200

Скрытое Сканирование

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 32 tcp syn сканирование

При вызове Nmap посылает SYN-пакет, как бы ради того, чтобы установить новое соединение

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 33 tcpdump L-SRV

**ТСР пакеты с какими флагами отправляются с Kali на сканируемый хост?**

**-** посылает SYN-пакет, как бы ради того, чтобы установить новое соединение

**Какие флаги установлены в ответных ТСР пакетах сканируемого хоста, о чем говорят флаги установленные в этих пакетах, с каких портов они отправлены?**

**-** Если в ответе присутствуют флаги SYN или ACK, считается, что порт открыт. Флаг RST говорит об обратном.  
Порт сканирующей машины (источника) 38563, порт сканируемой машины (назначения) submission

RPC-сканирование

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 34 RPC сканирование

Такое сканирование используется для определения программы, обслуживающей порт и её версии, и заключается в «затоплении»

Никогда не производить обратное преобразование DNS имен для каждого обнаруженного активного IP адреса:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 35 преобразование dns имен для активного адреса

Такое сканирование используется, чтобы никогда не производить обратное преобразование DNS имен для каждого обнаруженного активного IP адреса

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 36 сохранение результата сканирования

Сохраняем результат сканирования в созданный файл

Подменить MAC Адреса и подмена MAC Адреса Случайным MAC-ом:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 37 подмена mac адреса

*Несколько самых важных или интересных, по вашему мнению, результатов сохраните в файл, для демонстрации преподавателю.*

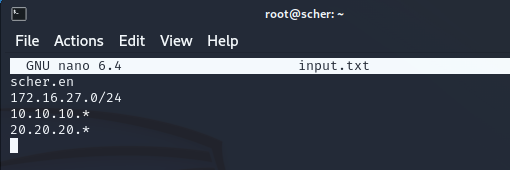


Рисунок 38 input.txt

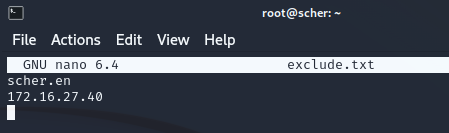


Рисунок 39 exclude.txt

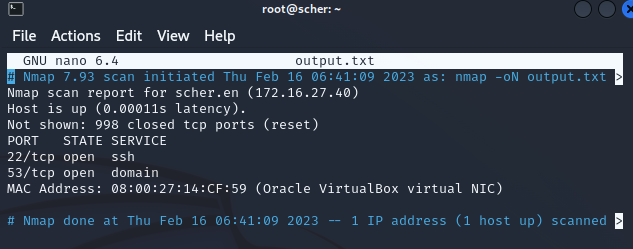


Рисунок 40 output.txt

*Приведите примеры комбинации нескольких параметров сканирования в одну попытку, приложить скрин.*

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 41 комбинация

Используется связка вывода скрытого syn-сканирования, определения ОС и 10 популярных портов сканируемого хоста

*С помощью источников в Интернет отыскать еще  2-3 не упомянутых в работе примера использования сканера nmap, скрины приложить в отчет.*

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 42 сканирование PO

Выполнение ping с использованием ip-протокола

*Изображение выглядит как текст

Автоматически созданное описание*

Рисунок 43 быстрое сканирование для всех портов

Используется для быстрого поиска всех открытых портов

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 44 сканирование интерфейсов и маршрутов

Используется для выведения интерфейсов и маршрутов сканируемого хоста

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 45 proxychains

1. **Как сделать сканирование незаметным или скрыть реальный источник сканирования? (устный ответ + демонстрация практического примера)**

**-** Для того чтобы остаться неузнанным при проведении сканирования можно запустить сканер nmap c настроенным proxychain. Тогда, даже если, администратор или система обнаружит процесс сканирования, определить реальный ip адрес источника им не удастся.

1. **Как защититься от сканирования? (устный ответ+практического примера).**

**- Honeypot («Ловушка»)** - ресурс, представляющий собой приманку для злоумышленников.  
Фактически основная задача Honeypot — подвергнуться атаке или несанкционированному сканированию с целью изучения стратегии и методов сканирования и определения перечня средств, необходимых для предотвращения будущих атак. Суть работы Honeypot заключается в создании ловушек — образов систем, которые извне воспринимаются как полноценные машины с установленными на них операционными системами, а, следовательно, поддающиеся сканированию.