Skillbox

Этичный хакинг с Nmap

Специалист по кибербезопасности. Модуль 2

Введение

Этот модуль посвящен активному сбору информации с использованием самой распространенной программы сетевого анализа — Network Mapper или nmap.

1. Мы получим навыки сетевого обнаружения и добычи подробной информации о хостах.

2. Научимся использовать скриптовый движок nmap для поиска уязвимостей и тестирования на проникновение в систему.

3. Узнаем об управлении производительностью и опциями вывода nmap.

Определение целей сканирования

Сканирование проводим из-под привилегированного пользователя, это необходимо для отправки «сырых» пакетов. Так нам не нужно устанавливать полное соединение — это уменьшит время сканирования и вероятность нашего обнаружения.

В консоли nmap отображаются результаты сканирования по 1000 самым популярным портам. Доменные имена можно указывать в CIDR-формате для сканирования подсети расположения домена. CIDR-формат доменных имен нужен, когда мы указываем не конкретный адрес, а подсеть.

В качестве целей nmap может принимать адреса и их диапазоны протокола ipv4. Эта опция упрощает сканирование больших диапазонов адресов:
nmap 192.168.7.1
nmap 192.168.1.1/24
nmap 192.168.1.1-255

В качестве целей nmap может принимать и список адресов в формате файла:
nmap -iL <Ваш список адресов>

Для исключения отдельных хостов и подсетей в сканировании пригодится опция:
nmap --exclude --excludefile <Ваш список адресов>

Обнаружение хостов

Запрос, который позволяет определить имена хостов в заданной сети:

nmap -sL skillbox.ru/24

Иногда вывод содержит полезную информацию о сетевой инфраструктуре сканируемого диапазона. На уроке мы нашли хост с именем radar.qrator.net — он уже был в выдачи поисковой системы Censys.io для skillbox.ru (https://censys.io/domain/skillbox.ru/table), что гарантирует использование этой системы в инфраструктуре skillbox.

Для обнаружения работающих хостов пригодится опция:

nmap -sn skillbox.ru/24

В результате nmap выдаст все активные хосты в указанных нами целях, а сканирование портов производиться не будет.

Также этап обнаружения пропускается опцией -Pn. А опция -sn нужна для отключения сканирования портов.

Чтобы отследить движение пакетов по сетевой инфраструктуре применим функцию трассировки:

nmap --traceroute skillbox.ru -sn -Pn

В стандартном выводе видим результаты трассировки, где указано количество узлов, время доступа и сетевые адреса нашего маршрута.

В графической версии nmap — zenmap есть функция визуализации топологии сети при построении отчетов.

Сканирование портов

Для TCP SYN (скрытого) сканирования используем запрос:
nmap -sS skillbox.ru

Иногда для тестирования нам нужно полное подключение. Для этого используется соединение TCP Connect с флагом -sT:
nmap -sT skillbox.ru

Отличие сканирования заметно лишь при детальном рассмотрении дампов трафика и логов систем обнаружения вторжения.

Некоторые службы используют UDP порты для установления соединения. Для определения таких сервисов пользуемся флагом -sU:
nmap -sU skillbox.ru

Другие флаги сканирования:
-sN (TCP Null scan) — устанавливает значение заголовка TCP флага равное 0.
-sF (FIN scan) — устанавливает только TCP FIN.
-sX (Xmas scan) — устанавливает флаги FIN, PSH, URG.

Такое сканирование отправляет неправильные пакеты, имитируя ошибки соединения, что иногда позволяет определить скрытые порты.

Подробнее про эти методы вы можете найти на сайте документации nmap:
https://nmap.org/book/scan-methods-null-fin-xmas-scan.html

Работа с FTP-сервером в nmap

Опция -b анализирует ответы о неправильной авторизации заданного сервера:
nmap -b ftpuser:PassW0rd@192.168.0.1:21 10.0.2.1

Диапазон сканируемых портов определяется ключом -p. Для перечисления всех портов можно использовать -p-.

nmap -p 80,443 skillbox.ru — сканирует только 80 и 443 порты.
nmap -p80-443 skillbox.ru — сканирует диапозон портов с 80 по 443.
nmap -p- skillbox.ru — сканирует весь диапозон портов.

Для исключения сканирования некоторых портов используем опцию --exclude-ports:
nmap -p21-443 --exclude-ports 80 skillbox.ru

Без опций nmap сканирует 1000 самых используемых портов, но мы можем задать собственное число опцией --top-ports:
nmap --top-ports 10 skillbox.ru

Эта опция полезна при сканировании защищенных систем, так как некоторые брандмауэры ограничивают возможность сканирования фиксированным количеством портов.

Также есть режимы быстрого сканирования -F и упорядоченного сканирования -r.

Обнаружение версий операционных систем и сервисов

Для обнаружения версий операционных систем используется ключ -O:
nmap -O -p 25,80,443 skillbox.ru

В результате nmap запустит скрипт обнаружения и выдаст наиболее вероятные результаты.

Следующая опция отвечает за обнаружение версий сервисов:
nmap -sV skillbox.ru -p25,80,443

Сервисы могут быть запрограммированы на заведомо неправильные ответы, но такое случается редко. И помните, что запущенные скрипты оставляют много следов для систем обнаружения.

Производительность и тайминг

Иногда необходимо замедлить сканирование, чтобы избежать обнаружения, или ускорить процесс в случае работы с сетью с высокой скоростью соединения.

Главная опция управления производительностью — -T<0-5>, у неё есть 5 режимов сканирования:
0 — на сканирование уйдет целая вечность.
1 — самый медленный режим, но самый скрытный.
2 — медленное сканирование для снижения нагрузки на полосу пропускания.
3 — «вежливый».
4 — быстрый и оптимальный режим.
5 — самый быстрый или «безумный».

Выглядит так: nmap -p- -T4 skillbox.ru

Тайминги — это время задержек и простоев в сканировании. Опция задает максимальное число параллельно запущенных потоков сканирования и диапазон задержки для подаваемых в сеть сигналов.

Определяем размер групп хостов для параллельного сканирования:
--min-hostgroup/max-hostgroup <size>
Задаём максимальное и минимальное количество запросов для группы хостов:
--min-parallelism/max-parallelism <numprobes>

Устанавливаем значение повторных попыток сканирования портов:
--max-retries

Устанавливаем паузы сканирования между портами:
--scan-delay/--max-scan-delay

Используйте опции с осторожностью, они могут существенно замедлить сканирование.

Skillbox

Обход фаерволов и спуфинг

Обход фаерволов

Ключ для разделения TCP заголовков на несколько пакетов:
nmap -f skillbox.ru

Можем задать размер фрагмента (не менее 16 байт и кратный 8) вручную опцией -mtu:
nmap -f skillbox.ru -mtu 16

Для сокрытия источника сканирования пользуемся методом отправки пакетов, подписанных фиктивными адресами:
nmap -n -D 192.168.1.1,192.168.1.2,192.168.1.3 192.168.1.100

Все пакеты подписаны указанными IP-адресами, несмотря на то, что отправлены с вашего адреса. Опция -n позволяет не использовать разрешение DNS.

Спуфинг

Спуфинг отправителя — это подмена источника сканирования. Функция -S указывает источник запроса, и все результаты сканирования будут отправлены на него. В запросе следует указать используемый интерфейс опцией -e. Опционально: порт отправителя опцией -g/--source-port и опция пропуска обнаружения хостов -sn:
nmap -S yandex.ru skillbox.ru -e eth0 -g 53 -sn

Некоторые сервисы оказывают доверие определенным исходящим портам:
DNS 53/TCP/UDP
FTP 20,21,22/TCP
DHCP 67/UDP
Kerberos 88/TCP/UDP

Чтобы скрыть свое сетевое местоположение, используем http или socks прокси:
nmap --proxies socks4://127.0.0.1:9050 skillbox.ru -p80

Опцией --data-length добавляем в пакет установленный размер случайных данных:
nmap --data-lenght 128 skillbox.ru

Вместо случайных данных можем добавить в пакет полезную нагрузку в двоичном коде:
nmap --data 0xDAEDBEEF skillbox.ru

Skillbox

Скриптовый движок Nmap

Nmap

Инвазивные скрипты способны совершать атаки грубой силы на сервисы и протоколы, имитировать вторжение и осуществлять ddos-атаки. Если ваша цель не защищена, а атака станет успешной, вы можете понести уголовную ответственность..

Начнём с безопасных примеров и попробуем получить субдомены нашей цели:

nmap --script=dns-brute -Pn -sn skillbox.ru

При сканировании некоторых целей можно извлечь доменные имена почтовых, тестовых и прокси-серверов, а также vpn и sip. Последние представляют наибольший интерес, так как часто они менее защищены и имеют уязвимости.

Если скрипт не дал никаких результатов, вы можете проверить его работу опцией режима отладки --script-trace

Не забывайте обновлять базу данных скриптов командой --script-updatedb

Некоторые скрипты требуют установки дополнительных модулей, подробнее об этом по ссылке: https://nmap.org/nsedoc/

Управление выводом

Рассмотрим возможности управления выводом в nmap и научимся правильно сохранять результаты для последующего использования.

Запрос для отображения результатов в стандартном формате nmap:

nmap skillbox.ru -oN result

Запрос для отображения результатов в XML-формате для передачи их другой программе или сервису:

nmap skillbox.ru -oX result

Наиболее удобным форматом для обработки из терминала является Grepable.

Для формирования отчета рекомендуем использовать ключ --webxml, который улучшает портируемость результата, сохраненного в XML.

Для детализации отображения процесса сканирования мы можем повысить уровень вербальности. Для этого нужна опция -v. Повышаем уровень, добавляя -vv -vvv -vvvv или нажимая v в процессе сканирования, уменьшаем с помощью shift + v.

Для вывода информации об оставшемся времени сканирования можно нажать i.

Можем ограничить вывод только открытыми портами опцией --open. Чтобы узнать, почему nmap считает порт открытым или закрытым, используем ключ --reason.