ПАМЯТКА
Этический хакинг с Nmap. Определение целей сканирования

Примеры команд	Ключ	Описание
Определение целей		
nmap 192.168.1.1		Сканирование одного IP
nmap 192.168.1.1 192.168.2.1		Сканирование определенных IP-адресов
nmap 192.168.1.1-254		Сканирование диапазона
nmap scanme.nmap.org		Сканирование домена
nmap 192.168.1.0/24		Сканирование с использованием CIDR
nmap -iL targets.txt	-iL	Сканирование целей из файла
nmap -iR 100	-iR	Сканирование 100 случайных хостов
nmap 192.168.1.0/24 --exclude 192.168.1.1	--exclude	Исключить перечисленные хосты
Техники сканирования		
nmap scanme.org -sS	-sS	Сканирование порта TCP SYN (по умолчанию)
nmap scanme.org -sT	-sT	Сканирование TCP-порта(По умолчанию без прав root)
nmap scanme.org -sU	-sU	Сканирование портов UDP
nmap scanme.org -sA	-sA	Сканирование порта TCP ACK
nmap scanme.org -sW	-sW	Сканирование портов TCP Window
nmap scanme.org -sM	-sM	Сканирование TCP Maimon (Применяется для обнаружение открытых портов используя RFC793)
nmap -sO scanme.org	-sO	Сканирование указанного протокола
nmap scanme.org -sN	-sN	Устанавливает заголовок флага TCP равный 0
nmap scanme.org -sF	-sF	Устанавливает только бит TCP FIN
nmap scanme.org -sX	-sX	Устанавливает флаги FIN, PSH и URG
nmap --scanflags	--scanflags	Устанавливает произвольные пользовательские флаги TCP
Обнаружение хостов		
nmap 192.168.1.1-254 -sL	-sL	List scan - Перечисление целей
nmap 192.168.1.1/24 -sn	-sn	Отключить сканирование портов
nmap 192.168.1.1-254 -Pn	-Pn	Отключить обнаружение хоста. Только сканирование портов
nmap 192.168.1.1-254 -PS22-25,80	-PS	Обнаружение TCP SYN на порту x. Порт 80 по умолчанию
nmap 192.168.1.1-254 -PA22-25,80	-PA	Обнаружение ACK TCP на порту x. Порт 80 по умолчанию
nmap 192.168.1.1-254 -PU53	-PU	UDP-обнаружение на порту x. Порт 40125 по умолчанию
nmap 192.168.1.1-1/24 -PR	-PR	Обнаружение ARP в локальной сети
nmap 192.168.1.1 -n	-n	Не устанавливать DNS resolving
Спецификация портов		
nmap scanme.org -p 21	-p	Сканирование для порта x
nmap scanme.org -p 21-80	-p	Диапазон портов
nmap scanme.org -p U:53,T:21-25,80	-p	Сканирование нескольких портов TCP и UDP
nmap scanme.org -p-	-p-	Сканирование всех портов
nmap scanme.org -p http,https	-p	Сканирование портов по имени службы
nmap scanme.org -F	-F	Быстрое сканирование портов (100 портов)
nmap scanme.org --top-ports 100	--top-ports	Сканирование самых популярных x портов
nmap scanme.org -p-65535	-p-65535	Если оставить исходный порт в диапазоне, сканирование начнется с порта 1
nmap scanme.org -p0-	-p0-	Если оставить в стороне дальний порт, сканирование пройдет до порта 65535
Обнаружение службы и версии		
nmap scanme.org -sV	-sV	Попытки определить версию службы, работающей на порту
nmap scanme.org -sV --version-intensity 8	-sV --version-intensity	Уровень интенсивности от 0 до 9. Чем выше число, тем выше вероятность правильности
nmap scanme.org -sV --version-light	-sV --version-light	Включить легкий режим. Меньшая вероятность правильности. Быстрее
nmap scanme.org -sV --version-all	-sV --version-all	Включите уровень интенсивности 9. Более высокая вероятность правильности. Помедленнее
nmap scanme.org -A	-A	Включает обнаружение ОС, обнаружение версий, сканирование скриптов и трассировку
nmap scanme.org -O	-O	Удаленное определение ОС с использованием стека TCP / IP
nmap scanme.org -O --osscan-limit	-O --osscan-limit	Если хотя бы один открытый и один закрытый порт TCP не найден, он не будет пытаться Обнаружение ОС хоста
nmap scanme.org -O --osscan-guess	-O --osscan-guess	Заставляет Nmap заведывать более агрессивно
nmap scanme.org -O --max-os-tries 1	-O --max-os-tries	Установите максимальное количество попыток обнаружения ОС против цели
nmap scanme.org -A	-A	Включает обнаружение ОС, обнаружение версий, сканирование скриптов и трассировку

Тайминг и Производительность		
nmap scanme.org -T0	-T0	Параноик (0) Уклонение от системы обнаружения вторжений
nmap scanme.org -T1	-T1	Подлый (1) Уклонение от системы обнаружения вторжений
nmap scanme.org -T2	-T2	Вежливый (2) Замедляет сканирование, чтобы использовать меньшую полосу пропускания и использовать меньше ресурсов целевой машины
nmap scanme.org -T3	-T3	Нормальный (3) который является скоростью по умолчанию
nmap scanme.org -T4	-T4	Агрессивные (4) скорости сканирования; предполагает, что вы находитесь в достаточно быстрой и надежной сети
nmap scanme.org -T5	-T5	Безумная (5) скорость сканирования; предполагает, что вы находитесь в чрезвычайно быстрой сети
nmap scanme.org --host-timeout 1s	--host-timeout 1s; 1m; 1h	Установление времени лимита сканирования
nmap scanme.org --min-rtt-timeout 1m	--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout 1s; 1m; 1h	Определяет время прохождения зонда
nmap scanme.org--min-hostgroup 50	--min-hostgroup/max-hostgroup 50; 1024	Размеры группы сканирования параллельного хоста
nmap --min-parallelism 10	--min-parallelism/max-parallelism 10; 1	Распараллеливание зонда
nmap scanme.org --scan-delay 1s	--scan-delay/--max-scan-delay 20ms; 1s; 1m; 1h	Отрегулируйте задержку между датчиками
nmap scanme.org --max-retries 1	--max-retries 1	Укажите максимальное количество повторных передач проверки порта
nmap scanme.org --min-rate 100	--min-rate 100	Отправка пакетов не медленнее, чем <число> в секунду
nmap scanme.org --max-rate100	--max-rate 100	Отправлять пакеты не быстрее, чем <число> в секунду
NSE скрипты		
nmap scanme.org -sC	-sC	Сканирование с использованием скриптов NSE
nmap scanme.org --script default	--script default	Сканирование с использованием стандартных скриптов NSE (тоже что и -sC)
nmap scanme.org --script=banner	--script	Сканирование с одним скриптом. Пример баннера
nmap scanme.org --script=http*	--script	Сканирование с подстановочным знаком. Пример http
nmap scanme.org --script=http,banner	--script	Сканирование двумя скриптами. Пример http и баннера
nmap scanme.org --script "not intrusive"	--script	Сканирование по умолчанию, но удаление навязчивых скриптов
nmap -Pn --script=http-sitemap-generator scanme.nmap.org	--script=http-sitemap-generator	Генератор карты сайта
nmap -n -Pn -p 80 --open -sV -vvv --script banner,http-title -iR 1000	--script banner,http-title	Быстрый поиск случайных веб-серверов
nmap -Pn --script=dns-brute scanme.org	--script=dns-brute	Поиск субдоменов методом перебора
nmap -n -Pn -vv -O -sV --script smb-enum*,smb-ls,smb-mbenum, smb-os-discovery,smb-s*,smb-vuln*,smbv2* -vv 192.168.1.1		Скрипты для поиска SMB уязвимостей
nmap --script whois* scanme.org -Pn	--script whois*	Получить информацию о домене
nmap -p80 --script http-unsafe-output-escaping scanme.nmap.org		Обнаружение уязвимостей межсайтового скриптинга
nmap -p80 --script http-sql-injection scanme.nmap.org		Проверка на SQL-инъекции
Фаерволы / IDS Уклонение и Спуфинг		
nmap scanme.org -f	-f	Фрагментированное сканирование. (Для обхода пакетных фильтров)
nmap scanme.org --mtu 32	--mtu	Установите свой собственный размер фрагмента
nmap -D 192.168.1.101,192.168.1.102,192.168.1.103,192.168.1.23 192.168.1.1	-D	Сканировать с поддельных IP-адресов
nmap -D decoy-ip1,decoy-ip2,your-own-ip,decoy-ip3,decoy-ip4 remote-host-ip	-D	Сканировать с поддельных доменов
nmap -S www.microsoft.com www.facebook.com	-S	Сканирование Facebook из Microsoft (-e eth0 -Pn может потребоваться)
nmap -g 53 scanme.org	-g	Использовать данный номер порта источника
nmap --proxies http://192.168.1.1:8080, http://192.168.1.2:8080 192.168.1.1	--proxies	Релейные соединения через HTTP / SOCKS4 прокси
	--data-length	Добавляет случайные данные в отправленные пакеты
Пример IDS команды уклонения		
nmap -f -t 0 -n -Pn --data-length 200 -D 192.168.1.101,192.168.1.102,192.168.1.103,192.168.1.23 192.168.1.1		
Результат		
nmap scanme.org -oN normal	-oN	Обычный вывод в файл normal
nmap scanme.org -oX xml	-oX	Вывод XML в файл xml
nmap scanme.org -oG grep	-oG	Grepable вывод в файл grep
nmap scanme.org -oA results	-oA	Вывод в трех основных форматах одновременно
nmap scanme.org -oG -	-oG -	Grepable вывод на экран. -oN -, -oX - также можно использовать
nmap scanme.org -oN file --append-output	--append-output	Добавить сканирование к предыдущему файлу сканирования
nmap scanme.org -v	-v	Увеличьте уровень verbose (используйте -vv или больше для большего эффекта)
nmap scanme.org -d	-d	Увеличьте уровень отладки (используйте -dd или more для большего эффекта)
nmap scanme.org --reason	--reason	Показать причину, по которой порт находится в определенном состоянии, тот же вывод, что и -vv

nmap scanme.org --open	--open	Показывать только открытые (или возможно открытые) порты
nmap scanme.org -T4 --packet-trace	--packet-trace	Показать все отправленные и полученные пакеты
nmap --iflist	--iflist	Показывает интерфейсы хоста и маршруты
nmap --resume results	--resume	Возобновить сканирование
Полезные примеры вывода Nmap		
nmap -p80 -sV -oG - --open 192.168.1.0/24 | grep open		Сканирование для веб-серверов и grep, чтобы показать, какие IP-адреса работают веб-серверы
nmap -iR 100 -n | grep "report" | cut -d " " -f5 > live-hosts.txt		Создайте список IP-адресов живых хостов
nmap -iR 100 -n | grep "report" | cut -d " " -f5 >> live-hosts.txt		Добавить IP в список живых хостов
ndiff scan1.xml scan2.xml		Сравните вывод из nmap с помощью ndiff
xsltproc nmap.xml -o nmap.html		Преобразование файлов Nmap XML в файлы HTML
Разные варианты		
nmap -p80 -6 2a03:2880:f10a:83:face:b00c:0:25de -Pn	-6	Включить сканирование IPv6
nmap -h	-h	экран справки nmap
Другие полезные команды Nmap		
nmap -iR 10 -PS22-25,80 -v -sn		Обнаружение только на портах x
nmap 192.168.1.1-1/24 -PR -sn -vv		Обнаружение Arp только в локальной сети, без сканирования портов
nmap -iR 10 -sn -traceroute		Трассировка на случайные цели, без сканирования портов
nmap 192.168.1.1-50 -sL --dns-server 192.168.1.1		Запрос внутреннего DNS для хостов, список целей только