NMAP Script Engine (NSE)

Расширение функционала за счет LUA скриптов. Запуск всех скриптов в соответствии с правилами внутри:

```
nmap -sC <target>
```

Размещение скриптов

/usr/share/nmap/scripts Можно вывести названия скриптов командой

```
ls /usr/share/nmap/scripts/
```

Типы скриптов

Количество выполняемых скриптов зависит от правил хоста или порта для этих скриптов.

auth	Скрипты, связанные с авторизацией пользователя
broadcast	Широковещательные запросы
brute	Брутфорс паролей
default	Скрипты, выполняемые по умолчанию
discovery	Поиск хостов и сервисов
dos	Атака dos
exploit	Скрипты, использующие уязвимости для атаки
external	Зависящие от каких-либо сервисов
fuzzer	Генераторы случайных последовательностей
intrusive	Могут уронить или сгенерировать большой сетевой трафик
malware	Скрипты, связанные с обнаружением вредоносных программ
safe	Безопасные

version	Определение версий
vuln	Скрипты, связанные с уязвимостями в системе безопасности

Некоторые скрипты требуют настройки.

nmap --script script_name <target>	запуск определенного скрипта. Имя скрипта или путь к папке с расширениями
nmap --script http-title --script-args http.useragent="Mozilla 999" <target>	--script-args настраивает параметры скрипта
nmap -sV --script vuln <target> nmap -sV --script="version,discovery" <target>	Определенная категория
nmap -sV --script "not exploit" <target>	Исключая категорию
nmap -sV --script "(http-*) and not(http-slowloris or http-brute)" <target>	

Трассировка выполнения скрипта

nmap -sC --script-trace <target>	Простая трассировка
-d[1-9]	Увеличение уровня выводимых сообщений

Добавление нового скрипта:

- скопировать скрипт в /scripts в директории установки nmap
- обновить базу

```
nmap --script-updatedb
```

Либо указать путь напрямую

```
nmap --script /root/loot/nonofficial.nse <target>
```

Библиотека скриптов вне основной поставки

Скрипты в поставке

Броадкастовые скрипты

broadcast-avahi-dos	Ищет хосты через DNS service discovery protocol и отправляет NULL UDP пакеты каждому найденному для проверки возможности DOS
broadcast-db2-discover	Ищет DB2 серверы через запрос на 523/udp

broadcast-dhcp-discover	Поиск DHCP сервера с использованием статического адреса DE:AD:CO:DE:CA:FE
broadcast-dns-service-discovery	Поиск DNS серверов через DNS-SD запросы
broadcast-dropbox-listener	Прослушивает сеть и ждет бродкастов от dropbox клиентов (раз в 20 секунд запросы)
broadcast-listener	Прослушивает сеть и ждет бродкасты. Пытается разобрать и вытащить данные.
broadcast-ms-sql-discover	Поиск Microsoft SQL серверов
broadcast-novell-locate	Поиск NCP серверов
broadcast-ping	Бродкастовый пинг с выводом IP и MAC Нужны привилегии.
broadcast-netbios-master-browser	Поиск NetBios доменов
broadcast-rip-discover	Отправляет RIPv2 запросы и определяет хосты на которых это крутится
broadcast-upnp-info	Поиск UPnP хостов
broadcast-wsdd-discover	Поиск хостов с поддержкой WS-Discovery протокола. Также определяет WCF (.NET 4.0+).
lltd-discovery	Использует Microsoft LLTD протокол для поиска хостов
targets-sniffer	Слушает сеть 10 секунд и выводит найденные адреса

Revision #5
Created 9 September 2025 13:36:47 by Admin
Updated 13 September 2025 11:13:09 by Admin