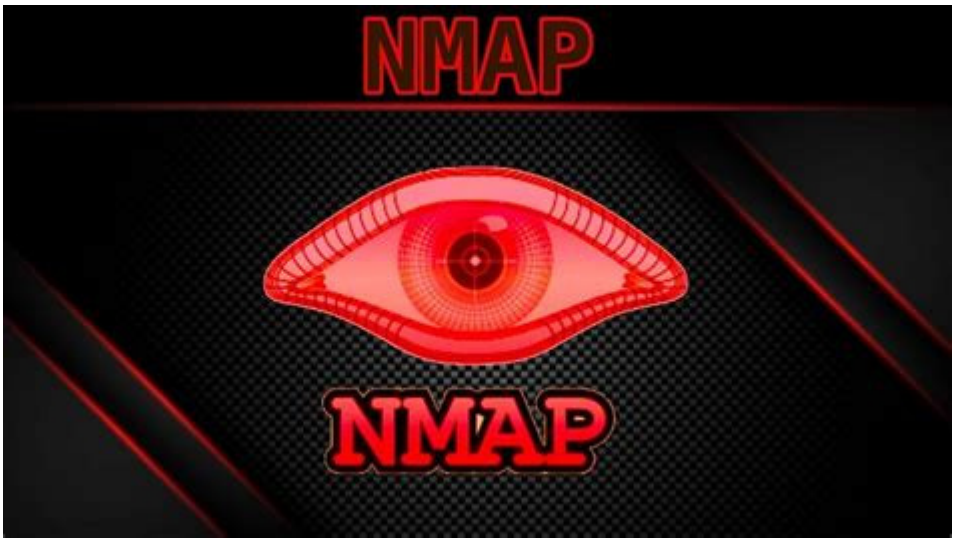
NMAP 1 часть – Telegraph

telegra.ph/NMAP-1-chast-05-07

Life-Hack - Linux/Хакинг/Хакер/ИБ/Osint May 7, 2024



Network Mapper (Nmap) — это инструмент сетевого анализа и аудита безопасности с открытым исходным кодом, написанный на C, C++, Python и Lua. Он предназначен для сканирования сетей и определения доступных в сети хостов, а также служб и приложений, включая имя и версию. Он также может идентифицировать операционную систему этих хостов. Помимо других функций, Nmap также предлагает возможности сканирования, которые могут определить, настроены ли фильтры пакетов, межсетевые экраны или системы обнаружения вторжений (IDS) необходимым образом.

Nmap является одним из наиболее часто используемых инструментов, среди сетевых администраторов и специалистов по информационной безопасности. Он используется для:

- Аудита аспектов безопасности сетей;
- Тестирования на проникновение;
- Проверки настроек и конфигурации брандмауэра и IDS;
- Отображения сети;
- Анализа ответов сетевых устройств;
- Определения открытых портов;
- Оценки защищенности сетевых устройств;

Nmap предлагает множество различных типов сканирования, которые можно использовать для получения различных результатов о наших целях. По сути, Nmap применяет следующие методы сканирования:

- Host discovery
- Port scanning
- Service enumeration and detection

- OS detection
- Scriptable interaction with the target service (Nmap Scripting Engine)

Синтаксис Nmap довольно прост и выглядит следующим образом:

```
nmap <scan types> <options> <target>
```

Например, сканирование TCP-SYN (-sS) является одним из параметров по умолчанию, если мы не определили иное, а также одним из самых популярных методов сканирования. Этот метод сканирования позволяет сканировать несколько тысяч портов в секунду. Сканирование TCP-SYN отправляет один пакет с флагом SYN и, следовательно, никогда не завершает трехстороннее подтверждение связи, в результате чего не устанавливается полное TCP-соединение со сканируемым портом.

Если Nmap получает пакет с флагом SYN-ACK, он принимает решение, что порт открыт.

Если в пакете содержится флаг RST, это индикатор того, что порт закрыт.

Если Nmap не получит пакет обратно, он отобразит его как отфильтрованный. В зависимости от конфигурации брандмауэра некоторые пакеты могут быть отброшены или проигнорированы.

Разберем такой пример:

```
$ sudo nmap -sS localhost

Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-12 22:50 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000010s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
5432/tcp open  postgresql
5901/tcp open  vnc-1

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

Мы видим, что у нас открыты четыре разных TCP-порта. В первом столбце мы видим номер порта. Затем во втором столбце мы видим статус службы, а в третьем - тип этой службы.

Например, когда нам нужно провести сканирование сети, мы должны иметь представление о том, какие устройства находятся в этой сети. Существует множество опций, с помощью которых Nmap определит жива наша цель или нет. Самый эффективный метод обнаружения хоста — использование эхо-запросов ICMP.

Всегда рекомендуется сохранять каждое сканирование. Позже это можно будет использовать для сравнения, документирования и составления отчетов. Ведь разные инструменты могут давать разные результаты.

```
$ sudo nmap 10.129.2.0/24 -sn -oA tnet | grep for | cut -d" " -f5

10.129.2.4
10.129.2.10
10.129.2.11
10.129.2.18
10.129.2.19
10.129.2.20
10.129.2.28
```

Здесь 10.129.2.0/24 - целевая сеть, -sn - запрет сканирования портов, -oA tnet - указание сохранить результаты во всех форматах, с именем 'tnet'.