NMAP 2 часть – Telegraph

telegra.ph/NMAP-2-chast-05-07

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

Во время тестирования на проникновение, нередко предоставляют список IP-адресов с хостами, которые нам нужно протестировать. Nmap имеет возможность работать со списками, вместо того, чтобы вручную вводить их.

Такой список может выглядеть примерно так:

```
$ cat hosts.lst

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
```

Для сканирования предопределенного списка, команда будет выглядеть так:

```
$ sudo nmap -sn -oA tnet -iL hosts.lst | grep for | cut -d" " -f5

10.129.2.18
10.129.2.19
10.129.2.20
```

Здесь, -sn - запрет сканирования портов, -oA tnet - указание сохранить результат во всех форматах, с именем 'tnet', -iL - провести сканирование целей, указанных в списке 'hosts.lst'.

В этом примере мы видим, что активны только 3 хоста из 7. Это может означать, что другие хосты игнорируют эхо-запросы ICMP по умолчанию из-за настроек их брандмауэра. Поскольку Nmap не получает ответа, он помечает эти хосты как

неактивные.

Если нужно просканировать только небольшую часть сети, можно указать несколько IP-адресов.

```
$ sudo nmap -sn -oA tnet 10.129.2.18 10.129.2.19 10.129.2.20| grep for | cut -d" "
-f5

10.129.2.18
10.129.2.19
10.129.2.20
```

Или так:

```
$ sudo nmap -sn -oA tnet 10.129.2.18-20| grep for | cut -d" " -f5

10.129.2.18
10.129.2.19
10.129.2.20
```

По умолчанию Nmap сканирует 1000 популярных TCP-портов с помощью сканирования SYN (-sS). Для этого сканирования необходимы права пользователя root, поскольку для создания сырых TCP-пакетов необходимы разрешения сокета. В противном случае выполняется сканирование TCP (-sT). Если мы не определяем порты и методы сканирования, эти параметры устанавливаются автоматически. Мы можем определить порты один за другим (-p 22,25,80,139,445), или в виде диапазона (-p 22-445), по популярности (--top-ports=10). Для сканирования всех портов применяется параметр -p-, а для быстрого сканирования, которое содержит 100 самых популярных портов -F.

```
$ sudo nmap 10.129.2.28 --top-ports=10

Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-15 15:36 CEST
Nmap scan report for 10.129.2.28
Host is up (0.021s latency).

PORT     STATE    SERVICE
21/tcp   closed   ftp
22/tcp   open     ssh
23/tcp   closed   telnet
25/tcp   open     smtp
80/tcp   open     http
110/tcp  open     pop3
139/tcp  filtered netbios-ssn
443/tcp  closed   https
445/tcp  filtered microsoft-ds
3389/tcp closed   ms-wbt-server
MAC Address: DE:AD:00:00:BE:EF (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
```

Здесь, 10.129.2.28 - цель, --top-ports=10 - сканировать 10 самых популярных портов.

```
$ sudo nmap 10.129.2.28 -p 21 --packet-trace -Pn -n --disable-arp-ping

Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-15 15:39 CEST
SENT (0.0429s) TCP 10.10.14.2:63090 > 10.129.2.28:21 S ttl=56 id=57322 iplen=44
seq=1699105818 win=1024 <mss 1460>
RCVD (0.0573s) TCP 10.129.2.28:21 > 10.10.14.2:63090 RA ttl=64 id=0 iplen=40
seq=0 win=0
Nmap scan report for 10.11.1.28
Host is up (0.014s latency).

PORT   STATE  SERVICE
21/tcp closed ftp
MAC Address: DE:AD:00:00:BE:EF (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

В данном примере 10.129.2.28 - целевой хост, -p 21 - порт для сканирования, --packet-trace - указание, показать все отправленные и принятые пакеты, -n - запрет DNS resolution, --disable-arp-ping - запрет ARP.

Некоторые системные администраторы иногда забывают фильтровать порты UDP. Поскольку UDP является протоколом без сохранения состояния и не требует трехстороннего рукопожатия, мы не получаем никакого подтверждения. Следовательно, время ожидания намного больше, что делает сканирование UDP (-sU) намного медленнее, чем сканирование TCP (-sS).

Давайте на примере рассмотрим, как может выглядеть UDP-сканирование (-sU) и какие результаты оно нам дает.

```
$ sudo nmap 10.129.2.28 -F -sU

Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-15 16:01 CEST
Nmap scan report for 10.129.2.28
Host is up (0.059s latency).
Not shown: 95 closed ports
PORT     STATE         SERVICE
68/udp   open|filtered dhcpc
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
631/udp  open|filtered ipp
5353/udp open          zeroconf
MAC Address: DE:AD:00:00:BE:EF (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 98.07 seconds
```

Здесь, 10.129.2.28 - цель, -F - сканирование 100 самых популярных портов, -sU - UDP сканирование.

Еще один удобный метод сканирования портов — опция -sV, которая используется для получения дополнительной доступной информации об открытых портах. Этот метод может определять версии, имена сервисов и подробную информацию о цели.

```
$ sudo nmap 10.129.2.28 -Pn -n --disable-arp-ping --packet-trace -p 445 --reason
-sV

Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-04 11:10 GMT
SENT (0.3426s) TCP 10.10.14.2:44641 > 10.129.2.28:445 S ttl=55 id=43401 iplen=44
seq=3589068008 win=1024 <mss 1460>
RCVD (0.3556s) TCP 10.129.2.28:445 > 10.10.14.2:44641 SA ttl=63 id=0 iplen=44
seq=2881527699 win=29200 <mss 1337>
NSOCK INFO [0.4980s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.4980s] nsock_connect_tcp(): TCP connection requested to
10.129.2.28:445 (IOD #1) EID 8
NSOCK INFO [0.5130s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for
EID 8 [10.129.2.28:445]
Service scan sending probe NULL to 10.129.2.28:445 (tcp)
NSOCK INFO [0.5130s] nsock_read(): Read request from IOD #1 [10.129.2.28:445]
(timeout: 6000ms) EID 18
NSOCK INFO [6.5190s] nsock_trace_handler_callback(): Callback: READ TIMEOUT for
EID 18 [10.129.2.28:445]
Service scan sending probe SMBProgNeg to 10.129.2.28:445 (tcp)
NSOCK INFO [6.5190s] nsock_write(): Write request for 168 bytes to IOD #1 EID 27
[10.129.2.28:445]
NSOCK INFO [6.5190s] nsock_read(): Read request from IOD #1 [10.129.2.28:445]
(timeout: 5000ms) EID 34
NSOCK INFO [6.5190s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for
EID 27 [10.129.2.28:445]
NSOCK INFO [6.5320s] nsock_trace_handler_callback(): Callback: READ SUCCESS for
EID 34 [10.129.2.28:445] (135 bytes)
Service scan match (Probe SMBProgNeg matched with SMBProgNeg line 13836):
10.129.2.28:445 is netbios-ssn.  Version: |Samba smbd|3.X - 4.X|workgroup:
WORKGROUP|
NSOCK INFO [6.5320s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
Nmap scan report for 10.129.2.28
Host is up, received user-set (0.013s latency).

PORT    STATE SERVICE     REASON         VERSION
445/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
Service Info: Host: Ubuntu

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.55 seconds
```

Здесь, -Pn - запрет ICMP Echo запросов, -n - запрет DNS resolution, --disable-arp-ping - запрет ARP, --packet-trace - указание, показать все отправленные и принятые пакеты, -p 445 - целевой порт, --reason - показать причину состояния порта, -sV - провести сканирование сервиса.