

探测行为选项实战 实验步骤

探测行为选项基础命令实践

1、--min-hostgroup

```
(root@kali)-[~]
# nmap --min-hostgroup 30 192.168.203.1/24
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 10:06 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.0056s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.203.2
Host is up (0.00017s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    filtered domain
MAC Address: 00:50:56:ED:7E:35 (VMware)

Nmap scan report for 192.168.203.254
Host is up (0.000087s latency).
All 1000 scanned ports on 192.168.203.254 are filtered
MAC Address: 00:50:56:E1:18:ED (VMware)

Nmap scan report for 192.168.203.131
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.203.131 are closed

Nmap done: 256 IP addresses (4 hosts up) scanned in 8.25 seconds
```

调整并行扫描组的大小进行探测

2、--min-parallelism

```
(root@kali)-[~]
# nmap --min-parallelism 100 192.168.203.1/24
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 10:08 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.0033s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.203.2
Host is up (0.00025s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    filtered domain
MAC Address: 00:50:56:ED:7E:35 (VMware)

Nmap scan report for 192.168.203.254
Host is up (0.00018s latency).
All 1000 scanned ports on 192.168.203.254 are filtered
MAC Address: 00:50:56:E1:18:ED (VMware)

Nmap scan report for 192.168.203.131
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.203.131 are closed

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.27 seconds
```

调整探测报文的并行度

3、--initial-rtt-timeout

```
(root@kali)-[~]  
# nmap --initial-rtt-timeout 1000ms 192.168.203.1  
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 10:10 CST  
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)  
Host is up (0.00074s latency).  
Not shown: 997 filtered ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
80/tcp    open  http  
3306/tcp  open  mysql  
MAC Address: 00:50:56:C0:00:08 (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 4.70 seconds
```

调整探测报文超时

4、-scan-delay

```
(root@kali)-[~]
# nmap --scan-delay 1s 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 10:27 CST
Stats: 0:02:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 6.25% done; ETC: 11:03 (0:34:15 remaining)
Stats: 0:04:37 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 12.55% done; ETC: 11:04 (0:32:03 remaining)
Stats: 0:04:38 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 12.60% done; ETC: 11:04 (0:32:01 remaining)
Stats: 0:09:51 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 26.65% done; ETC: 11:04 (0:27:04 remaining)
Stats: 0:09:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 26.70% done; ETC: 11:04 (0:27:02 remaining)
Stats: 0:14:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 39.55% done; ETC: 11:04 (0:22:17 remaining)
Stats: 0:19:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 51.80% done; ETC: 11:04 (0:17:48 remaining)
Stats: 0:19:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 51.85% done; ETC: 11:04 (0:17:47 remaining)
Stats: 0:28:30 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 77.10% done; ETC: 11:04 (0:08:28 remaining)
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00067s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2219.38 seconds
```

调整探测报文的时间间隔