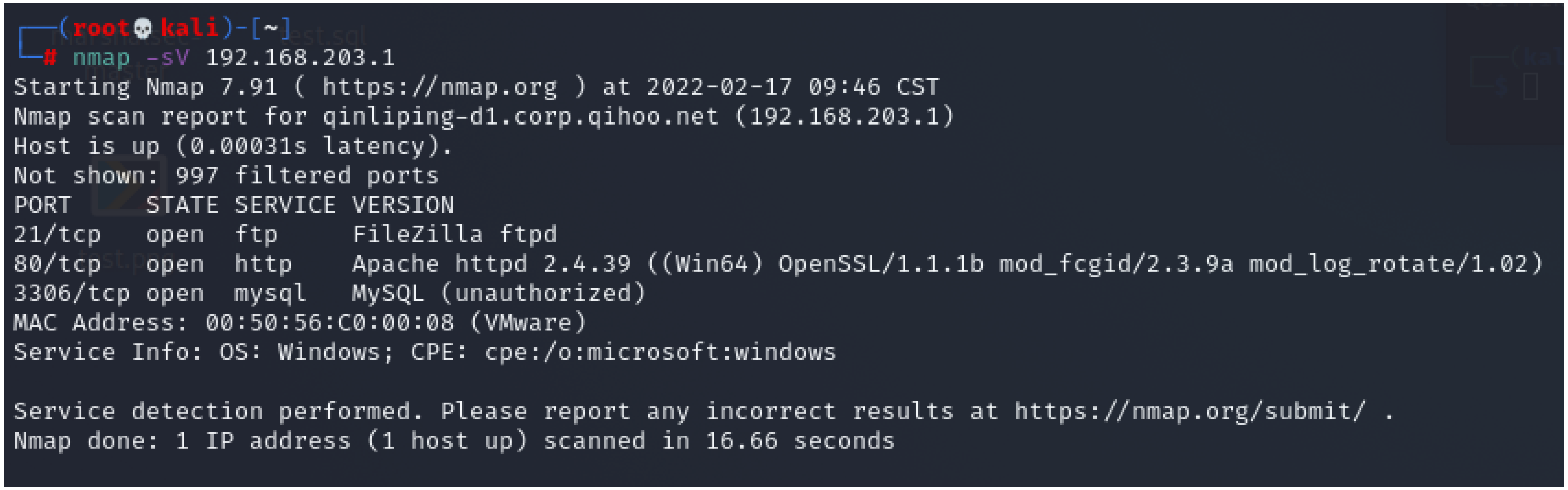
指纹探测与识别实战 实验步骤

指纹探测与识别基础命令实践

1、-sV



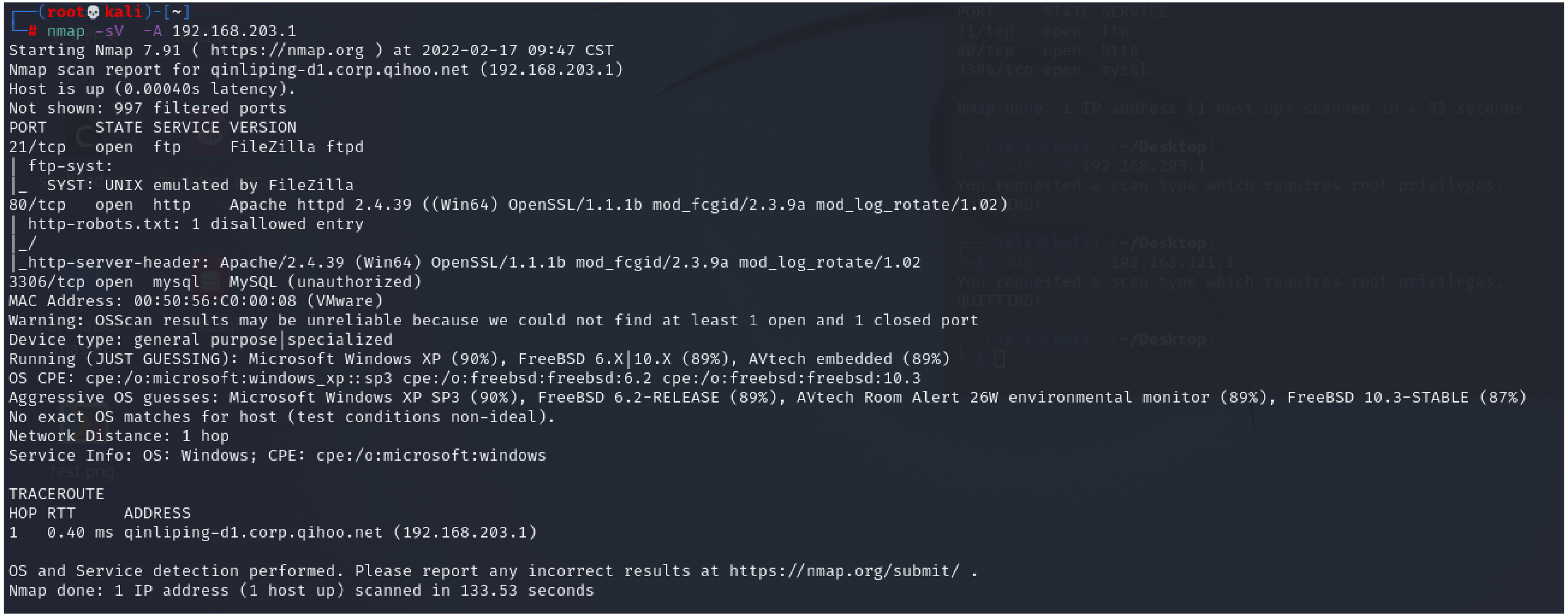
```
┌──(root💀kali)-[~]
└─# nmap -sV 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 09:46 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00031s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     FileZilla ftpd
80/tcp   open  http    Apache httpd 2.4.39 ((Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02)
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 00:50:56:C0:00:08 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.66 seconds
```

对192.168.203.1进行版本探测

结果：主机开放端口为21、80、3306且运行服务分别为ftp、http、mysql，并获取了服务版本，ftp为FileZilla ftped，http为Apache 2.4.39，但MySQL并未成功识别。然后获知主机操作系统信息——操作系统为windows。

还可以配合-A参数使用进行更加细致的操作系统探测和版本探测。

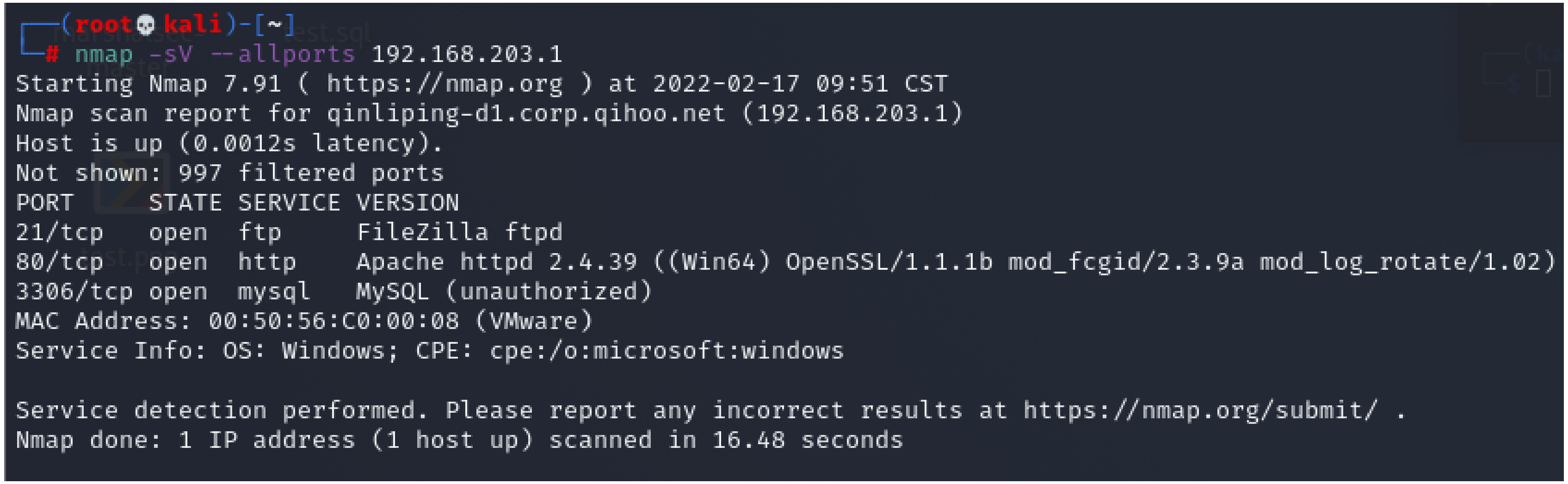


```
┌──(root💀kali)-[~]
└─# nmap -sV  -A 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 09:47 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00040s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     FileZilla ftpd
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
80/tcp   open  http    Apache httpd 2.4.39 ((Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02)
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 00:50:56:C0:00:08 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows XP (90%), FreeBSD 6.X|10.X (89%), AVtech embedded (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:freebsd:freebsd:6.2 cpe:/o:freebsd:freebsd:10.3
Aggressive OS guesses: Microsoft Windows XP SP3 (90%), FreeBSD 6.2-RELEASE (89%), AVtech Room Alert 26W environmental monitor (89%), FreeBSD 10.3-STABLE (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT     ADDRESS
1   0.40 ms qinliping-d1.corp.qihoo.net (192.168.203.1)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 133.53 seconds
```

2、--allports



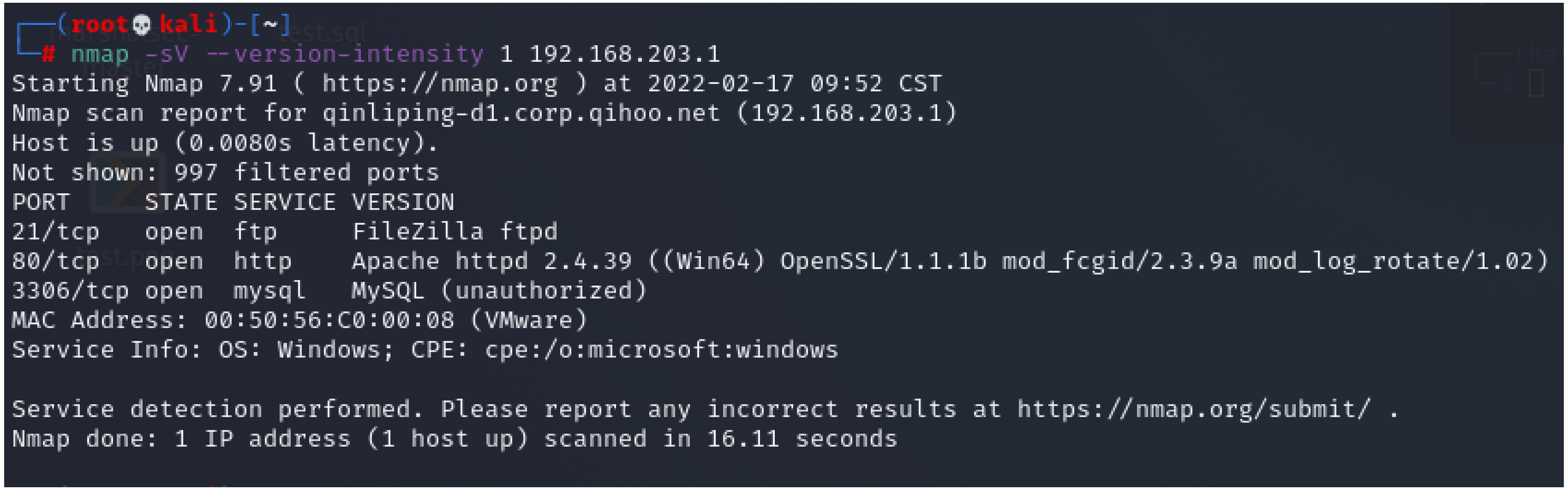
```
┌──(root💀kali)-[~]
└─# nmap -sV --allports 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 09:51 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.0012s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     FileZilla ftpd
80/tcp   open  http    Apache httpd 2.4.39 ((Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02)
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 00:50:56:C0:00:08 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.48 seconds
```

对192.168.203.1进行全端口探测

结果：主机开放端口为21、80、3306且运行服务分别为ftp、http、mysql，并获取了服务版本，ftp为FileZilla ftped，http为Apache 2.4.39，但MySQL并未成功识别，操作系统为windows。

3、--version-intensity



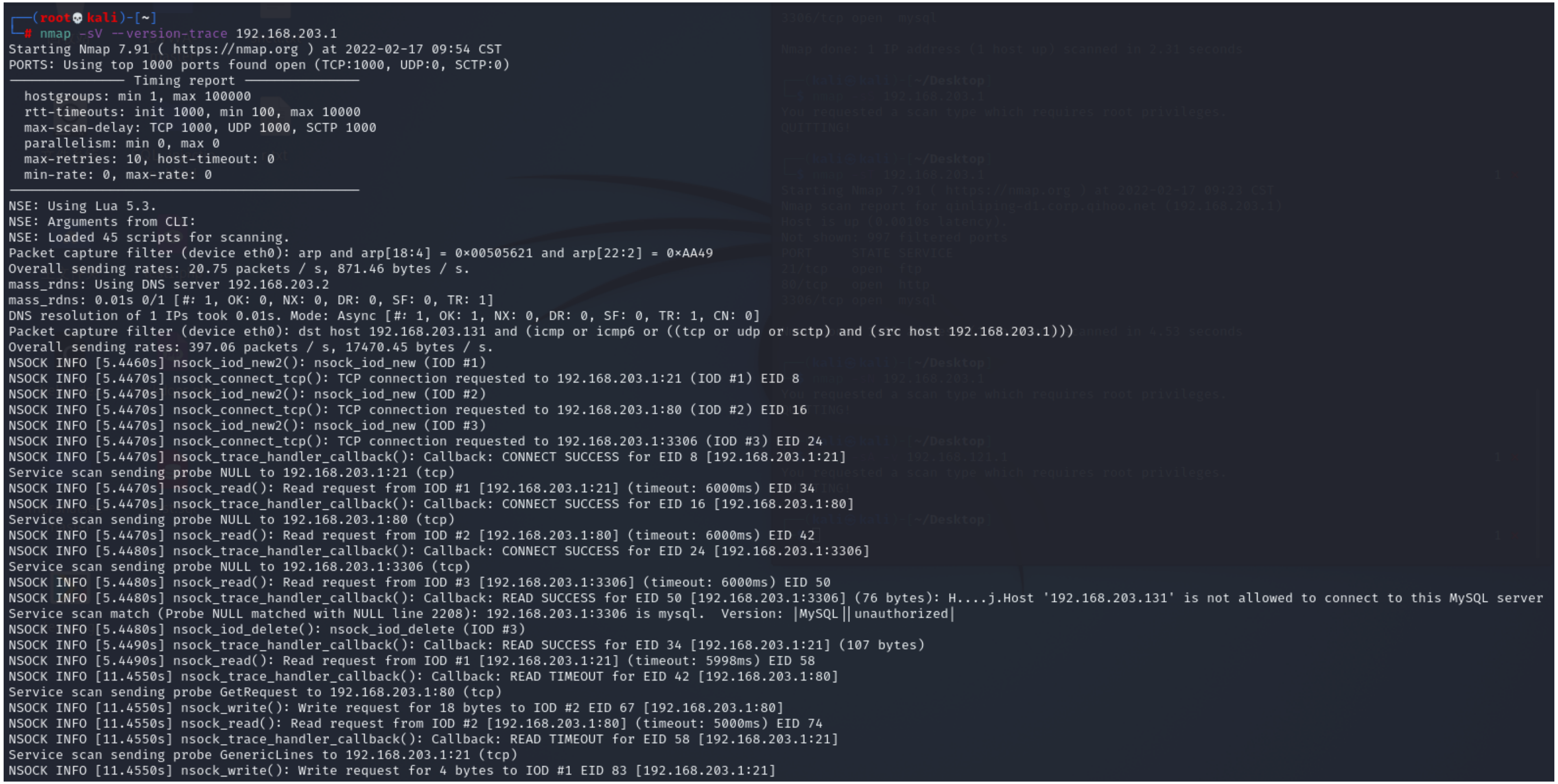
```
┌──(root💀kali)-[~]
└─# nmap -sV --version-intensity 1 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 09:52 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.0080s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     FileZilla ftpd
80/tcp   open  http    Apache httpd 2.4.39 ((Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02)
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 00:50:56:C0:00:08 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.11 seconds
```

对192.168.203.1进行强度为1的探测

结果：主机开放端口为21、80、3306且运行服务分别为ftp、http、mysql，并获取了服务版本，ftp为FileZilla ftped，http为Apache 2.4.39，但MySQL并未成功识别，操作系统为windows。

4、--version-trace

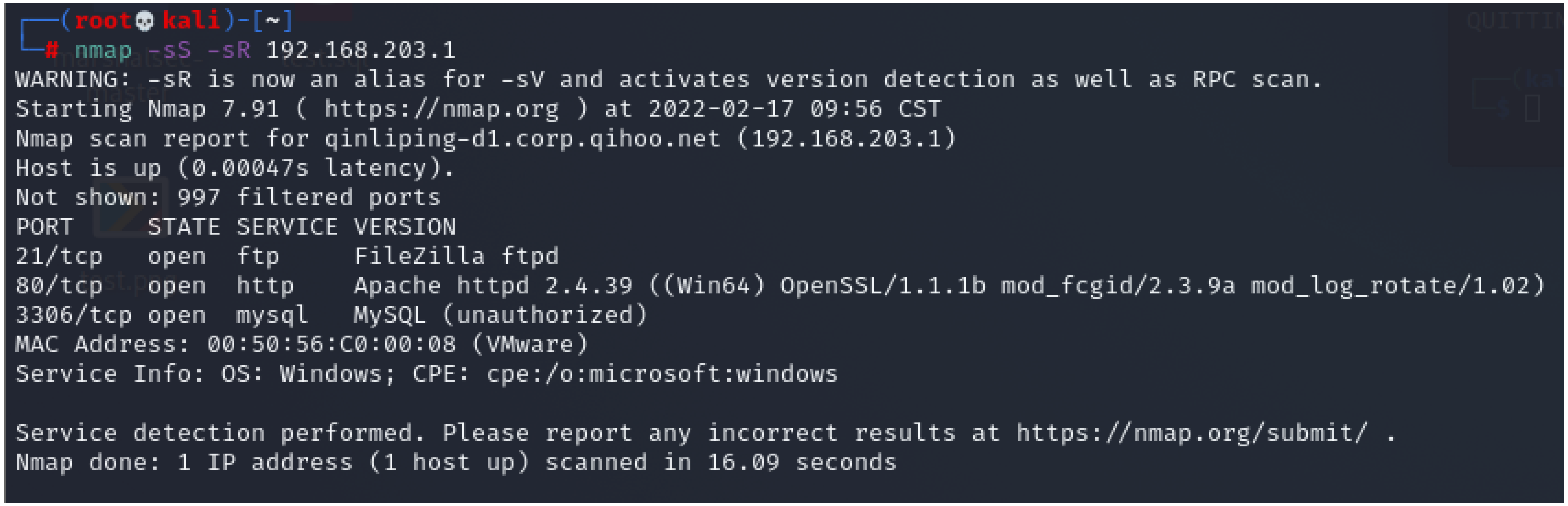


```
┌──(root💀kali)-[~]
└─# nmap -sV --version-trace 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 09:54 CST
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
─────────────── Timing report ───────────────
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
─────────────────────────────────────────────

NSE: Using Lua 5.3.
NSE: Arguments from CLI:
NSE: Loaded 45 scripts for scanning.
Packet capture filter (device eth0): arp and arp[18:4] = 0×00505621 and arp[22:2] = 0×AA49
Overall sending rates: 20.75 packets / s, 871.46 bytes / s.
mass_rdns: Using DNS server 192.168.203.2
mass_rdns: 0.01s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Packet capture filter (device eth0): dst host 192.168.203.131 and (icmp or icmp6 or ((tcp or udp or sctp) and (src host 192.168.203.1)))
Overall sending rates: 397.06 packets / s, 17470.45 bytes / s.
NSOCK INFO [5.4460s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [5.4470s] nsock_connect_tcp(): TCP connection requested to 192.168.203.1:21 (IOD #1) EID 8
NSOCK INFO [5.4470s] nsock_iod_new2(): nsock_iod_new (IOD #2)
NSOCK INFO [5.4470s] nsock_connect_tcp(): TCP connection requested to 192.168.203.1:80 (IOD #2) EID 16
NSOCK INFO [5.4470s] nsock_iod_new2(): nsock_iod_new (IOD #3)
NSOCK INFO [5.4470s] nsock_connect_tcp(): TCP connection requested to 192.168.203.1:3306 (IOD #3) EID 24
NSOCK INFO [5.4470s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [192.168.203.1:21]
Service scan sending probe NULL to 192.168.203.1:21 (tcp)
NSOCK INFO [5.4470s] nsock_read(): Read request from IOD #1 [192.168.203.1:21] (timeout: 6000ms) EID 34
NSOCK INFO [5.4470s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 16 [192.168.203.1:80]
Service scan sending probe NULL to 192.168.203.1:80 (tcp)
NSOCK INFO [5.4470s] nsock_read(): Read request from IOD #2 [192.168.203.1:80] (timeout: 6000ms) EID 42
NSOCK INFO [5.4480s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 24 [192.168.203.1:3306]
Service scan sending probe NULL to 192.168.203.1:3306 (tcp)
NSOCK INFO [5.4480s] nsock_read(): Read request from IOD #3 [192.168.203.1:3306] (timeout: 6000ms) EID 50
NSOCK INFO [5.4480s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 50 [192.168.203.1:3306] (76 bytes): H....j.Host '192.168.203.131' is not allowed to connect to this MySQL server
Service scan match (Probe NULL matched with NULL line 2208): 192.168.203.1:3306 is mysql.  Version: |MySQL||unauthorized|
NSOCK INFO [5.4480s] nsock_iod_delete(): nsock_iod_delete (IOD #3)
NSOCK INFO [5.4490s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 34 [192.168.203.1:21] (107 bytes)
NSOCK INFO [5.4490s] nsock_read(): Read request from IOD #1 [192.168.203.1:21] (timeout: 5998ms) EID 58
NSOCK INFO [11.4550s] nsock_trace_handler_callback(): Callback: READ TIMEOUT for EID 42 [192.168.203.1:80]
Service scan sending probe GetRequest to 192.168.203.1:80 (tcp)
NSOCK INFO [11.4550s] nsock_write(): Write request for 18 bytes to IOD #2 EID 67 [192.168.203.1:80]
NSOCK INFO [11.4550s] nsock_read(): Read request from IOD #2 [192.168.203.1:80] (timeout: 5000ms) EID 74
NSOCK INFO [11.4550s] nsock_trace_handler_callback(): Callback: READ TIMEOUT for EID 58 [192.168.203.1:21]
Service scan sending probe GenericLines to 192.168.203.1:21 (tcp)
NSOCK INFO [11.4550s] nsock_write(): Write request for 4 bytes to IOD #1 EID 83 [192.168.203.1:21]
```

对192.168.203.1进行探测，并期望获详细的版本信息

5、-sR



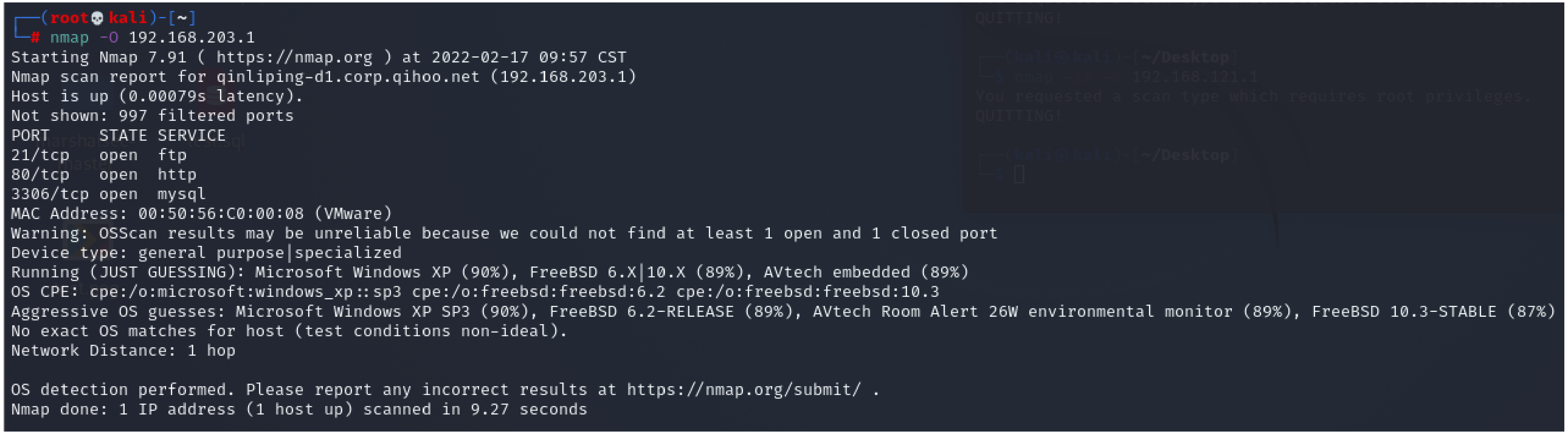
```
┌──(root💀kali)-[~]
└─# nmap -sS -sR 192.168.203.1
WARNING: -sR is now an alias for -sV and activates version detection as well as RPC scan.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 09:56 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00047s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     FileZilla ftpd
80/tcp   open  http    Apache httpd 2.4.39 ((Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02)
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 00:50:56:C0:00:08 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.09 seconds
```

对192.168.203.1进行RPC扫描

结果：结果：主机开放端口为21、80、3306且运行服务分别为ftp、http、mysql，并获取了服务版本，ftp为FileZilla ftped，http为Apache 2.4.39，但MySQL并未成功识别，操作系统为windows。

6、-O



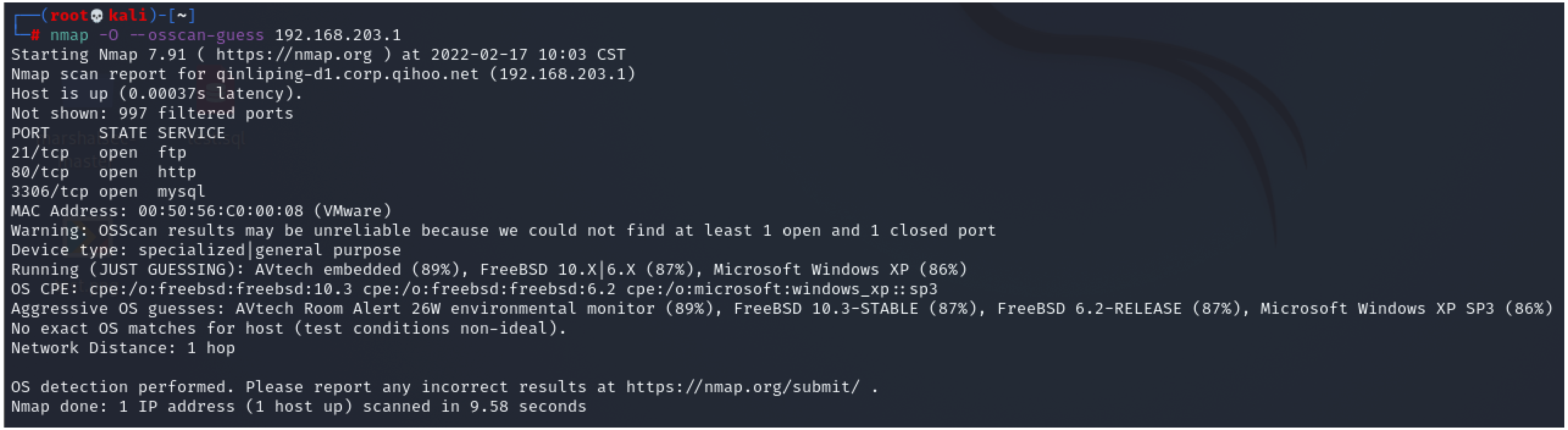
```
┌──(root💀kali)-[~]
└─# nmap -O 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 09:57 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00079s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 00:50:56:C0:00:08 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows XP (90%), FreeBSD 6.X|10.X (89%), AVtech embedded (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:freebsd:freebsd:6.2 cpe:/o:freebsd:freebsd:10.3
Aggressive OS guesses: Microsoft Windows XP SP3 (90%), FreeBSD 6.2-RELEASE (89%), AVtech Room Alert 26W environmental monitor (89%), FreeBSD 10.3-STABLE (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.27 seconds
```

对192.168.203.1进行主机操作系统探测

结果：结果并不准确，因为目标机为windows10的操作系统，而其给出的可能性中并没有windows10操作系统。随着操作系统的迭代，在有防火墙的情况下对于主机操作系统的信息搜集难度也在增加。

7、--osscan-guess



```
┌──(root💀kali)-[~]
└─# nmap -O --osscan-guess 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 10:03 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00037s 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)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|general purpose
Running (JUST GUESSING): AVtech embedded (89%), FreeBSD 10.X|6.X (87%), Microsoft Windows XP (86%)
OS CPE: cpe:/o:freebsd:freebsd:10.3 cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (89%), FreeBSD 10.3-STABLE (87%), FreeBSD 6.2-RELEASE (87%), Microsoft Windows XP SP3 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.58 seconds
```

对192.168.203.1进行主机操作系统探测，且进行大胆猜测。

结果：结果并不准确，因为目标机为windows10的操作系统，而其给出的可能性中并没有windows10操作系统。随着操作系统的迭代，在有防火墙的情况下对于主机操作系统的信息搜集难度也在增加。