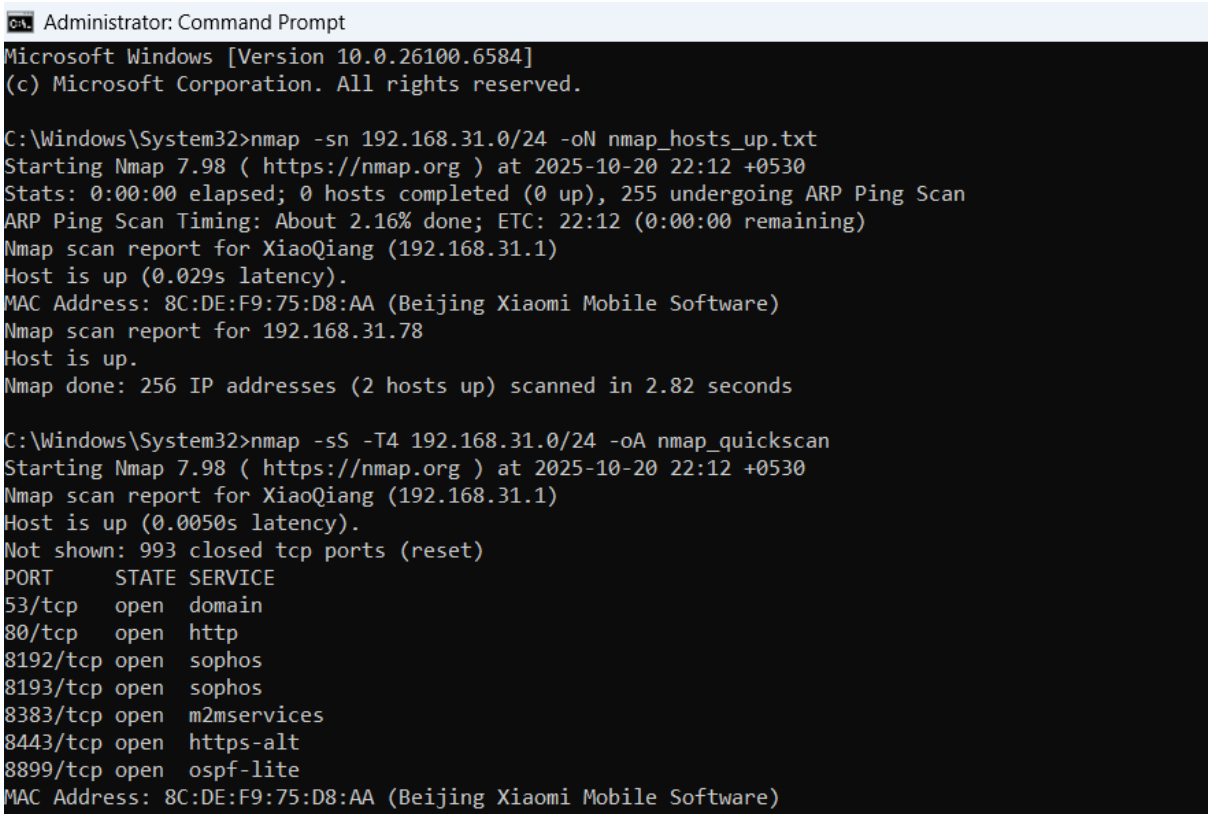
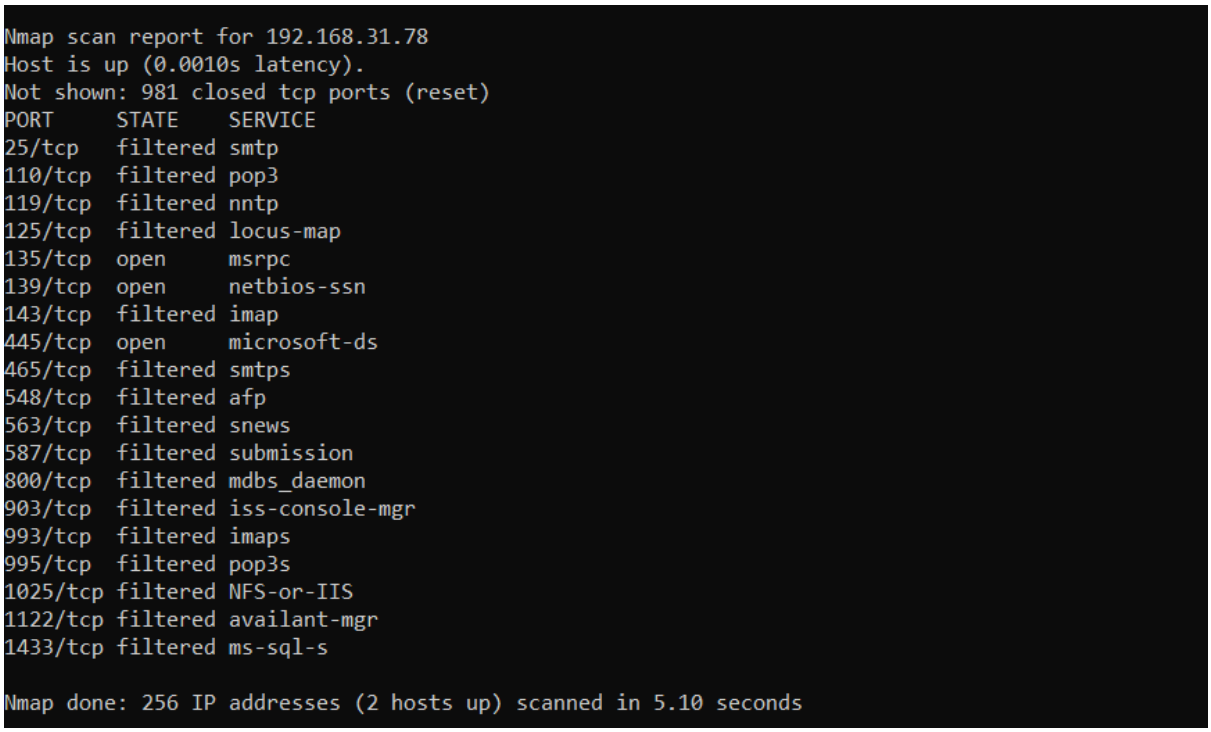
Nmap captures



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.26100.6584]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>nmap -sn 192.168.31.0/24 -oN nmap_hosts_up.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-20 22:12 +0530
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 2.16% done; ETC: 22:12 (0:00:00 remaining)
Nmap scan report for XiaoQiang (192.168.31.1)
Host is up (0.029s latency).
MAC Address: 8C:DE:F9:75:D8:AA (Beijing Xiaomi Mobile Software)
Nmap scan report for 192.168.31.78
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.82 seconds

C:\Windows\System32>nmap -sS -T4 192.168.31.0/24 -oA nmap_quickscan
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-20 22:12 +0530
Nmap scan report for XiaoQiang (192.168.31.1)
Host is up (0.0050s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
8192/tcp open  sophos
8193/tcp open  sophos
8383/tcp open  m2mservices
8443/tcp open  https-alt
8899/tcp open  ospf-lite
MAC Address: 8C:DE:F9:75:D8:AA (Beijing Xiaomi Mobile Software)
```



```
Nmap scan report for 192.168.31.78
Host is up (0.0010s latency).
Not shown: 981 closed tcp ports (reset)
PORT     STATE    SERVICE
25/tcp   filtered smtp
110/tcp  filtered pop3
119/tcp  filtered nntp
125/tcp  filtered locus-map
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
143/tcp  filtered imap
445/tcp  open     microsoft-ds
465/tcp  filtered smtps
548/tcp  filtered afp
563/tcp  filtered snews
587/tcp  filtered submission
800/tcp  filtered mdbs_daemon
903/tcp  filtered iss-console-mgr
993/tcp  filtered imaps
995/tcp  filtered pop3s
1025/tcp filtered NFS-or-IIS
1122/tcp filtered availant-mgr
1433/tcp filtered ms-sql-s

Nmap done: 256 IP addresses (2 hosts up) scanned in 5.10 seconds
```

```
C:\Windows\System32>nmap -sS -sV -T4 --top-ports 200 192.168.31.78 -oN nmap_self_top200.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-20 22:12 +0530
Nmap scan report for 192.168.31.78
Host is up (0.00082s latency).
Not shown: 186 closed tcp ports (reset)
PORT     STATE    SERVICE       VERSION
25/tcp   filtered smtp
110/tcp  filtered pop3
119/tcp  filtered nntp
135/tcp  open     msrpc         Microsoft Windows RPC
139/tcp  open     netbios-ssn   Microsoft Windows netbios-ssn
143/tcp  filtered imap
445/tcp  open     microsoft-ds?
465/tcp  filtered smtps
548/tcp  filtered afp
587/tcp  filtered submission
993/tcp  filtered imaps
995/tcp  filtered pop3s
1025/tcp filtered NFS-or-IIS
1433/tcp filtered ms-sql-s
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 8.48 seconds
```

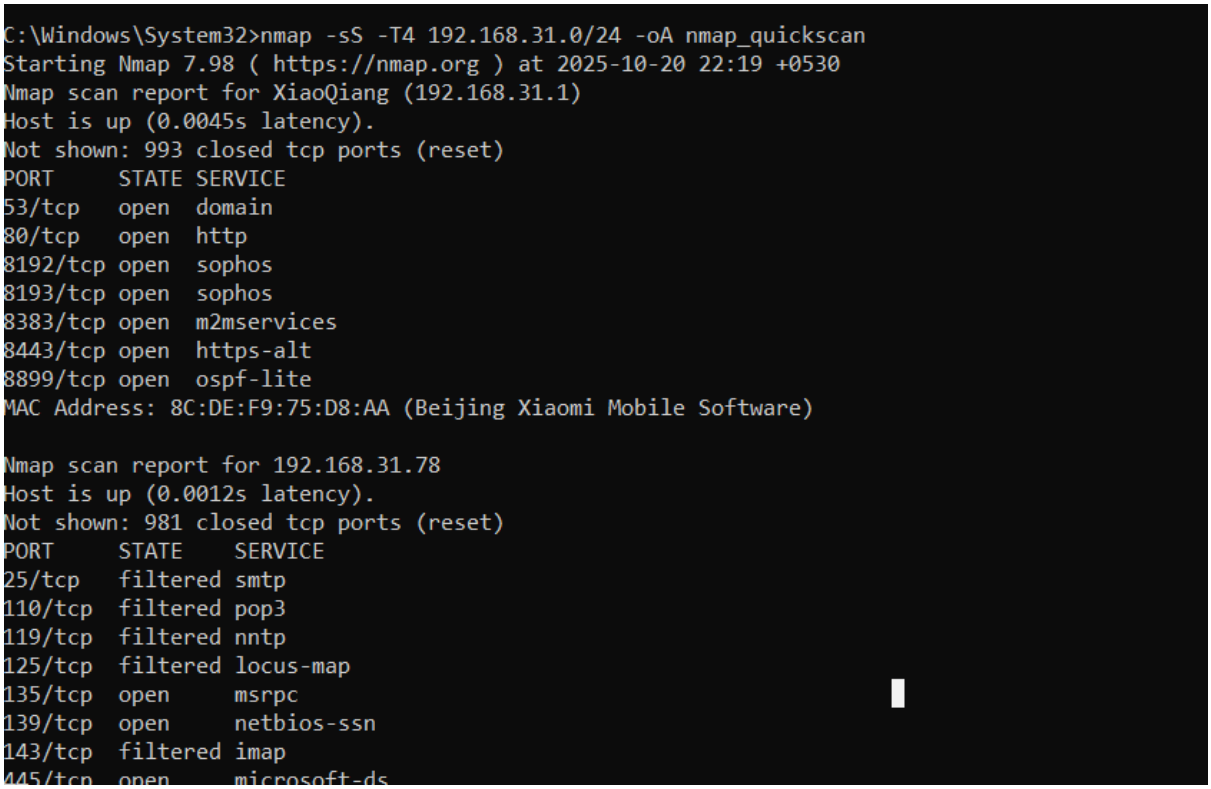
```
C:\Windows\System32>nmap -sS -sV --script=vuln 192.168.31.1 -oN nmap_router_vuln.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-20 22:13 +0530
Nmap scan report for XiaoQiang (192.168.31.1)
Host is up (0.0052s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
53/tcp   open  domain  dnsmasq 2018.a
80/tcp   open  http    nginx
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
8192/tcp open  http    nginx
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-cookie-flags:
|   /:
|     JSESSIONID:
|_      httponly flag not set
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| http-aspnet-debug:
|_  status: DEBUG is enabled
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
| http-enum:
|_  /blog/: Blog
| http-vuln-cve2010-0738:
|_  /jmx-console/: Authentication was not required
|_http-trane-info: Problem with XML parsing of /evox/about
8193/tcp open  http    nginx
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-csrf: Couldn't find any CSRF vulnerabilities.
```

```
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
8383/tcp open  http    nginx
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
8443/tcp open  http    nginx
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
8899/tcp open  http    nginx
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
MAC Address: 8C:DE:F9:75:D8:AA (Beijing Xiaomi Mobile Software)
```

```
C:\Windows\System32>nmap -Pn -sS -T4 192.168.31.0/24 -oN nmap_no_ping.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-20 22:22 +0530
Nmap scan report for XiaoQiang (192.168.31.1)
Host is up (0.0066s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
8192/tcp open  sophos
8193/tcp open  sophos
8383/tcp open  m2mservices
8443/tcp open  https-alt
8899/tcp open  ospf-lite
MAC Address: 8C:DE:F9:75:D8:AA (Beijing Xiaomi Mobile Software)

Nmap scan report for 192.168.31.78
Host is up (0.0012s latency).
Not shown: 981 closed tcp ports (reset)
PORT     STATE    SERVICE
25/tcp   filtered smtp
110/tcp  filtered pop3
119/tcp  filtered nntp
125/tcp  filtered locus-map
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
143/tcp  filtered imap
445/tcp  open     microsoft-ds
465/tcp  filtered smtps
548/tcp  filtered afp
563/tcp  filtered snews
587/tcp  filtered submission
800/tcp  filtered mdbs_daemon
903/tcp  filtered iss-console-mgr
993/tcp  filtered imaps
995/tcp  filtered pop3s
1025/tcp filtered NFS-or-IIS
1122/tcp filtered availant-mgr
1433/tcp filtered ms-sql-s

Nmap done: 256 IP addresses (2 hosts up) scanned in 5.32 seconds
```


C:\Windows\System32>nmap -sS -T4 192.168.31.0/24 -oA nmap_quickscan
Starting Nmap 7.98 (https://nmap.org) at 2025-10-20 22:19 +0530
Nmap scan report for XiaoQiang (192.168.31.1)
Host is up (0.0045s latency).
Not shown: 993 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
80/tcp open http
8192/tcp open sophos
8193/tcp open sophos
8383/tcp open m2mservices
8443/tcp open https-alt
8899/tcp open ospf-lite
MAC Address: 8C:DE:F9:75:D8:AA (Beijing Xiaomi Mobile Software)
Nmap scan report for 192.168.31.78
Host is up (0.0012s latency).
Not shown: 981 closed tcp ports (reset)
PORT STATE SERVICE
25/tcp filtered smtp
110/tcp filtered pop3
119/tcp filtered nntp
125/tcp filtered locus-map
135/tcp open msrpc
139/tcp open netbios-ssn
143/tcp filtered imap
445/tcp open microsoft-ds