

--	--	--	--	--	--

[illegible]

EX: -A -Pn

```
nmap -A -Pn {IP}
```

```
Nmap scan report for [REDACTED]
Host is up (0.018s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
80/tcp    open  http              Apache httpd 2.4.27 ((Win64) OpenSSL/1.1.0f PHP/5.6.31)
|_ http-server-header: Apache/2.4.27 (Win64) OpenSSL/1.1.0f PHP/5.6.31
|_ http-title: \xA4F\xABn\xAC\xEC\xA4j\xAE\xD5\xB6\xE9\xB8\xEA\xB0T\xA8t\xB2\xCE
| http-robots.txt: 2 disallowed entries
|_ / /*.jpg$
135/tcp   open  msrpc             Microsoft Windows RPC
139/tcp   open  netbios-ssn       Microsoft Windows netbios-ssn
443/tcp   open  ssl/http           Apache httpd 2.4.27 ((Win64) OpenSSL/1.1.0f PHP/5.6.31)
|_ http-title: \xA4F\xABn\xAC\xEC\xA4j\xAE\xD5\xB6\xE9\xB8\xEA\xB0T\xA8t\xB2\xCE
|_ ssl-cert: Subject: commonName=[REDACTED]
| Subject Alternative Name:
| Not valid before: 2024-08-16T06:26:59
|_ Not valid after: 2025-08-27T15:59:59
|_ ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|_ http/1.1
| http-robots.txt: 2 disallowed entries
|_ / /*.jpg$
|_ http-server-header: Apache/2.4.27 (Win64) OpenSSL/1.1.0f PHP/5.6.31
445/tcp   open  microsoft-ds       Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp   open  ssl/ms-wbt-server?
|_ ssl-cert: Subject: commonName=SERVER04
| Not valid before: 2024-12-28T04:59:51
|_ Not valid after: 2025-06-29T04:59:51
|_ ssl-date: 2025-05-02T08:44:37+00:00; +1s from scanner time.
49154/tcp open  msrpc             Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ nbstat: NetBIOS name: SERVER04, NetBIOS user: <unknown>, NetBIOS MAC: [REDACTED] (VMware)
| smb2-time:
| date: 2025-05-02T08:43:57
|_ start_date: 2025-03-13T04:12:50
| smb2-security-mode:
| 2:1:0:
```

--	--	--	--

```
nmap 192.168.0.* --exclude 192.168.0.100
```

■■■■■

```
nmap -iL hostlist.txt --excludefile excludelist.txt
```

■■■■■■■■■

```
nmap -sA scanme.nmap.org
```

■■■■■■■■■

```
nmap -PN scanme.nmap.org
```

■■■■■■■■(ping scan)

```
nmap -sP 140.115.35.0/24
```

```
nmap -F www.hinet.net
```

```
■■■■ ■■■■-T5■■■-T3
```

■■port■■

```
nmap -p 80,443 192.168.1.1
```

```
nmap -p 80-200 192.168.1.1
```

■■tcp■■

```
nmap -p T:80 192.168.1.1
```

■■udp■■

```
nmap -p U:53 192.168.1.1
```

■■■■10port

```
nmap --top-ports 10 192.168.1.1
```

■■■■

```
nmap -sS -P0 -sV -O 192.168.56.102
```

param:

-sS: Scan Syn

-sV: Determine OS Version

- P0: Protocol Scan
- O : Operation System

script scan

SCRIPT SCAN:

-sC: equivalent to --script=default

```
--script=<Lua scripts>: <Lua scripts> is a comma separated list of
                        directories, script-files or script-categories
```

```
--script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
```

--script-args-file=filename: provide NSE script args in a file

```
--script-trace: Show all data sent and received
```

--script-updatedb: Update the script database.

```
--script-help=<Lua scripts>: Show help about scripts.
```

<Lua scripts> is a comma-separated list of script-files or script-categories.

□□□□□□□□TLS□□

```
nmap --script ssl-enum-ciphers -p 443 {url}
```

[illegible]

```
echo 10.0.{1..254}.{1..254} >> iplist.txt
```

```
sh[ ]tls1.0-1.[ ]
```

```
#!/bin/bash
```

```
IPLIST=$(cat iplist.txt)
```

```
TLS_VER=(TLSv1.0 TLSv1.1 TLSv1.2)
```

```
SCAN_PORT="443"
```

```
NMAP_OPS="--host-timeout 3000ms --max-rtt-timeout 3000ms --script ssl-enum-ciphers -p ${SCAN_PORT}"
```

```
OUTPUT="output.csv"
```

```
for (( i = 0; i < ${#IPLIST[@]}; i++ )); do
```

```
SUP_TLS=$(nmap $NMAP_OPS ${IPLIST[i]} | egrep "${TLS_VER[0]}${TLS_VER[1]}${TLS_VER[2]}" | cut -c 5-11)
```

```
if [[ ! -z $SUP_TLS ]]; then
```

```
echo -ne "\n${IPLIST[i]}" >> $OUTPUT
```

```
for (( j = 0; j < ${#SUP_TLS[@]}; j++ )); do
    echo -n "${SUP_TLS[@]}" >> $OUTPUT
done

fi

unset SUP_TLS
done
```



[nmap](#) [TLS](#) [Ciphers](#) [Mr.](#)

Revision #5

Created 26 October 2024 09:09:34 by Ron

Updated 14 May 2025 01:21:20 by Ron