💻

Nmap

Nmap Cheat Sheet

The definitive Nmap guide for beginners and advanced users

Host discovery and identification

Basic Scanning

- Launch a Ping scan:

  `nmap -sn <target>`

- Ping scan (subnet):

  `nmap -sn <target> Ex: nmap -sn 192.168.1.0/24`

- Scan a list of targets:

  `nmap -iL <targets.txt>`

- Ping scan with traceroute:

  `nmap -sn --traceroute <target>`

- TCP SYN Ping:

  `nmap -PS <target>`

- UDP Ping:

  `nmap -PU <target>`

- Scan IPv4 target:

  `nmap -4 <target>`

- Specify NSE script:

  `nmap -sn --script <nse-script>`

- Manually assign DNS servers:

  `nmap --dns-servers <dns>`

- IPv6 Ping:

  `nmap -6 <target>`

- Specify outgoing interface:

  `nmap -e <interface> <target>`

- TCP ACK Ping:

  `nmap -PA <target>`

- No DNS resolution:

  `nmap -n <target>`

- Scan list of hosts:

  `nmap -iL <hosts.txt>`

Timing and performance

- Rate limiting:

  `nmap --scan-delay <time>`

- Adjust delay between probes:

  `nmap --min-rate <time> --max-scan-delay <time>`

- Paranoid timing template:

  `nmap -T0 <target>`

- Sneaky - Evasion (also T0):

```
nmap -T1 <target>
```

- Polite - Slower than normal scan:

```
nmap -T2 <target>
```

- Normal - Default speed:

```
nmap -T3 <target>
```

- Aggressive - Recommended mode:

```
nmap -T4 <target>
```

- Insane - Very fast networks:

```
nmap -T5 <target>
```

- Host timeouts - give up on hosts:

```
nmap --host-timeout <time>
```

Version detection

- Service detection:

```
nmap -sV <target> Ex: nmap -sV scanme.nmap.org
```

- OS detection:

```
nmap -O <target>
```

- Attempt OS guessing:

```
nmap -O --osscan-guess <target>
```

- Increasing version detection:

```
nmap -sV --version-intensity <0-9> <target>
```

- Troubleshoot version scans:

```
nmap -sV --version-trace <target>
```

- Aggressive detection mode:

  `nmap -A <target>`

- Verbose mode:

  `nmap -v <target>`

Network and port scanning

- TCP SYN ping scan:

  `nmap -sn -PS <target> or nmap -sS <target>`

- Scanning multiple ports:

  `nmap -p 5600,1000-2000 <target>`

- TCP ACK ping scan:

  `nmap -sn -PA <target> or nmap -sA <target>`

- UDP ping scan:

  `nmap -sn -PU <target>`

- ICMP ping scan:

  `nmap -sn -PE <target>`

- SCTP INIT ping scan:

  `nmap -sn -PY <target> or nmap -sY <target>`

- IP protocol ping scan (tracing):

  `nmap -sn --packet-trace <target>`

- Scan random number of hosts:

  `nmap -iR <number>`

- Broadcast pings:

`nmap --script=broadcast-ping --packet-trace`

- Xmas scan (sets the FIN, PSH, URG flags):

  `nmap -sX <target>`

- UDP scan (with verbosity):

  `nmap -sU -v <target>`

- Scan a firewall (specify TCP header to imply fragmentation):

  `nmap -f -f <target>`

- Cloak a scan with decoys:

  `nmap -D <decoy1,decoy2> <target> Ex: nmap -D Rnd:10 <target>`

- Spoof source IP address:

  `nmap -S <IP_Address> <target>`

- Spoof MAC address:

  `nmap --spoof-mac [MAC_ADDRESS] <target>`

- Scan using a random MAC address:

  `nmap -vv --iflist --spoof-mac 0 <target>`

Nmap Scripting Engine (NSE)

- Safe category - Default:

  `nmap -sC <host> Ex: nmap -sC scanme.nmap.org`

- Execute (multiple) scripts by name:

  `nmap --script <script1,script2> <target>`

- Select script by category:

  `nmap --script <category> <target>`

- Execute NSE script file:

```
nmap --script <path/to/script.nse> <target>
```

- Exclude a specific category:

```
nmap --script "not exploit" <target>
```

- Include two different categories:

```
nmap --script "default and discover" <target>
```

- Combining wildcards:

```
nmap --script "http-* <target>
```

- Set arguments:

```
nmap --script http-useragent --script-args http.useragent="Mozilla/537.36" <target>
```

- Load arguments from a file:

```
nmap --script-args-file <file> <target>
```

Scanning mail servers

- Brute-force SMTP:

```
nmap -p25 --script smtp-brute <target>
```

- Brute-force IMAP:

```
nmap -p143 --script imap-brute <target>
```

- Brute-force POP3:

```
nmap -p110 --script pop3-brute <target>
```

- Enumerate users:

```
nmap -p25 --script smtp-enum-users <target>
```

- SMTP run on alternate port(s):

`nmap -p<port> --script smtp-ntp-enum <target>`

- Discovering open relays:

  `nmap -p<port> --script smtp-open-relay <target>`

- Find available SMTP commands:

  `nmap -p25 --script smtp-commands <target>`

Scanning databases

- Identify MS SQL servers:

  `nmap -p1433 --script ms-sql-info <target>`

- Brute-force MS SQL passwords:

  `nmap -p1433 --script ms-sql-brute <target>`

- Dump password hashes (MS SQL):

  `nmap -p1433 --script ms-sql-dump-hashes <target>`

- List databases (MySQL):

  `nmap -p3306 --script mysql-databases <target>`

- Brute-force MySQL passwords:

  `nmap -p3306 --script mysql-brute <target>`

- Identify MongoDB servers:

  `nmap -p27017 --script mongodb-info <target>`

- Brute-force Redis passwords:

  `nmap -p6379 --script redis-brute <target>`

Scanning web servers

- List supported HTTP methods:

```
nmap -p80,443 --script http-methods <target>
```

- Discover interesting paths/folders:

```
nmap --script http-enum <target>
```

- Brute-forcing HTTP basic auth:

```
nmap --script http-brute <target>
```

- Provide own users/password list:

```
nmap --script http-brute --script-args userdb=users.txt,passdb=pass.txt <target>
```

- Detect a Web Application Firewall:

```
nmap -p80 --script http-waf-detect <target>
```

- Detect XST vulnerabilities (via HTTP TRACE method):

```
nmap -p80 --script http-methods --script-args http-methods.retest <target>
```

- Detect XSS vulnerabilities:

```
nmap --script http-sql-injection <target>
```

- Identify vulnerable web platforms (e.g. WordPress):

```
nmap --script http-wordpress-enum <target>
```

ICS/SCADA systems

- Detect standard (open) ports:

```
nmap -sU -p<port-list> <target>
```

- Control system ports (BACnet/IP):

```
nmap -sU -p47808 --script bacnet-info <target>
```

- Ethernet/IP:

```
nmap -p44818 --script enip-info <target>
```

- Discover a Modbus device:

  ```
  nmap -p502 --script modbus-discover <target>
  ```

- Discover a Niagara Fox device:

  ```
  nmap -p<port> --script fox-info <target>
  ```

Generating reports

- Normal output to filename:

  ```
  nmap -oN <filename> <target>
  ```

- Send results to XML format:

  ```
  nmap -oX <filename.xml> <target>
  ```

- Output to all formats (normal, XML & grep):

  ```
  nmap -oA <filename> <target>
  ```

- Increase verbosity and debugging level:

  ```
  nmap -v -d <target>
  ```

- Display host and port state reasons:

  ```
  nmap --reason <target>
  ```

- Print periodic timing stats:

  ```
  nmap --stats-every 10s <target>
  ```

- Trace packets and data sent and received:

  ```
  nmap --packet-trace <target>
  ```

- Show open ports only:

  ```
  nmap --open <target>
  ```

- List interfaces and routes:

```
nmap --iflist
```