***NMAP COMMANDS:-*** [Nmap Cheat Sheet (stationx.net)](https://www.stationx.net/nmap-cheat-sheet/)

♣***BANNER GRABING:-***

nmap --script banner target ip/name

nmap -A targetip/ name (Aggressive scan included banner grabbing services and open ports scanning)

nmap -sV target ip/name (getting banners of services)

***An attacker uses the following Nmap commands and NSE scripts to extract information:-***

**♣ Discover virtual domains with hostmap**:

$nmap --script hostmap

**♣ Detect a vulnerable server that uses the TRACE method:**

nmap --script http-trace -p80 localhost

**♣ Harvest email accounts with http-google-email:**

$nmap --script http-google-email

**♣ Enumerate users with http-userdir-enum:**

nmap -p80 --script http-userdir -enum localhost

**♣ Detect HTTP TRACE:**

$nmap -p80 --script http-trace

**♣ Check if the web server is protected by a web application firewall (WAF) or IPS:**

$nmap -p80 --script http-waf-detect --script-args=”http-waf-detect.uri=/testphp.vulnweb.com/artists.php,http-waf-detect.detectBodyChanges” [www.modsecurity.org](http://www.modsecurity.org)

**♣ Enumerate common web applications**

$nmap --script http-enum -p80 <target>

**♣ Obtain robots.txt**

$nmap -p80 --script http-robots.txt <target>

## ♣smb-check-vulns

## nmap –script smb-check-vulns.nse <target>

## ♣updatedb

## nmap –script-updatedb

**EVASION IDS/ FIREWALL**

**♣ using DECOY (means fake hosts)**

nmap -sA -F -D <fake ip> <target ip>

**♣ send no. of req using RND; use -g if we want to set all random ips having specific source port (eg. -g 13 here 13 is port no.)**

nmap -sA -F -D RND:4 <target ip> (RND is a parameter by which we can generate random fake ip addresses here we are generate only 4 or you can generate more )

**♣fragment packets by -f**

nmap -sA -F -D RND:4 -f –send-eth <target ip>

nmap -f <target ip> ; shows open ports even in firewall enable;

**♣MTU size of 1500bytes**

nmap -sA -F -D RND:4 -f mtu -16 –send-eth <target ip> (eg. Value 16 bytes of each fragmented packet send setting value for -mtu is multiple of 8 and >o )

**♣MAC SPOOFING**

nmap -sA -F -D RND:4 –spoof-mac 0 <target ip>

nmap –spoof-mac <specific vendor eg. Cisco or specific mac> <target ip>

**♣ZOMBIE SCAN USING -sI**

nmap -sI <any other pc ip in n/w> <target ip>

**♣ping sweep -sP for getting no. of ip’s in n/w**

nmap -sP ip with subnet (eg. 10.0.2.0/24)

**♣TCP ACK PACKET using -sA** (basically it is very easy method to check firewall is enabled in target or not without trace because firewall does’nt make logs of ack packet treat as response)

nmap -sA <target ip>

**♣ TCP WINDOW SCAN (SO THIS IS USED TO CHECK PORTS ARE CLOSED OR OPEN EVEN IN FIREWALL DISABLE BECAUSE AFTER OFF FIRRWALL IT SHOWS UNFILTERED PORT )**

**Nmap -Sw <target ip>**

**♣ SCAN WEBSITE BY OTHER WEBSITE FOR SECURITY**

**Nmap -S** [**www.microsoft.com**](http://www.microsoft.com)[**www.facebook.co**](http://www.facebook.co)**m**

**The following are some additional Nmap commands used to extract web server information**:

♣ nmap -sV –O –p target IP address

♣ nmap -sV --script http-enum target IP address

♣ nmap target IP address -p 80 --script = http-frontpage-login

♣ nmap --script http-passwd --script-args http-passwd.root =/ target IP address

**Scan Techniques**

|  |  |  |
| --- | --- | --- |
| **Switch** | **Example** | **Description** |
| -sS | nmap 192.168.1.1 -sS | TCP SYN port scan (Default) |
| -sT | nmap 192.168.1.1 -sT | TCP connect port scan (Default without root privilege) |
| -sU | nmap 192.168.1.1 -sU | UDP port scan |
| -sA | nmap 192.168.1.1 -sA | TCP ACK port scan |
| -sW | nmap 192.168.1.1 -sW | TCP Window port scan |
| -sM | nmap 192.168.1.1 -sM | TCP Maimon port scan |
|  |  |  |

**OS Detection**

|  |  |  |
| --- | --- | --- |
| **Switch** | **Example** | **Description** |
| -O | nmap 192.168.1.1 -O | Remote OS detection using TCP/IP stack fingerprinting |
| -O --osscan-limit | nmap 192.168.1.1 -O --osscan-limit | If at least one open and one closed TCP port are not found it will not try OS detection against host |
| -O --osscan-guess | nmap 192.168.1.1 -O --osscan-guess | Makes Nmap guess more aggressively |
| -O --max-os-tries | nmap 192.168.1.1 -O --max-os-tries 1 | Set the maximum number x of OS detection tries against a target |
| -A | nmap 192.168.1.1 -A | Enables OS detection, version detection, script scanning, and traceroute |

**Service and Version Detection**

|  |  |  |
| --- | --- | --- |
| **Switch** | **Example** | **Description** |
| -sV | nmap 192.168.1.1 -sV | Attempts to determine the version of the service running on port |
| -sV --version-intensity | nmap 192.168.1.1 -sV --version-intensity 8 | Intensity level 0 to 9. Higher number increases possibility of correctness |
| -sV --version-light | nmap 192.168.1.1 -sV --version-light | Enable light mode. Lower possibility of correctness. Faster |
| -sV --version-all | nmap 192.168.1.1 -sV --version-all | Enable intensity level 9. Higher possibility of correctness. Slower |
| -A | nmap 192.168.1.1 -A | Enables OS detection, version detection, script scanning, and traceroute |

Host Discovery

|  |  |  |
| --- | --- | --- |
| **Switch** | **Example** | **Description** |
| -sL | nmap 192.168.1.1-3 -sL | No Scan. List targets only |
| -sn | nmap 192.168.1.1/24 -sn | Disable port scanning. Host discovery only. |
| -Pn | nmap 192.168.1.1-5 -Pn | Disable host discovery. Port scan only. |
| -PS | nmap 192.168.1.1-5 -PS22-25,80 | TCP SYN discovery on port x.  Port 80 by default |
| -PA | nmap 192.168.1.1-5 -PA22-25,80 | TCP ACK discovery on port x.  Port 80 by default |
| -PU | nmap 192.168.1.1-5 -PU53 | UDP discovery on port x.  Port 40125 by default |
| -PR | nmap 192.168.1.1-1/24 -PR | ARP discovery on local network |
| -n | nmap 192.168.1.1 -n | Never do DNS resolution |