Nmap Cheat Sheet

Ping Sweep

```
sudo nmap -sP 192.168.0.1-24
```

Ping Sweep No DNS

```
sudo nmap -sP 192.168.0.1-24 -n
```

TCP Scan All Ports

```
sudo nmap -sT -p0- 192.169.0.1
```

UDP Scan All Port

```
sudo nmap -sU -p0- 192.168.0.1
```

Version and Operating System Detection

```
sudo nmap -sV -O -p0- 192.168.0.1
```

XMAS Scan

```
sudo nmap -sX -p0- -Pn 192.168.0.1
```

Locate Nmap Scripts

```
sudo locate *.nse | grep string
```

Update Nmap Scripts

```
sudo nmap --script-updatedb
```

Banner Grab

```
sudo nmap --script=banner 192.168.0.1
```

SSL Certificate

```
sudo nmap --script ssl-cert -p 443 domain.com
```

SSL Ciphers

```
sudo nmap -sV --script ssl-enum-ciphers -p 443
```

DNS Zone Transfer

```
sudo nmap --script dns-zone-transfer.nse --script-args dns-zone-
transfer.domain=zonetransfer.me -p53 nsztm1.digi.ninja
```

SMB Share Enumeration

```
sudo nmap --script smb-enum-shares.nse -p445 192.168.0.1
```

SMB User Enumeration

```
sudo nmap --script smb-enum-users.nse -p445 192.168.0.1
```

Disclaimer – This is a basic Nmap cheat sheet created to help people with exams. It is not for the purposes of hacking public IP's. Furthermore, there are far better cheat sheets out there for that.

Nmap Cheat Sheet

FTP Brute Force

```
sudo nmap --script ftp-brute -p21 192.168.0.1 --script-args
userdb=ftp_defuser.lst,passdb=ftp_defuser.lst
```

SSH Brute Force

```
sudo nmap -p 22 --script ssh-brute --script-args userdb=ssh-
user.txt,passdb=ssh-password.txt 192.168.0.1
```

Network Layer Authentication

```
sudo nmap -p 3389 --script rdp-enum-encryption 192.168.0.1
```

SMB Signing

```
sudo nmap -p137,139,445 --script smb-security-mode 192.168.0.1
```

Ping Sweep To File

```
sudo nmap -n -sn -vv 10.51.0.0/16 | grep 'Host is up' -B 1 | grep
Nmap | cut -d " " -f 5 > liveips.txt
```

Increase Speed

```
-T1, -T2, -T3, -T4
```

```
sudo nmap -sT -p0- 192.169.0.1 -T4
```

Increase Verbosity

```
-v1, -v2, -v3, -v4
```

```
sudo nmap -sT -p0- 192.169.0.1 -v4
```

Input List

```
sudo nmap -iL targets.txt
```

Save To File

```
sudo nmap 192.168.0.1 -oN scan.txt
```

Save To XML

```
sudo nmap 192.168.0.1 -oX scan.xml
```

Save To Grepable

```
sudo nmap 192.168.0.1 -oG scan.grep.txt
```

Disclaimer – This is a basic Nmap cheat sheet created to help people with exams. It is not for the purposes of hacking public IP's. Furthermore, there are far better cheat sheets out there for that.