Sadiq S.

NMAP

Nmap is a free open-source tool, employed to discover hosts and services on a computer network by sending packets and analyzing the retrieved responses. Nmap offers some features for probing computer networks, including host discovery and service and operating system detection.

Nmap can provide further information on targets, including reverse DNS names, device types, and MAC addresses.

Host discovery – Identifying hosts on a network. For example, listing the hosts that respond to TCP and/or ICMP requests or have a particular port open.

Port scanning – Enumerating the open ports on target hosts.

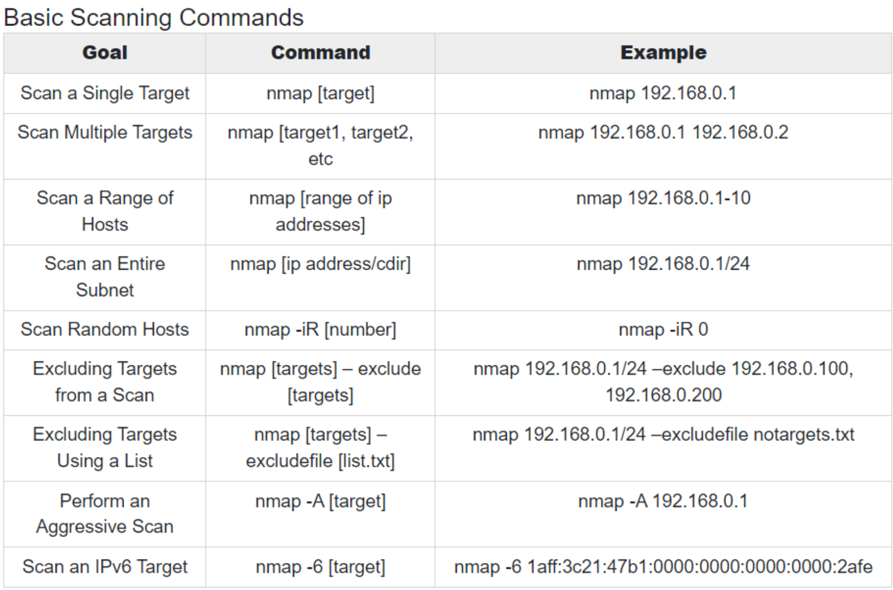
OS detection – Determining the operating system and hardware characteristics of network devices.

Version detection – Interrogating network services on remote devices to determine the application name and version number.

Usage of Nmap:

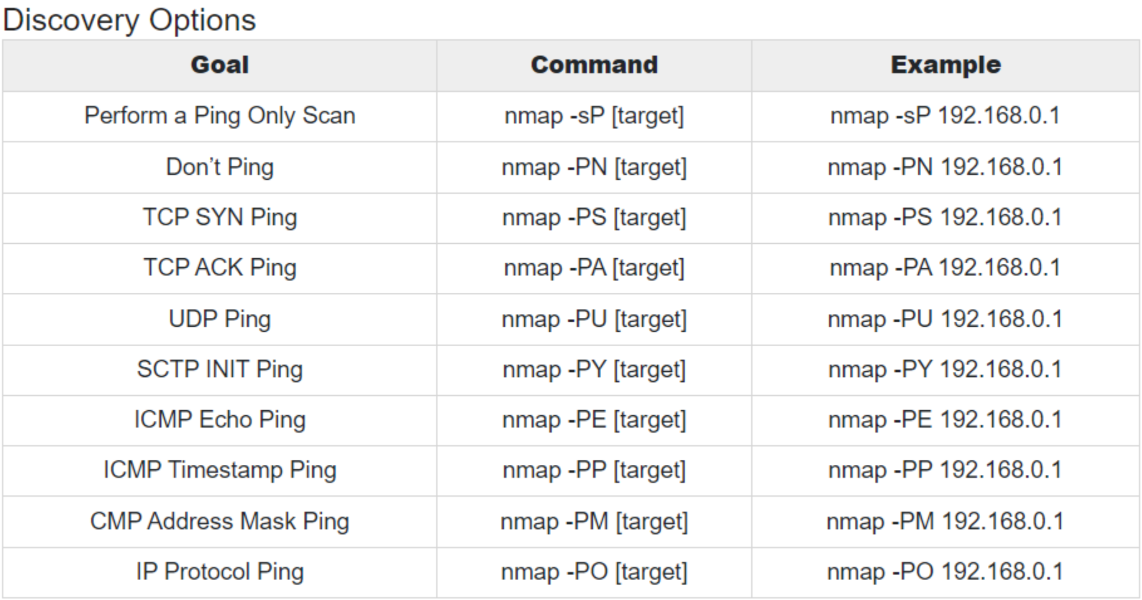
- Auditing the security of a device or firewall by identifying the network connections which can be made to, or through it.
- Identifying open ports on a target host in preparation for auditing.
- Auditing the security of a network by identifying new servers.
- Generating traffic to hosts on a network, response analysis and response time measurement.
- Finding and exploiting vulnerabilities in a network.

NMAP Commands:



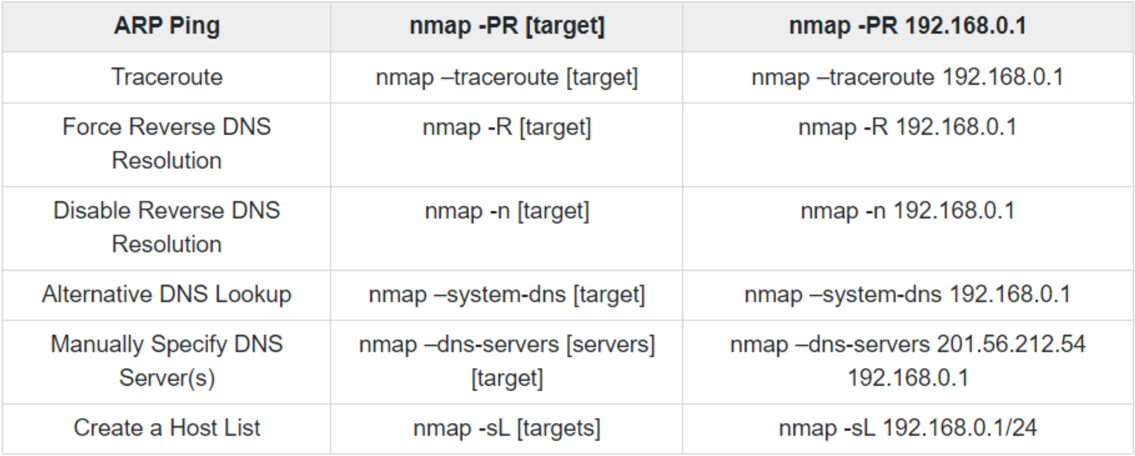
Basic Scanning Commands

Goal	Command	Example
Scan a Single Target	nmap [target]	nmap 192.168.0.1
Scan Multiple Targets	nmap [target1, target2, etc	nmap 192.168.0.1 192.168.0.2
Scan a Range of Hosts	nmap [range of ip addresses]	nmap 192.168.0.1-10
Scan an Entire Subnet	nmap [ip address/cdir]	nmap 192.168.0.1/24
Scan Random Hosts	nmap -iR [number]	nmap -iR 0
Excluding Targets from a Scan	nmap [targets] – exclude [targets]	nmap 192.168.0.1/24 –exclude 192.168.0.100, 192.168.0.200
Excluding Targets Using a List	nmap [targets] – excludefile [list.txt]	nmap 192.168.0.1/24 –excludefile notargets.txt
Perform an Aggressive Scan	nmap -A [target]	nmap -A 192.168.0.1
Scan an IPv6 Target	nmap -6 [target]	nmap -6 1aff:3c21:47b1:0000:0000:0000:0000:2afe

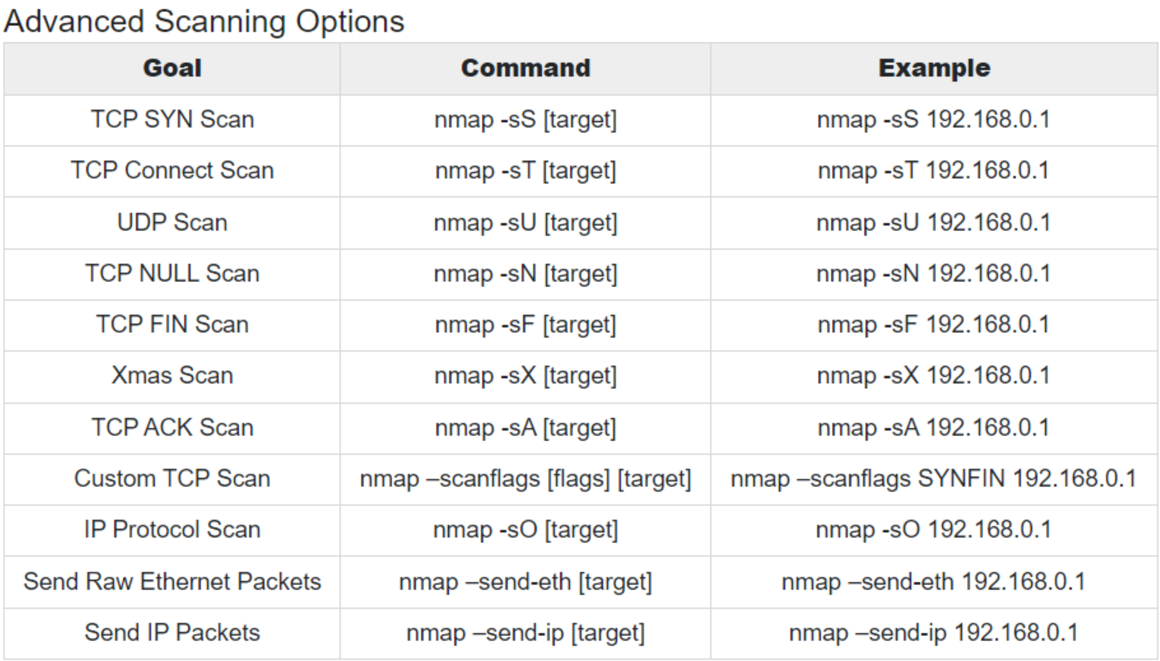


Discovery Options

Goal	Command	Example
Perform a Ping Only Scan	nmap -sP [target]	nmap -sP 192.168.0.1
Don't Ping	nmap -PN [target]	nmap -PN 192.168.0.1
TCP SYN Ping	nmap -PS [target]	nmap -PS 192.168.0.1
TCP ACK Ping	nmap -PA [target]	nmap -PA 192.168.0.1
UDP Ping	nmap -PU [target]	nmap -PU 192.168.0.1
SCTP INIT Ping	nmap -PY [target]	nmap -PY 192.168.0.1
ICMP Echo Ping	nmap -PE [target]	nmap -PE 192.168.0.1
ICMP Timestamp Ping	nmap -PP [target]	nmap -PP 192.168.0.1
CMP Address Mask Ping	nmap -PM [target]	nmap -PM 192.168.0.1
IP Protocol Ping	nmap -PO [target]	nmap -PO 192.168.0.1

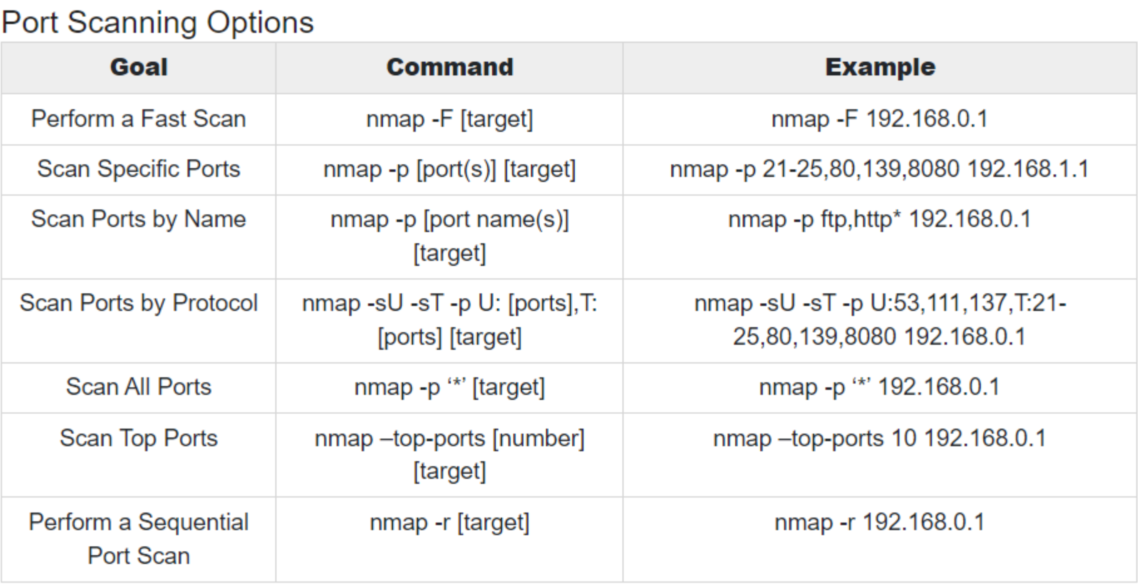


ARP Ping	nmap -PR [target]	nmap -PR 192.168.0.1
Traceroute	nmap –traceroute [target]	nmap –traceroute 192.168.0.1
Force Reverse DNS Resolution	nmap -R [target]	nmap -R 192.168.0.1
Disable Reverse DNS Resolution	nmap -n [target]	nmap -n 192.168.0.1
Alternative DNS Lookup	nmap –system-dns [target]	nmap –system-dns 192.168.0.1
Manually Specify DNS Server(s)	nmap –dns-servers [servers] [target]	nmap –dns-servers 201.56.212.54 192.168.0.1
Create a Host List	nmap -sL [targets]	nmap -sL 192.168.0.1/24



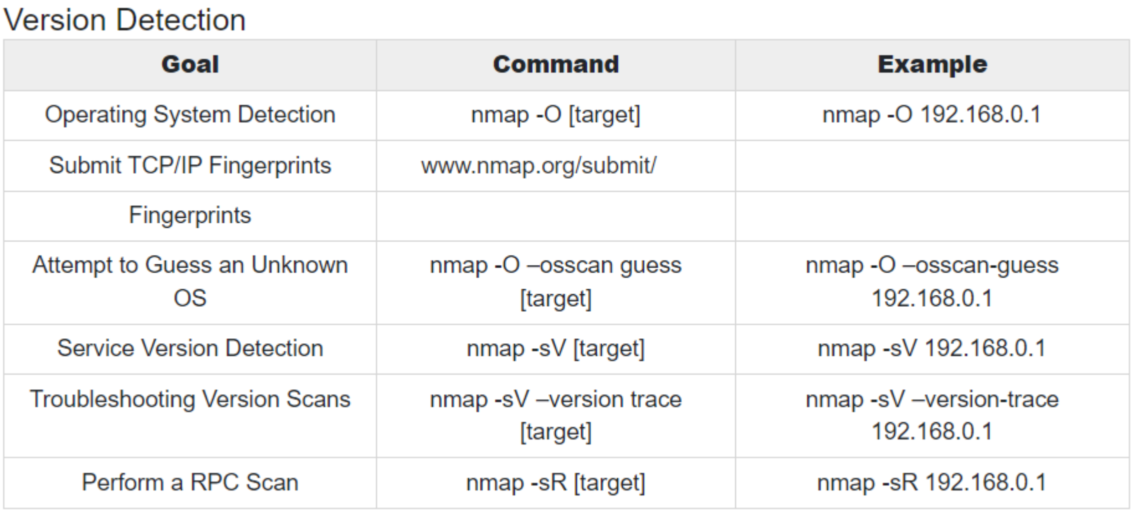
Advanced Scanning Options

Goal	Command	Example
TCP SYN Scan	nmap -sS [target]	nmap -sS 192.168.0.1
TCP Connect Scan	nmap -sT [target]	nmap -sT 192.168.0.1
UDP Scan	nmap -sU [target]	nmap -sU 192.168.0.1
TCP NULL Scan	nmap -sN [target]	nmap -sN 192.168.0.1
TCP FIN Scan	nmap -sF [target]	nmap -sF 192.168.0.1
Xmas Scan	nmap -sX [target]	nmap -sX 192.168.0.1
TCP ACK Scan	nmap -sA [target]	nmap -sA 192.168.0.1
Custom TCP Scan	nmap –scanflags [flags] [target]	nmap –scanflags SYNFIN 192.168.0.1
IP Protocol Scan	nmap -sO [target]	nmap -sO 192.168.0.1
Send Raw Ethernet Packets	nmap –send-eth [target]	nmap –send-eth 192.168.0.1
Send IP Packets	nmap –send-ip [target]	nmap –send-ip 192.168.0.1



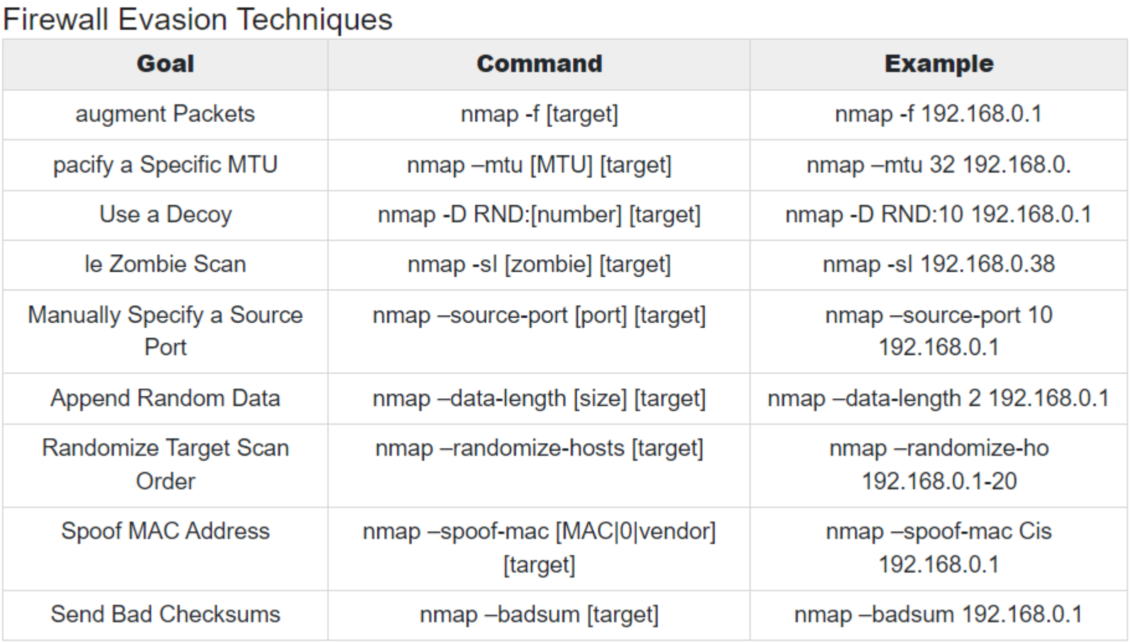
Port Scanning Options

Goal	Command	Example
Perform a Fast Scan	nmap -F [target]	nmap -F 192.168.0.1
Scan Specific Ports	nmap -p [port(s)] [target]	nmap -p 21-25,80,139,8080 192.168.1.1
Scan Ports by Name	nmap -p [port name(s)] [target]	nmap -p ftp,http* 192.168.0.1
Scan Ports by Protocol	nmap -sU -sT -p U: [ports],T: [ports] [target]	nmap -sU -sT -p U:53,111,137,T:21-25,80,139,8080 192.168.0.1
Scan All Ports	nmap -p ‘*’ [target]	nmap -p ‘*’ 192.168.0.1
Scan Top Ports	nmap –top-ports [number] [target]	nmap –top-ports 10 192.168.0.1
Perform a Sequential Port Scan	nmap -r [target]	nmap -r 192.168.0.1



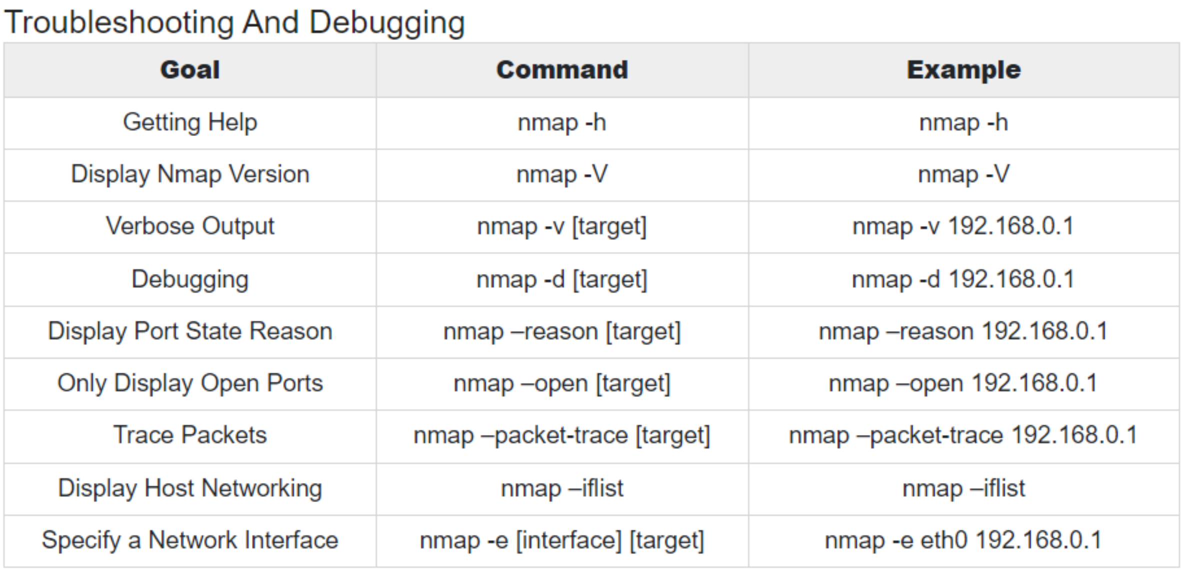
Version Detection

Goal	Command	Example
Operating System Detection	nmap -O [target]	nmap -O 192.168.0.1
Submit TCP/IP Fingerprints	www.nmap.org/submit/	
Fingerprints		
Attempt to Guess an Unknown OS	nmap -O –osscan guess [target]	nmap -O –osscan-guess 192.168.0.1
Service Version Detection	nmap -sV [target]	nmap -sV 192.168.0.1
Troubleshooting Version Scans	nmap -sV –version trace [target]	nmap -sV –version-trace 192.168.0.1
Perform a RPC Scan	nmap -sR [target]	nmap -sR 192.168.0.1



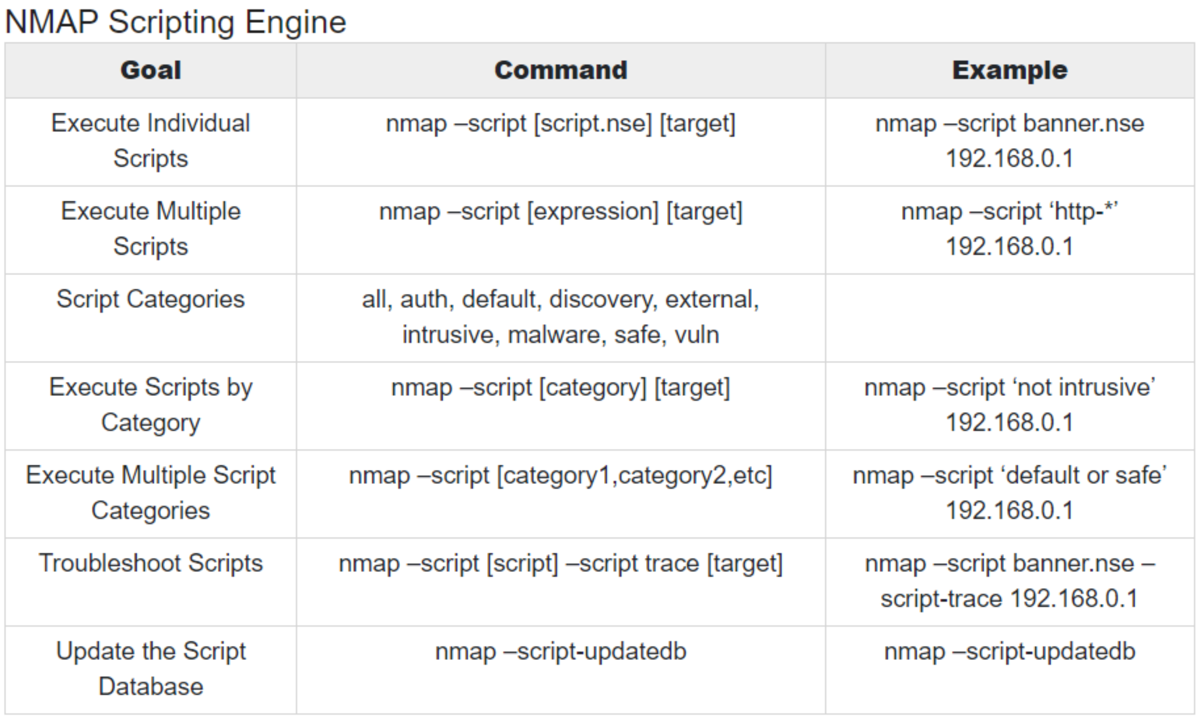
Firewall Evasion Techniques

Goal	Command	Example
augment Packets	nmap -f [target]	nmap -f 192.168.0.1
pacify a Specific MTU	nmap –mtu [MTU] [target]	nmap –mtu 32 192.168.0.
Use a Decoy	nmap -D RND:[number] [target]	nmap -D RND:10 192.168.0.1
le Zombie Scan	nmap -sI [zombie] [target]	nmap -sI 192.168.0.38
Manually Specify a Source Port	nmap –source-port [port] [target]	nmap –source-port 10 192.168.0.1
Append Random Data	nmap –data-length [size] [target]	nmap –data-length 2 192.168.0.1
Randomize Target Scan Order	nmap –randomize-hosts [target]	nmap –randomize-ho 192.168.0.1-20
Spoof MAC Address	nmap –spoof-mac [MAC|0|vendor] [target]	nmap –spoof-mac Cis 192.168.0.1
Send Bad Checksums	nmap –badsum [target]	nmap –badsum 192.168.0.1



Troubleshooting And Debugging

Goal	Command	Example
Getting Help	nmap -h	nmap -h
Display Nmap Version	nmap -V	nmap -V
Verbose Output	nmap -v [target]	nmap -v 192.168.0.1
Debugging	nmap -d [target]	nmap -d 192.168.0.1
Display Port State Reason	nmap –reason [target]	nmap –reason 192.168.0.1
Only Display Open Ports	nmap –open [target]	nmap –open 192.168.0.1
Trace Packets	nmap –packet-trace [target]	nmap –packet-trace 192.168.0.1
Display Host Networking	nmap –iflist	nmap –iflist
Specify a Network Interface	nmap -e [interface] [target]	nmap -e eth0 192.168.0.1

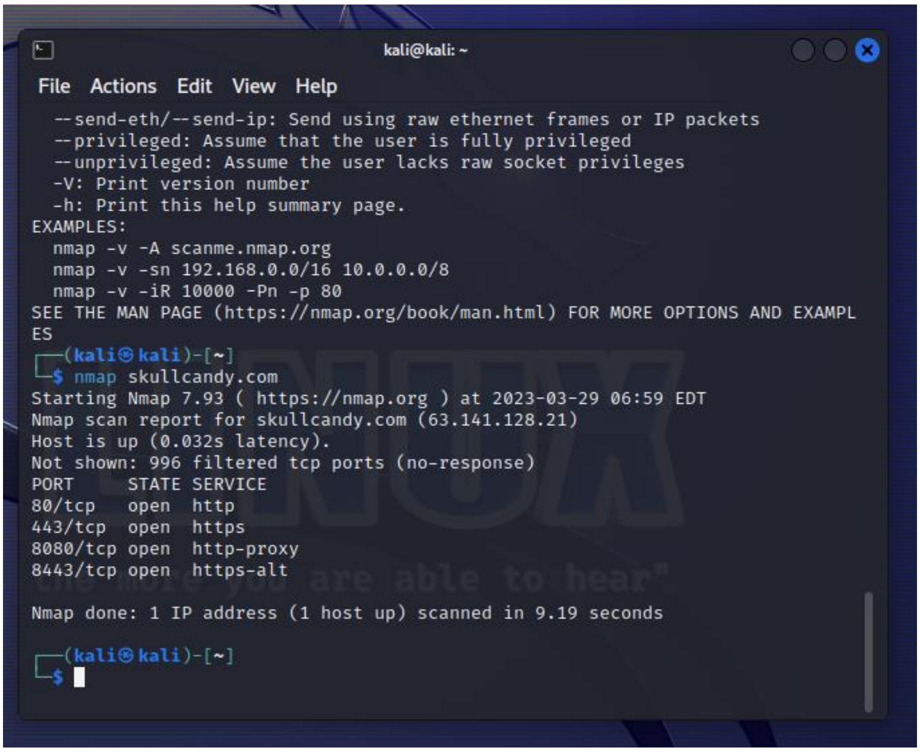


NMAP Scripting Engine

Goal	Command	Example
Execute Individual Scripts	nmap –script [script.nse] [target]	nmap –script banner.nse 192.168.0.1
Execute Multiple Scripts	nmap –script [expression] [target]	nmap –script ‘http-*’ 192.168.0.1
Script Categories	all, auth, default, discovery, external, intrusive, malware, safe, vuln	
Execute Scripts by Category	nmap –script [category] [target]	nmap –script ‘not intrusive’ 192.168.0.1
Execute Multiple Script Categories	nmap –script [category1,category2,etc]	nmap –script ‘default or safe’ 192.168.0.1
Troubleshoot Scripts	nmap –script [script] –script trace [target]	nmap –script banner.nse –script-trace 192.168.0.1
Update the Script Database	nmap –script-updatedb	nmap –script-updatedb

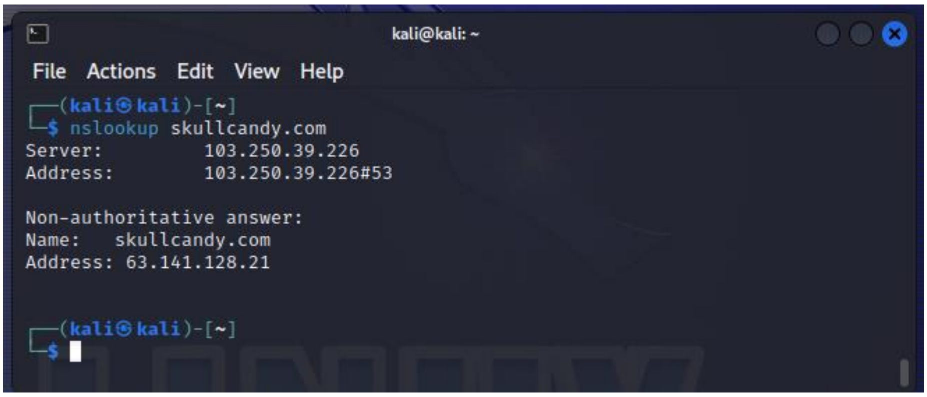
We will do our NMAP Scan on ‘skullcandy.com’ and my MS2 machine whose IP ADDRESS is 192.168.0.5

NMAP Scan: Will return IP Address and some information



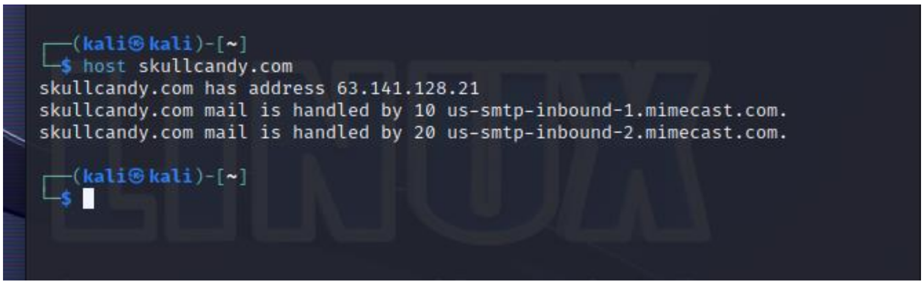
```
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPL
ES
┌──(kali㉿kali)-[~]
└─$ nmap skullcandy.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-29 06:59 EDT
Nmap scan report for skullcandy.com (63.141.128.21)
Host is up (0.032s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 9.19 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Nslookup: Will return the name server and it’s IP Address



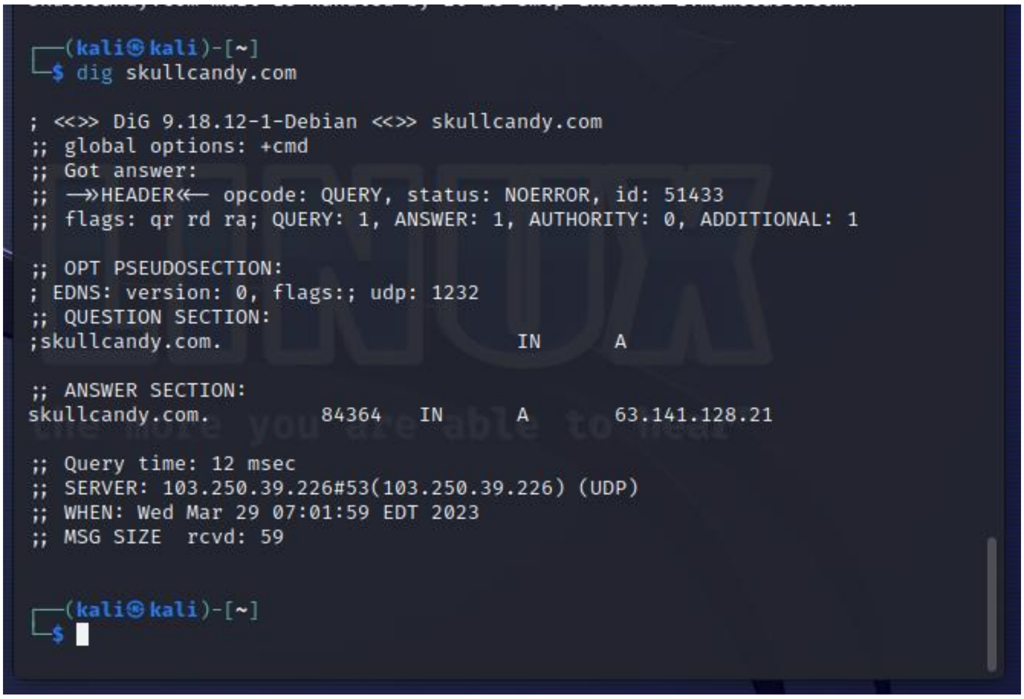
```
┌──(kali㉿kali)-[~]
└─$ nslookup skullcandy.com
Server:         103.250.39.226
Address:        103.250.39.226#53

Non-authoritative answer:
Name:   skullcandy.com
Address: 63.141.128.21


┌──(kali㉿kali)-[~]
└─$ 
```

Host: Will give us the SMTP inbound.



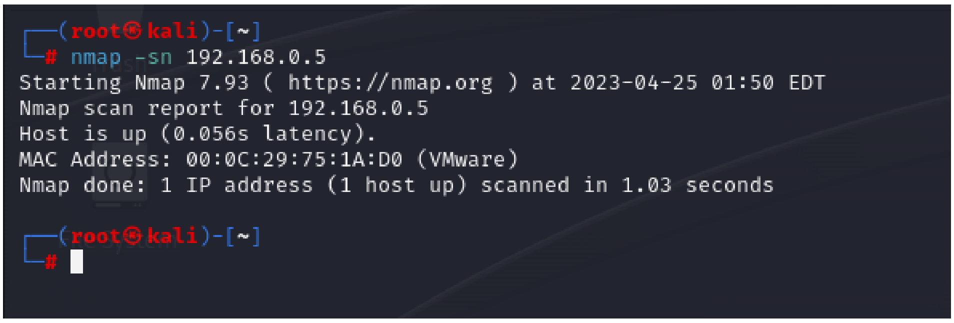
```
┌──(kali㉿kali)-[~]
└─$ host skullcandy.com
skullcandy.com has address 63.141.128.21
skullcandy.com mail is handled by 10 us-smtp-inbound-1.mimecast.com.
skullcandy.com mail is handled by 20 us-smtp-inbound-2.mimecast.com.

┌──(kali㉿kali)-[~]
└─$ 
```

Dig: Will give us more information about the target.



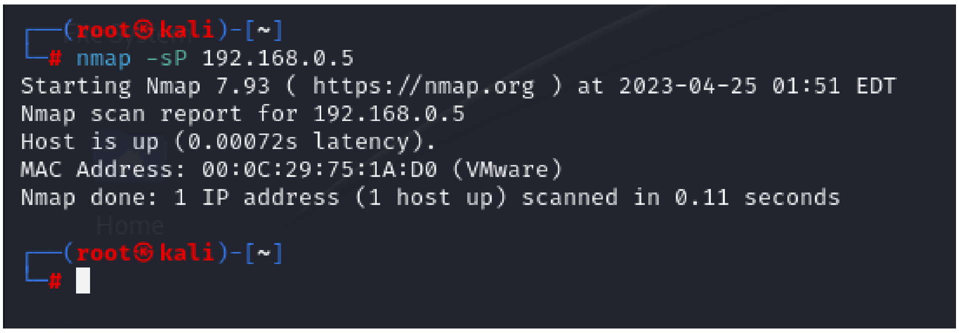
```
┌──(kali㉿kali)-[~]
└─$ dig skullcandy.com

; <<>> DiG 9.18.12-1-Debian <<>> skullcandy.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51433
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;skullcandy.com.                IN      A

;; ANSWER SECTION:
skullcandy.com.         84364   IN      A       63.141.128.21

;; Query time: 12 msec
;; SERVER: 103.250.39.226#53(103.250.39.226) (UDP)
;; WHEN: Wed Mar 29 07:01:59 EDT 2023
;; MSG SIZE  rcvd: 59


┌──(kali㉿kali)-[~]
└─$ 
```

Nmap -sn IP Address: Will check whether Server/Host is Up or not.



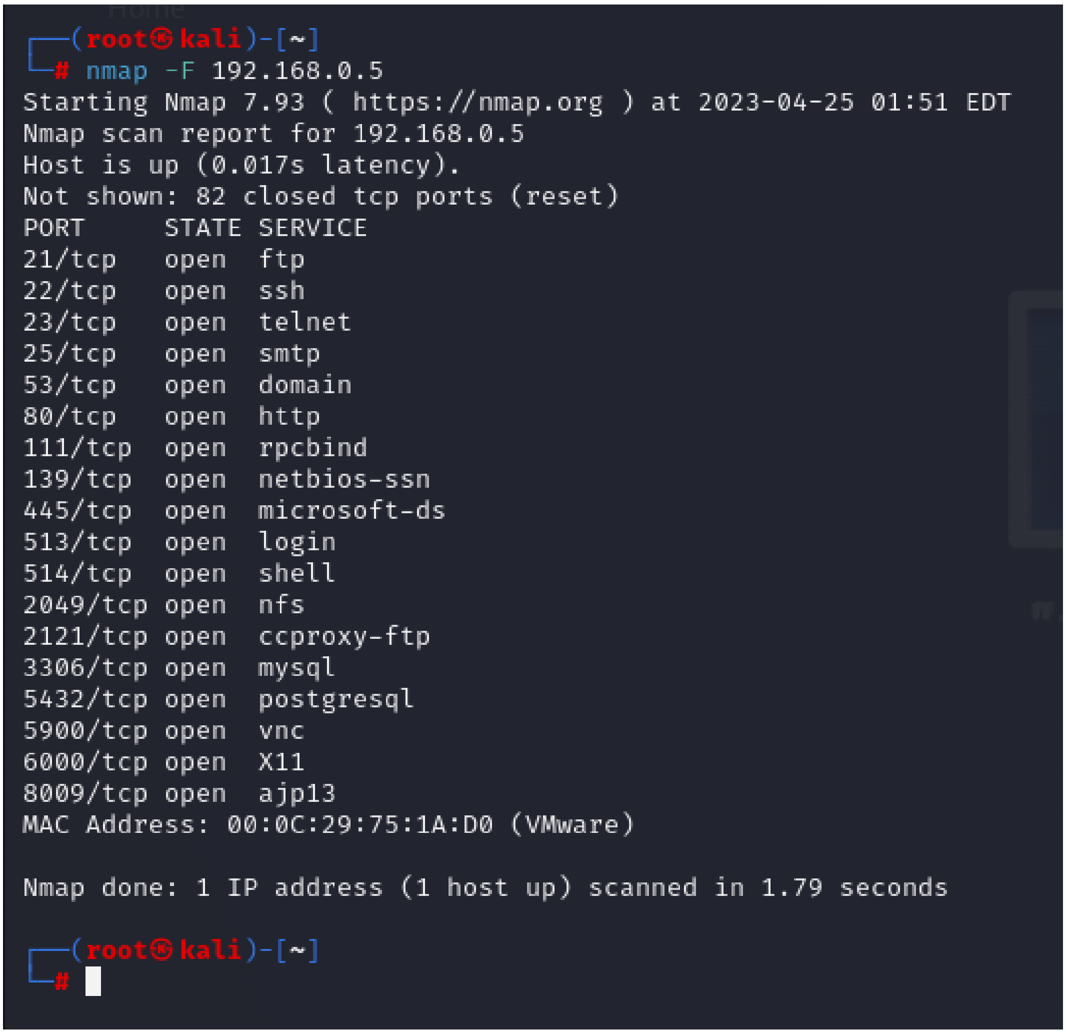
```
┌──(root㉿kali)-[~]
└─# nmap -sn 192.168.0.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-25 01:50 EDT
Nmap scan report for 192.168.0.5
Host is up (0.056s latency).
MAC Address: 00:0C:29:75:1A:D0 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 1.03 seconds

┌──(root㉿kali)-[~]
└─# 
```

Nmap -sP IP Address: Will ping the Server.



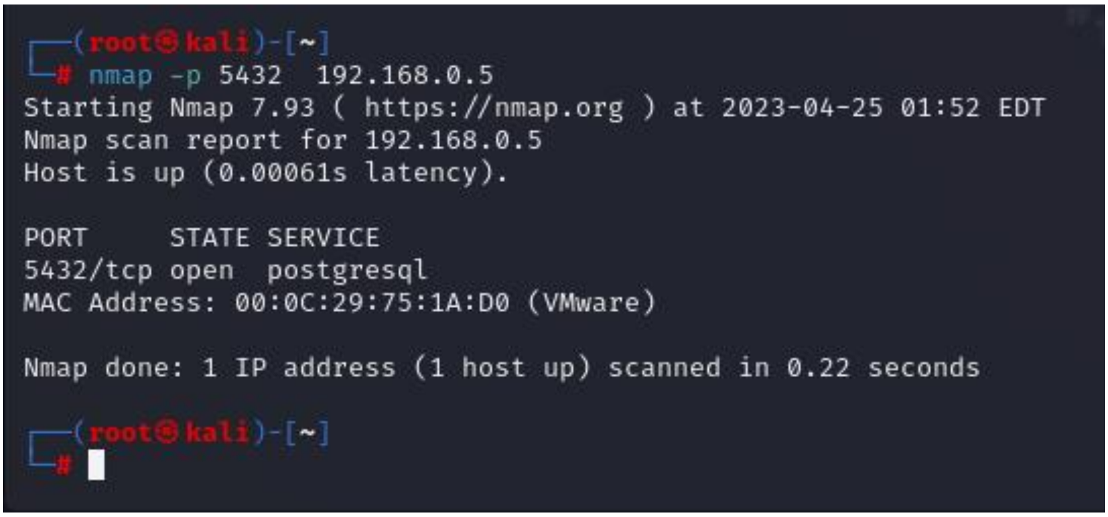
```
┌──(root㉿kali)-[~]
└─# nmap -sP 192.168.0.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-25 01:51 EDT
Nmap scan report for 192.168.0.5
Host is up (0.00072s latency).
MAC Address: 00:0C:29:75:1A:D0 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds

┌──(root㉿kali)-[~]
└─# 
```

Nmap -F IP Address: Will do a Fast Scan on the server and will show open ports.



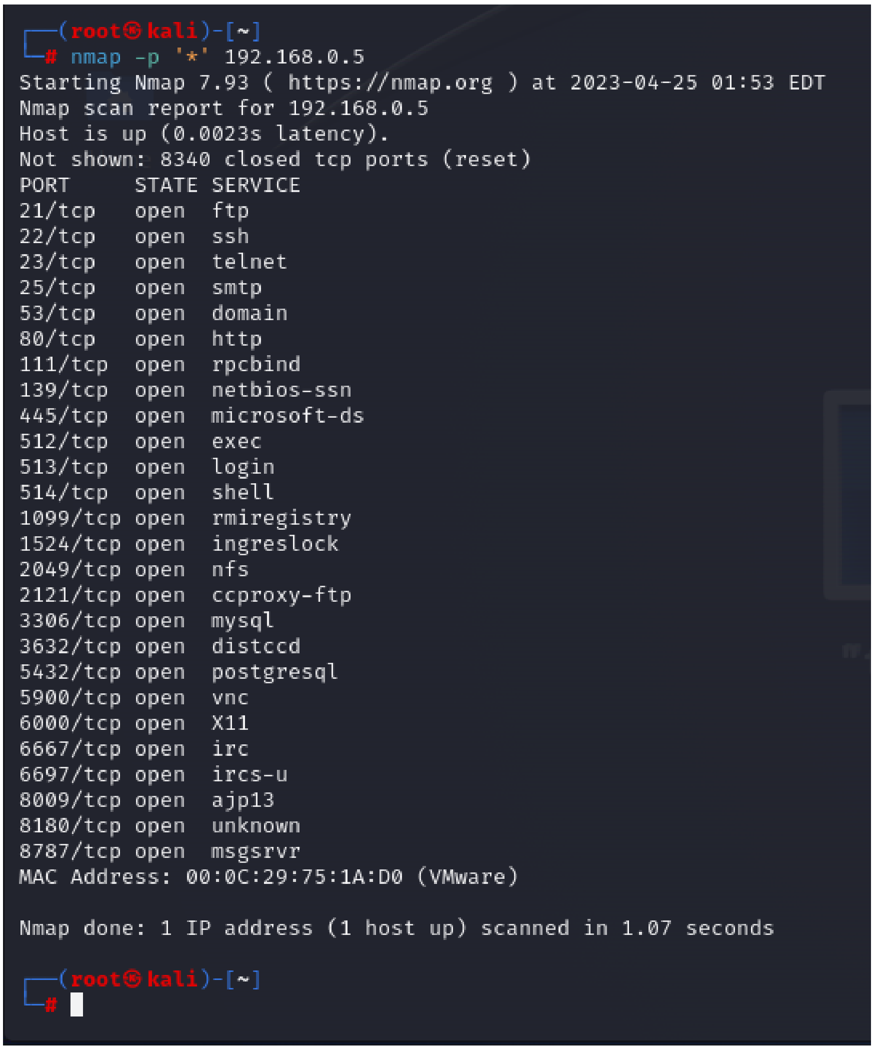
```
┌──(root㉿kali)-[~]
└─# nmap -F 192.168.0.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-25 01:51 EDT
Nmap scan report for 192.168.0.5
Host is up (0.017s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
513/tcp  open  login
514/tcp  open  shell
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
8009/tcp open  ajp13
MAC Address: 00:0C:29:75:1A:D0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.79 seconds

┌──(root㉿kali)-[~]
└─# 
```

Nmap -p port number IP Address: Will scan a particular port number.



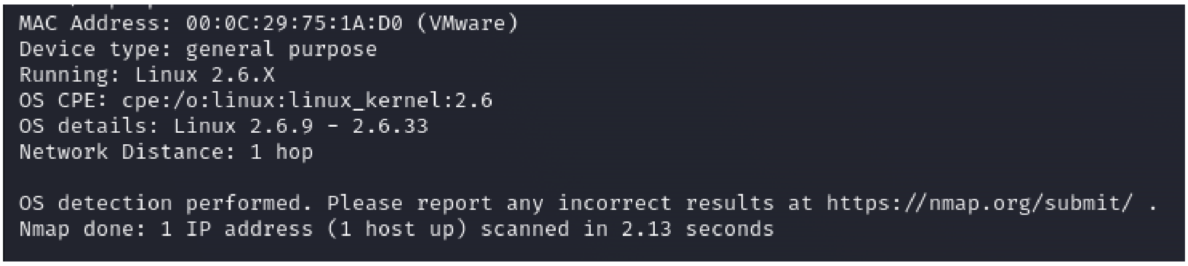
```
┌──(root㉿kali)-[~]
└─# nmap -p 5432  192.168.0.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-25 01:52 EDT
Nmap scan report for 192.168.0.5
Host is up (0.00061s latency).

PORT     STATE SERVICE
5432/tcp open  postgresql
MAC Address: 00:0C:29:75:1A:D0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds

┌──(root㉿kali)-[~]
└─# 
```

Nmap -p '*' IP Address: Will scan all the open ports.



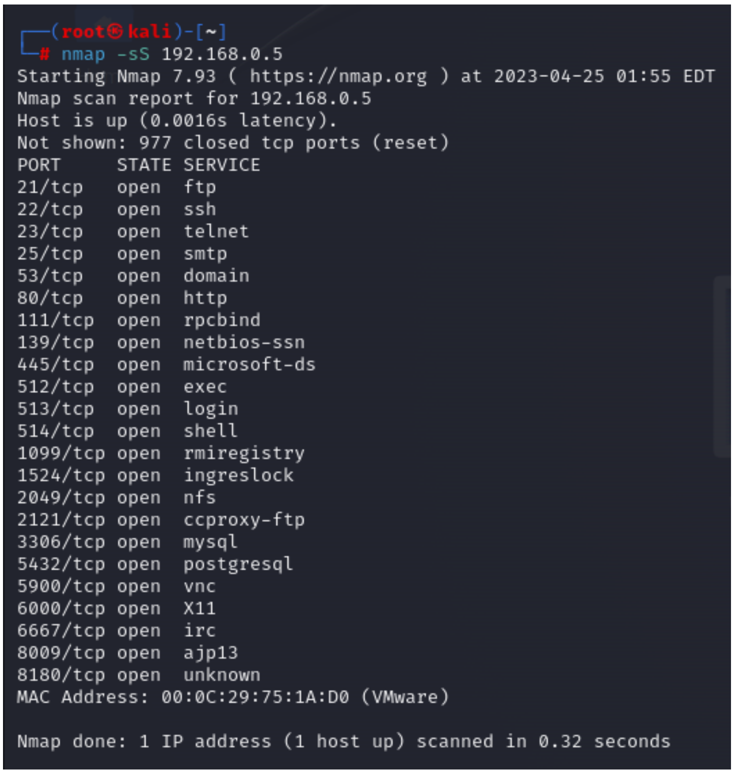
```
┌──(root㉿kali)-[~]
└─# nmap -p '*' 192.168.0.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-25 01:53 EDT
Nmap scan report for 192.168.0.5
Host is up (0.0023s latency).
Not shown: 8340 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
3632/tcp open  distccd
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
6697/tcp open  ircs-u
8009/tcp open  ajp13
8180/tcp open  unknown
8787/tcp open  msgsrvr
MAC Address: 00:0C:29:75:1A:D0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.07 seconds

┌──(root㉿kali)-[~]
└─# 
```

Sudo Nmap -O IP Address: Will return the operating system being used. It requires root privileges. So we use sudo.



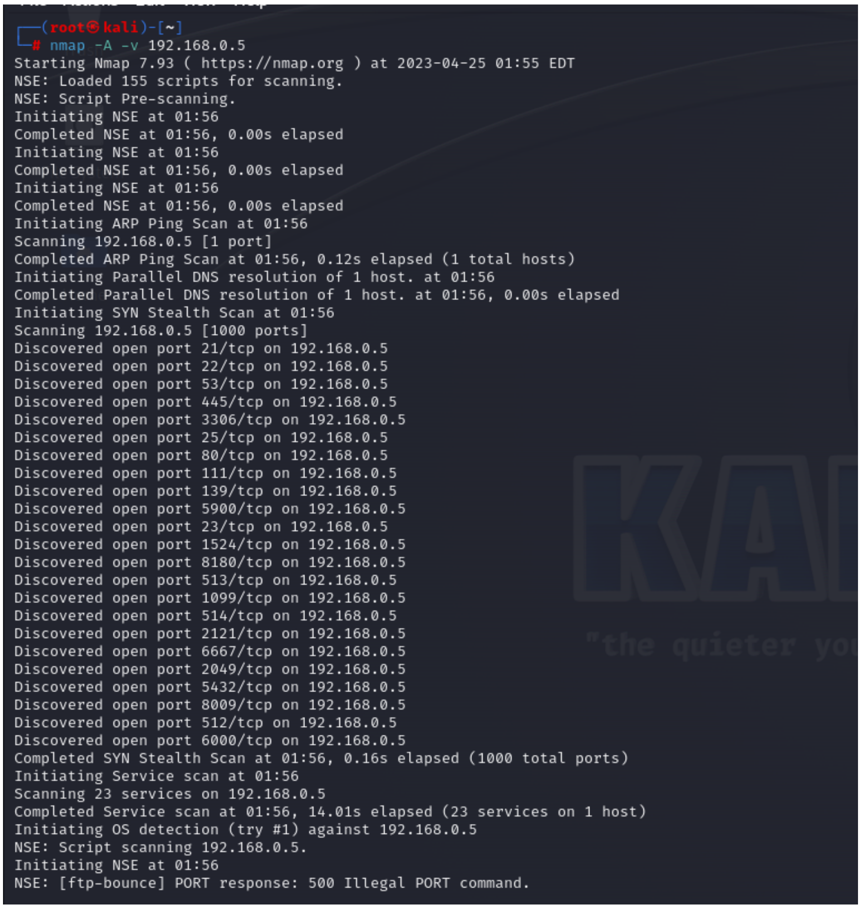
```
MAC Address: 00:0C:29:75:1A:D0 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.13 seconds
```

Nmap -sS IP Address: Will perform a stealth scan.

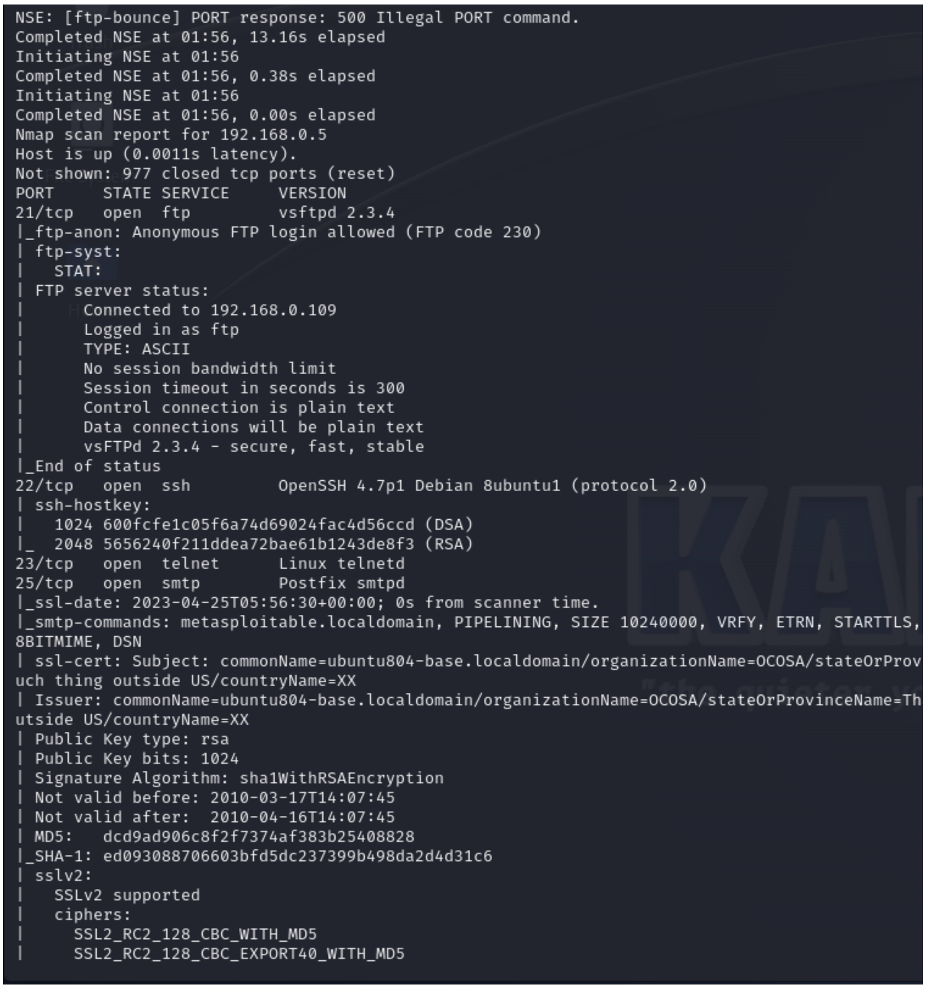


```
┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.0.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-25 01:55 EDT
Nmap scan report for 192.168.0.5
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:75:1A:D0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

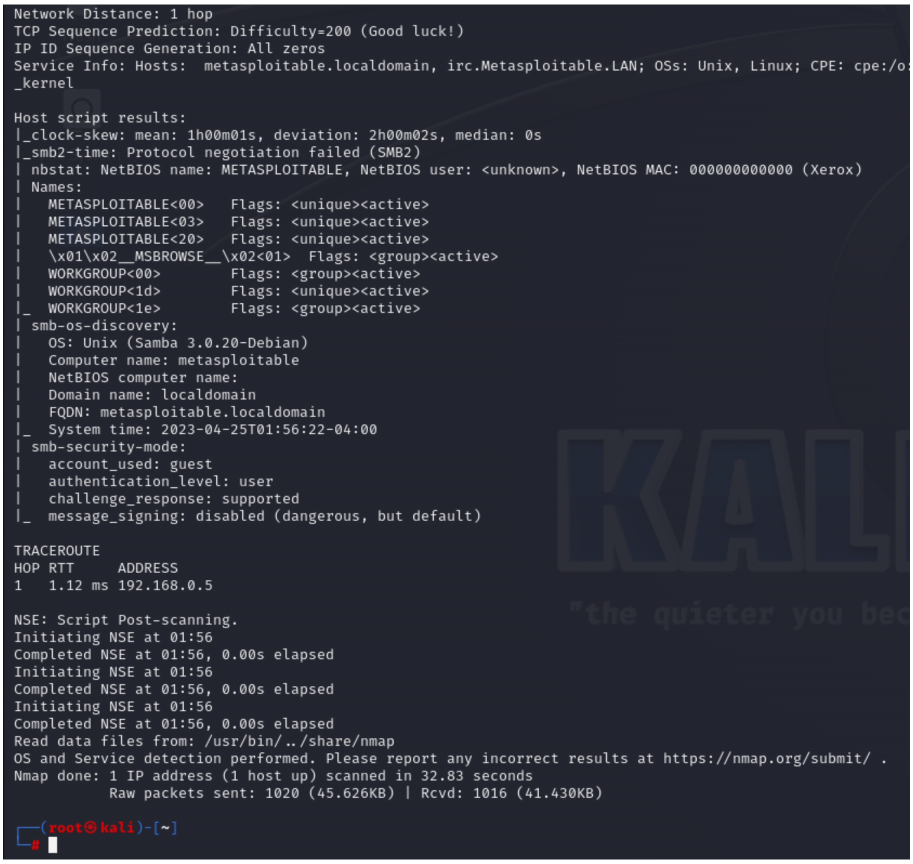
Nmap -A -v IP Address: Intense scan. It will perform various scans. Will give details about the port no., State of the port, Service running on that port and the version.



```
┌──(root㉿kali)-[~]
└─# nmap -A -v 192.168.0.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-25 01:55 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 01:56
Completed NSE at 01:56, 0.00s elapsed
Initiating NSE at 01:56
Completed NSE at 01:56, 0.00s elapsed
Initiating NSE at 01:56
Completed NSE at 01:56, 0.00s elapsed
Initiating ARP Ping Scan at 01:56
Scanning 192.168.0.5 [1 port]
Completed ARP Ping Scan at 01:56, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:56
Completed Parallel DNS resolution of 1 host. at 01:56, 0.00s elapsed
Initiating SYN Stealth Scan at 01:56
Scanning 192.168.0.5 [1000 ports]
Discovered open port 21/tcp on 192.168.0.5
Discovered open port 22/tcp on 192.168.0.5
Discovered open port 53/tcp on 192.168.0.5
Discovered open port 445/tcp on 192.168.0.5
Discovered open port 3306/tcp on 192.168.0.5
Discovered open port 25/tcp on 192.168.0.5
Discovered open port 80/tcp on 192.168.0.5
Discovered open port 111/tcp on 192.168.0.5
Discovered open port 139/tcp on 192.168.0.5
Discovered open port 5900/tcp on 192.168.0.5
Discovered open port 23/tcp on 192.168.0.5
Discovered open port 1524/tcp on 192.168.0.5
Discovered open port 8180/tcp on 192.168.0.5
Discovered open port 513/tcp on 192.168.0.5
Discovered open port 1099/tcp on 192.168.0.5
Discovered open port 514/tcp on 192.168.0.5
Discovered open port 2121/tcp on 192.168.0.5
Discovered open port 6667/tcp on 192.168.0.5
Discovered open port 2049/tcp on 192.168.0.5
Discovered open port 5432/tcp on 192.168.0.5
Discovered open port 8009/tcp on 192.168.0.5
Discovered open port 512/tcp on 192.168.0.5
Discovered open port 6000/tcp on 192.168.0.5
Completed SYN Stealth Scan at 01:56, 0.16s elapsed (1000 total ports)
Initiating Service scan at 01:56
Scanning 23 services on 192.168.0.5
Completed Service scan at 01:56, 14.01s elapsed (23 services on 1 host)
Initiating OS detection (try #1) against 192.168.0.5
NSE: Script scanning 192.168.0.5.
Initiating NSE at 01:56
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
```

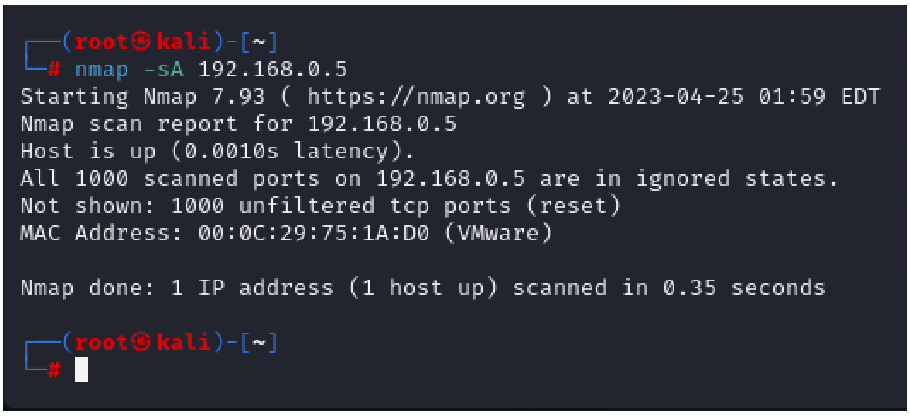


```
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Completed NSE at 01:56, 13.16s elapsed
Initiating NSE at 01:56
Completed NSE at 01:56, 0.38s elapsed
Initiating NSE at 01:56
Completed NSE at 01:56, 0.00s elapsed
Nmap scan report for 192.168.0.5
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.0.109
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2023-04-25T05:56:30+00:00; 0s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProv
uch thing outside US/countryName=XX
| Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=Th
utside US/countryName=XX
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
| MD5:   dcd9ad906c8f2f7374af383b25408828
|_SHA-1: ed093088706603bfd5dc237399b498da2d4d31c6
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
```



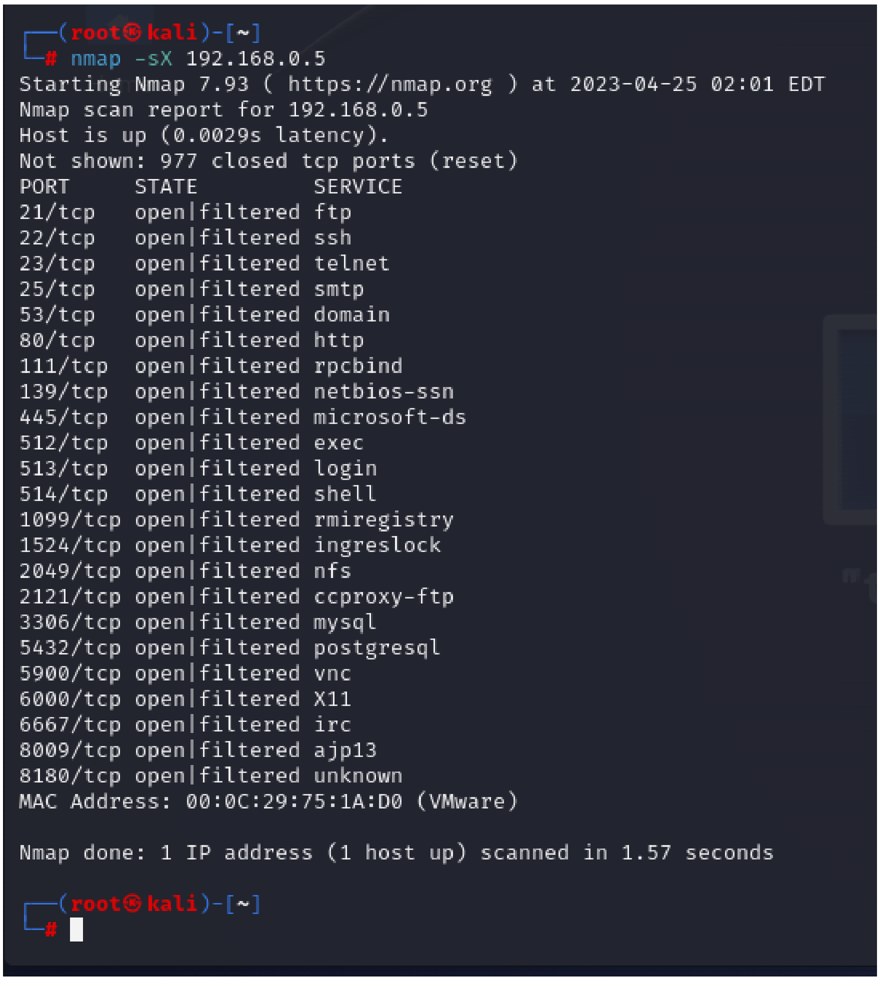
```
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=200 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:
_kernel

Host script results:
|_clock-skew: mean: 1h00m01s, deviation: 2h00m02s, median: 0s
|_smb2-time: Protocol negotiation failed (SMB2)
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| Names:
|   METASPLOITABLE<00>   Flags: <unique><active>
|   METASPLOITABLE<03>   Flags: <unique><active>
|   METASPLOITABLE<20>   Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  WORKGROUP<1e>        Flags: <group><active>
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-04-25T01:56:22-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   1.12 ms 192.168.0.5

NSE: Script Post-scanning.
Initiating NSE at 01:56
Completed NSE at 01:56, 0.00s elapsed
Initiating NSE at 01:56
Completed NSE at 01:56, 0.00s elapsed
Initiating NSE at 01:56
Completed NSE at 01:56, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.83 seconds
           Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.430KB)

┌──(root㉿kali)-[~]
└─#
```

Nmap -sA IP Address: Will check for firewall on the ports.



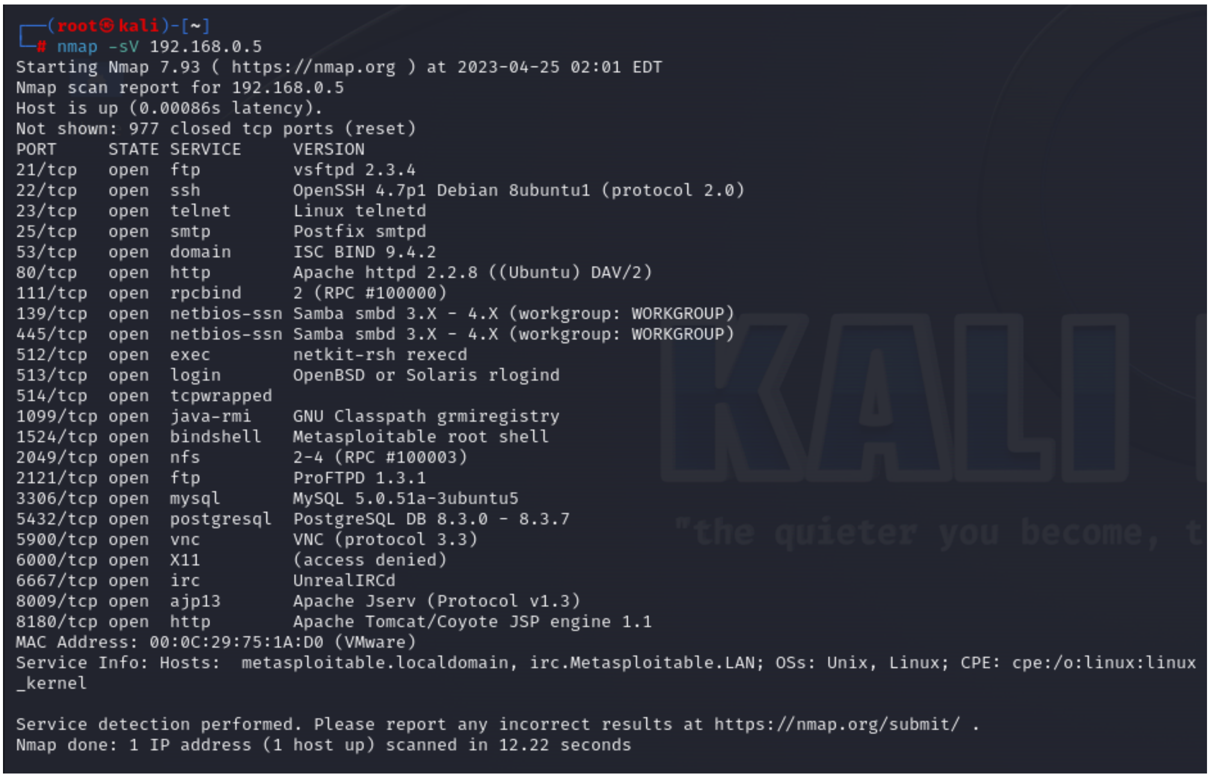
```
┌──(root㉿kali)-[~]
└─# nmap -sA 192.168.0.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-25 01:59 EDT
Nmap scan report for 192.168.0.5
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.0.5 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 00:0C:29:75:1A:D0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds

┌──(root㉿kali)-[~]
└─# 
```

Nmap -sX IP Address: Will perform a Xmas Scan on the MS2.



```
┌──(root㉿kali)-[~]
└─# nmap -sX 192.168.0.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-25 02:01 EDT
Nmap scan report for 192.168.0.5
Host is up (0.0029s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 00:0C:29:75:1A:D0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds

┌──(root㉿kali)-[~]
└─# 
```

Nmap -sV IP Address: Will return us the service Version.



```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.0.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-25 02:01 EDT
Nmap scan report for 192.168.0.5
Host is up (0.00086s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:75:1A:D0 (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux
_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.22 seconds
```