Cyber Security by Threat Prism

BATCH 7

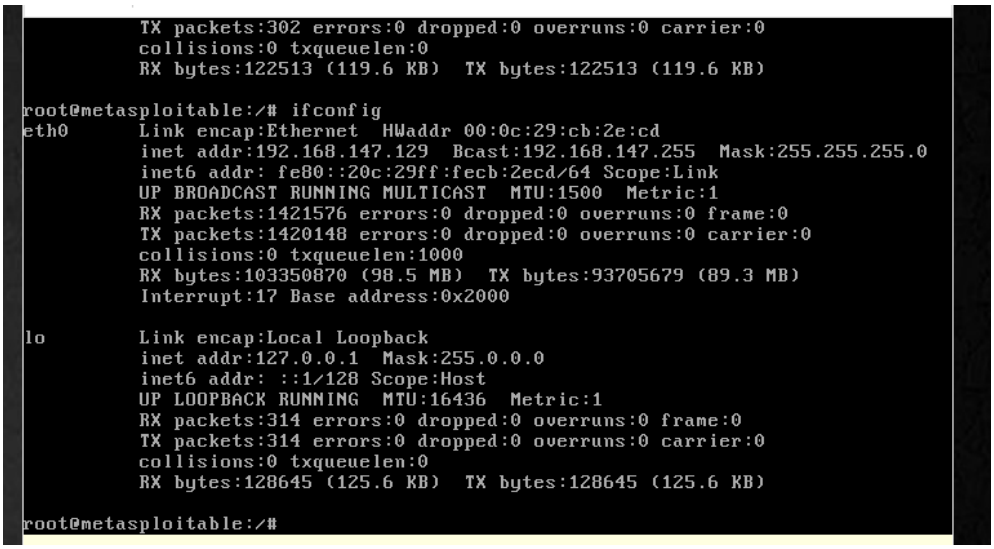
Sai Goutham Reddy Alavala

Cyber Security/Ethical Hacking - Scanning for Open ports and Attacking Threat Prism Project – 2

---In this we are using nmap scanning which has different type of scanning methods to obtain the information on ports whether they are open, closed, filtered, unfiltered or tcp trapped.

Task1:

Let's use metasploit server to perform all this scanning techniques, whose IP address is as followed: 192.168.147.129



Task 2:

Sync Scanning.

i) nmap –v –sS 192.168.147.129

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -V -sS 192.168.147.129
Nmap version 7.92 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.6 openssl-1.1.1o libssh2-1.10.0 libz-1.2.11 libpcre-8.39 nmap-libpcap-1.7.3 nmap-libdnet-
1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

ii) nmap -v -sS -p 21 192.168.147.129

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -v -sS -p 21 192.168.147.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 21:25 EST
Initiating ARP Ping Scan at 21:25
Scanning 192.168.147.129 [1 port]
Completed ARP Ping Scan at 21:25, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:25
Completed Parallel DNS resolution of 1 host. at 21:25, 0.01s elapsed
Initiating SYN Stealth Scan at 21:25
Scanning 192.168.147.129 [1 port]
Discovered open port 21/tcp on 192.168.147.129
Completed SYN Stealth Scan at 21:25, 0.08s elapsed (1 total ports)
Nmap scan report for 192.168.147.129
Host is up (0.0013s latency).

PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 00:0C:29:CB:2E:CD (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
           Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
```

Acknowledgement Scanning.

i) nmap –sA 192.168.147.129

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sA 192.168.147.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 21:26 EST
Nmap scan report for 192.168.147.129
Host is up (0.0070s latency).
All 1000 scanned ports on 192.168.147.129 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 00:0C:29:CB:2E:CD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds
```

ii) nmap -sA -p 22 -sV -O 192.168.147.129

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sA -p 22 -sV -O 192.168.147.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 21:26 EST
Nmap scan report for 192.168.147.129
Host is up (0.00055s latency).

PORT   STATE      SERVICE VERSION
22/tcp unfiltered ssh
MAC Address: 00:0C:29:CB:2E:CD (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Aruba IAP-105 WAP (95%), AVM FRITZ!Box FON WLAN 7240 WAP (95%), Belkin N600 DB WAP (95%), Bu
ffalo LinkStation NAS device (95%), Buffalo LS-WXL NAS device (95%), Check Point VPN-1 UTM appliance (95%), Cisco C
P 8945 VoIP phone (95%), D-Link DSR-1000N WAP (95%), EnGenius ESR-9250 WAP (95%), Android 2.3.5 (Linux 2.6.35) (95%
)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

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 4.08 seconds
```

Finn Scanning

i) nmap –sF 192.168.147.129

ii) nmap –sF –p 22 192.168.147.129

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sF 192.168.147.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 21:27 EST
Nmap scan report for 192.168.147.129
Host is up (0.012s 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:CB:2E:CD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.73 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -sF -p 22 192.168.147.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 21:27 EST
Nmap scan report for 192.168.147.129
Host is up (0.00048s latency).

PORT   STATE         SERVICE
22/tcp open|filtered ssh
MAC Address: 00:0C:29:CB:2E:CD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds
```

iii) nmap –sF –p 22 –sV –O 192.168.147.129

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sF -p 22 -sV -O  192.168.147.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 21:28 EST
Nmap scan report for 192.168.147.129
Host is up (0.00061s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
MAC Address: 00:0C:29:CB:2E:CD (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 2.22 seconds
```

XMAS Scanning

i)nmap –sX 192.168.147.129

ii) nmap –sX –p 21 192.168.147.129

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sX 192.168.147.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 21:28 EST
Nmap scan report for 192.168.147.129
Host is up (0.0087s 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:CB:2E:CD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.77 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -sX -p 21 -sV 192.168.147.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 21:28 EST
Nmap scan report for 192.168.147.129
Host is up (0.00053s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
MAC Address: 00:0C:29:CB:2E:CD (VMware)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.74 seconds
```

iii) nmap –sX –p 21 -sV 192.168.147.129

iv) nmap –sX –p 21-30 -sV 192.168.147.129

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sX -p 21 -sV 192.168.147.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 21:28 EST
Nmap scan report for 192.168.147.129
Host is up (0.00053s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
MAC Address: 00:0C:29:CB:2E:CD (VMware)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.74 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sX -p 21-30 -sV 192.168.147.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 21:29 EST
Nmap scan report for 192.168.147.129
Host is up (0.00035s latency).

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
24/tcp closed priv-mail
25/tcp open   smtp     Postfix smtpd
26/tcp closed rsftp
27/tcp closed nsw-fe
28/tcp closed unknown
29/tcp closed msg-icp
30/tcp closed unknown
MAC Address: 00:0C:29:CB:2E:CD (VMware)
Service Info: Host:  metasploitable.localdomain; 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 1.92 seconds
```

Fast Scanning

i) nmap –F 192.168.147.129

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -F 192.168.147.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 21:29 EST
Nmap scan report for 192.168.147.129
Host is up (0.00013s 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:CB:2E:CD (VMware)

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

ii) nmap –F -sV 192.168.147.129

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -F -sV 192.168.147.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 21:29 EST
Nmap scan report for 192.168.147.129
Host is up (0.00012s latency).
Not shown: 82 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)
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
MAC Address: 00:0C:29:CB:2E:CD (VMware)
Service Info: Host:  metasploitable.localdomain; 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 11.87 seconds
```

Aggressive Scanning

i) nmap –A 192.168.147.129

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.147.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 21:30 EST
Nmap scan report for 192.168.147.129
Host is up (0.00099s 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 192.168.147.128
|      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 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES,
8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no s
uch thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
|_ssl-date: 2022-11-21T14:24:58+00:00; -15d12h05m44s from scanner time.
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
```

```
|_ssl-date: 2022-11-21T14:24:58+00:00; -15d12h05m44s from scanner time.
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2          111/tcp   rpcbind
|   100000  2          111/udp   rpcbind
|   100003  2,3,4      2049/tcp   nfs
|   100003  2,3,4      2049/udp   nfs
|   100005  1,2,3      58362/udp   mountd
|   100005  1,2,3      59050/tcp   mountd
|   100021  1,3,4      42462/udp   nlockmgr
|   100021  1,3,4      44521/tcp   nlockmgr
|   100024  1          42329/tcp   status
|_  100024  1          42617/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsCompression, LongColumnFlag, SwitchToSSLAfterHandshake, SupportsTrans
actions, ConnectWithDatabase, Speaks41ProtocolNew
|   Status: Autocommit
|_  Salt: Nd,M!Xxuds6Rx(YgzPaw
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2022-11-21T14:24:58+00:00; -15d12h05m44s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no s
uch thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
```

```
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2022-11-21T14:24:58+00:00; -15d12h05m44s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no s
uch thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 1:00:42
|   source ident: nmap
|   source host: A8E68A13.578A7F3A.FFFA6D49.IP
|_  error: Closing Link: thezlnkts[192.168.147.128] (Quit: thezlnkts)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 00:0C:29:CB:2E:CD (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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux
_kernel

Host script results:
|_clock-skew: mean: -15d10h50m43s, deviation: 2h30m00s, median: -15d12h05m44s
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
```

```
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 00:0C:29:CB:2E:CD (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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux
_kernel

Host script results:
|_clock-skew: mean: -15d10h50m43s, deviation: 2h30m00s, median: -15d12h05m44s
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-11-21T09:24:47-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   0.99 ms 192.168.147.129

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 26.36 seconds
```

TCP Scanning

i) nmap –sT 192.168.147.129

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.147.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 21:33 EST
Nmap scan report for 192.168.147.129
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (conn-refused)
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:CB:2E:CD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

ii) nmap –sT –p 21-30 –sV –O 192.168.147.129

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT -p 21-30 -sV -O 192.168.147.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 21:33 EST
Nmap scan report for 192.168.147.129
Host is up (0.00063s latency).
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
24/tcp closed priv-mail
25/tcp open   smtp      Postfix smtpd
26/tcp closed rsftp
27/tcp closed nsw-fe
28/tcp closed unknown
29/tcp closed msg-icp
30/tcp closed unknown
MAC Address: 00:0C:29:CB:2E:CD (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
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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 1.95 seconds
```

UDP Scanning

i) nmap –sU 192.168.147.129

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sU 192.168.147.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 21:34 EST
Warning: 192.168.147.129 giving up on port because retransmission cap hit (10).
Stats: 0:06:34 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 20.25% done; ETC: 22:06 (0:25:52 remaining)
Stats: 0:11:45 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 35.15% done; ETC: 22:07 (0:21:39 remaining)
Nmap scan report for 192.168.147.129
Host is up (0.00076s latency).
Not shown: 967 closed udp ports (port-unreach), 29 open|filtered udp ports (no-response)
PORT     STATE SERVICE
53/udp   open  domain
111/udp  open  rpcbind
137/udp  open  netbios-ns
2049/udp open  nfs
MAC Address: 00:0C:29:CB:2E:CD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1409.04 seconds
```

ii) nmap –sU –p 21-30 192.168.147.129

iii) nmap –sU –p 21-30 –sV –O 192.168.147.129

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sU -p 21-30 192.168.147.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 21:39 EST
Nmap scan report for 192.168.147.129
Host is up (0.00030s latency).

PORT   STATE         SERVICE
21/udp open|filtered ftp
22/udp open|filtered ssh
23/udp open|filtered telnet
24/udp open|filtered priv-mail
25/udp open|filtered smtp
26/udp open|filtered unknown
27/udp open|filtered nsw-fe
28/udp open|filtered unknown
29/udp open|filtered msg-icp
30/udp open|filtered unknown
MAC Address: 00:0C:29:CB:2E:CD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.53 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sU -p 21-30 -sV -O 192.168.147.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 21:40 EST
Nmap scan report for 192.168.147.129
Host is up (0.00046s latency).

PORT   STATE         SERVICE   VERSION
21/udp open|filtered ftp
22/udp open|filtered ssh
23/udp open|filtered telnet
24/udp open|filtered priv-mail
25/udp open|filtered smtp
26/udp open|filtered unknown
27/udp open|filtered nsw-fe
28/udp open|filtered unknown
29/udp open|filtered msg-icp
30/udp open|filtered unknown
MAC Address: 00:0C:29:CB:2E:CD (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

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 102.43 seconds
```