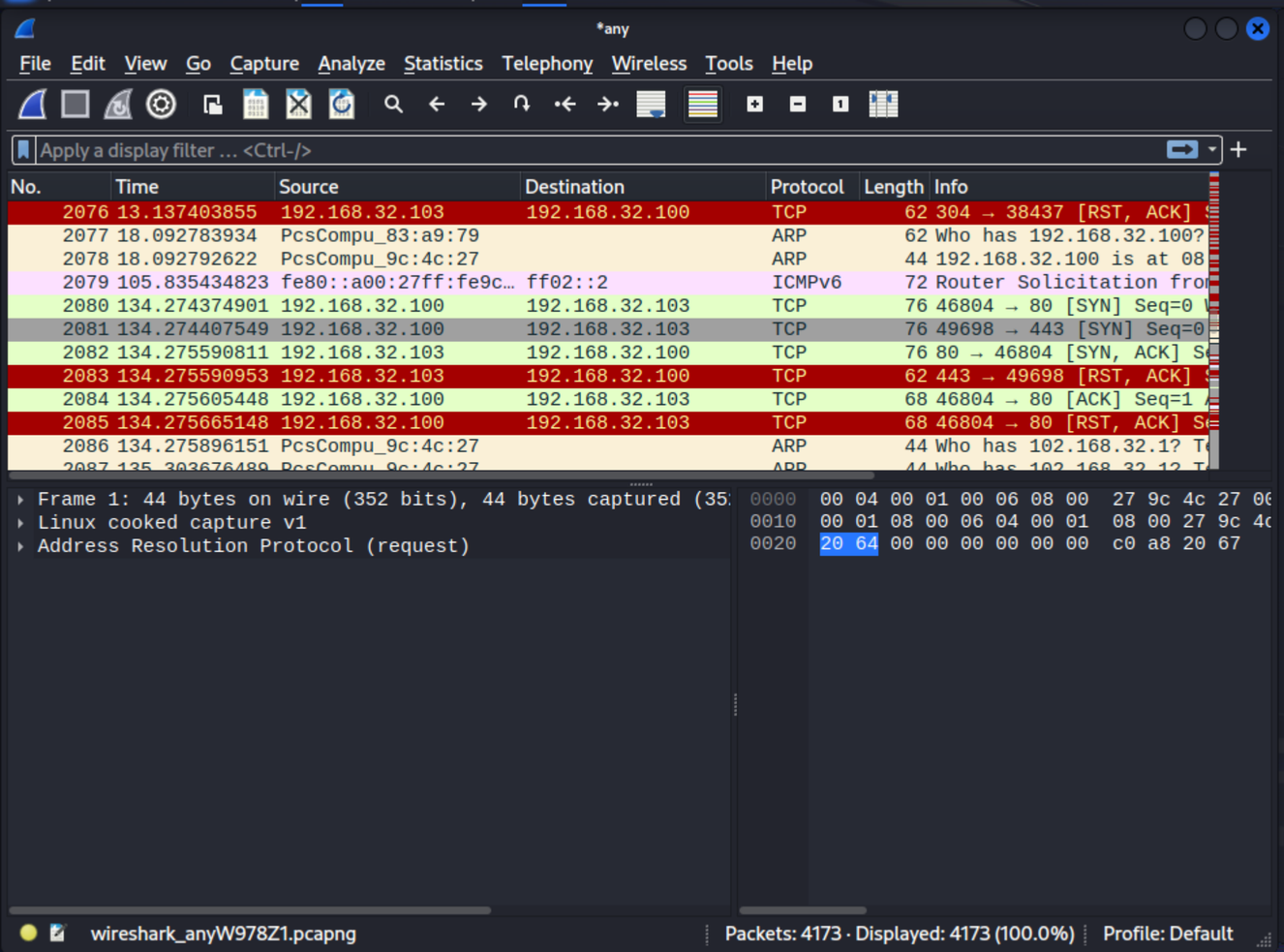
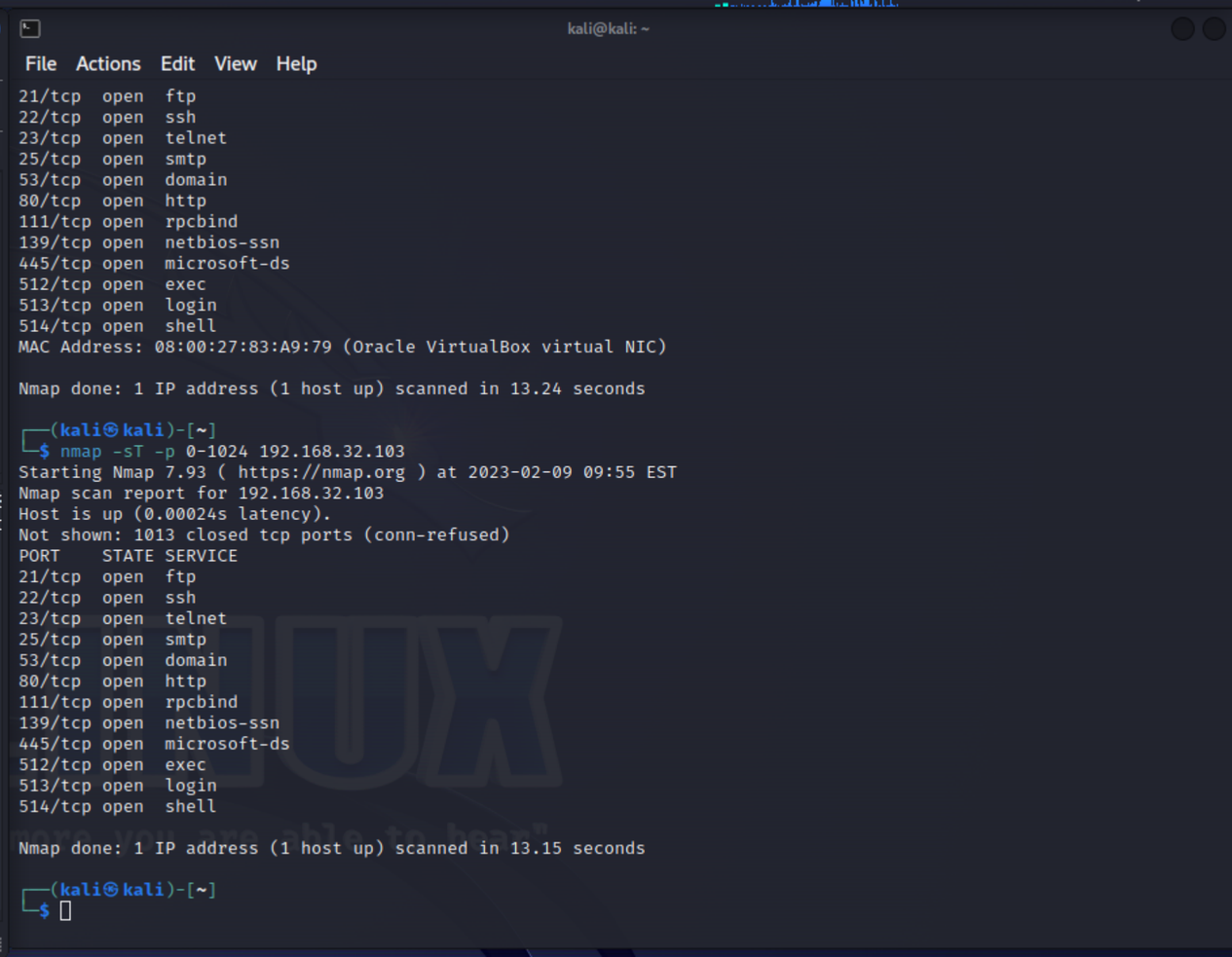
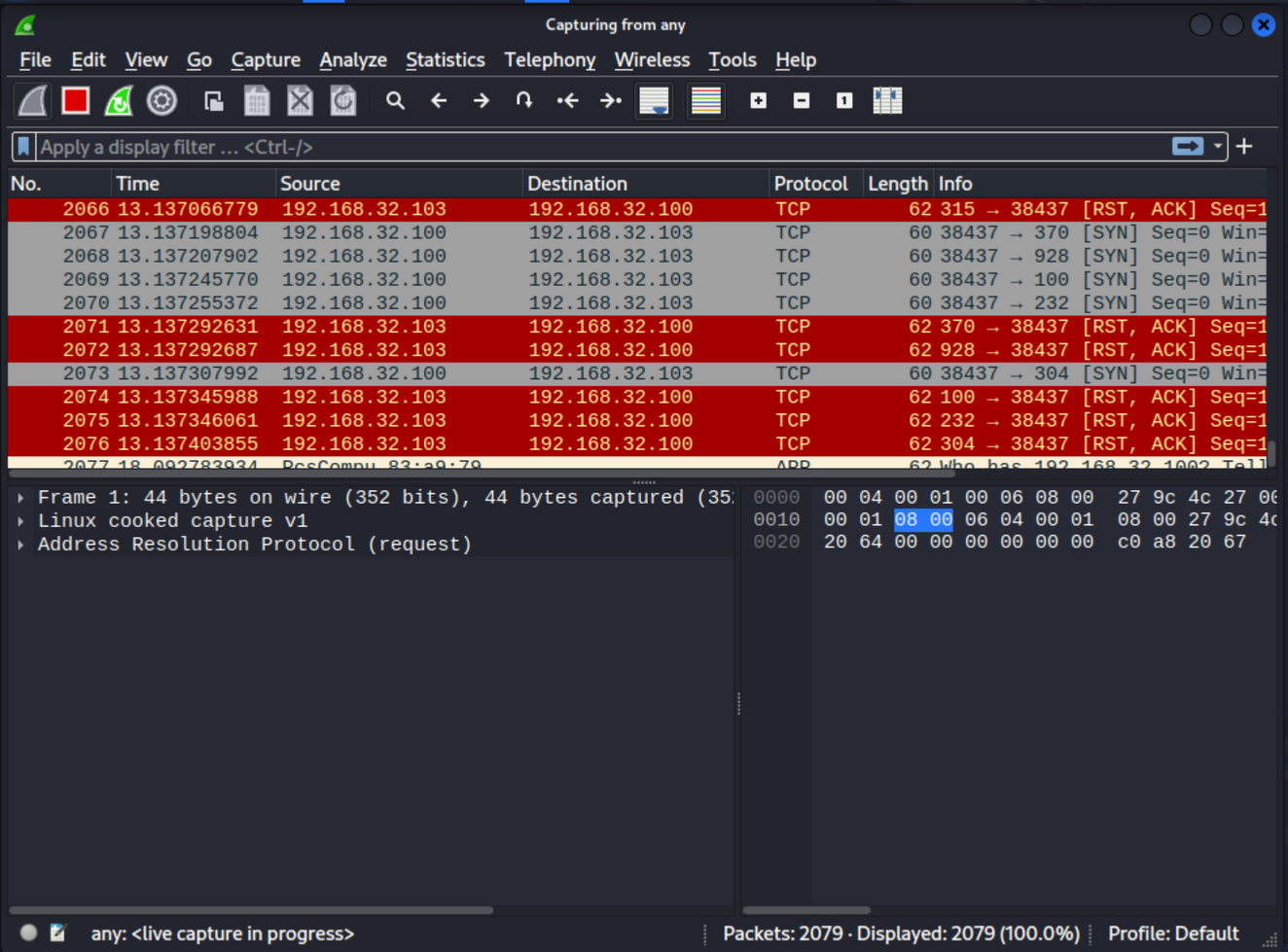
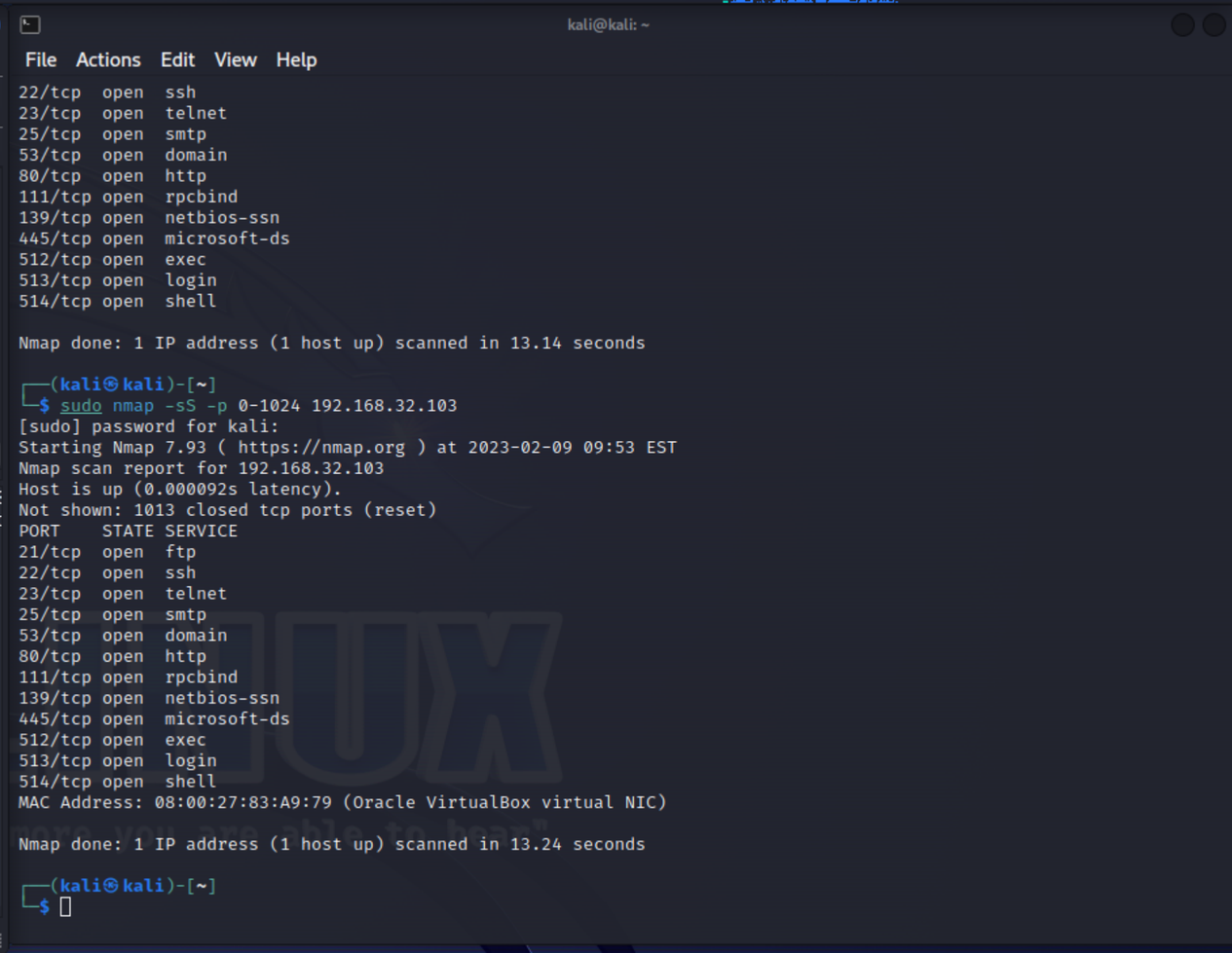

*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
2076 13.137403855 192.168.32.103 192.168.32.100 TCP 62 304 → 38437 [RST, ACK]
2077 18.092783934 PcsCompu_83:a9:79 ARP 62 Who has 192.168.32.100?
2078 18.092792622 PcsCompu_9c:4c:27 ARP 44 192.168.32.100 is at 08
2079 105.835434823 fe80::a00:27ff:fe9c… ff02::2 ICMPv6 72 Router Solicitation fro
2080 134.274374901 192.168.32.100 192.168.32.103 TCP 76 46804 → 80 [SYN] Seq=0
2081 134.274407549 192.168.32.100 192.168.32.103 TCP 76 49698 → 443 [SYN] Seq=0
2082 134.275590811 192.168.32.103 192.168.32.100 TCP 76 80 → 46804 [SYN, ACK]
2083 134.275590953 192.168.32.103 192.168.32.100 TCP 62 443 → 49698 [RST, ACK]
2084 134.275605448 192.168.32.100 192.168.32.103 TCP 68 46804 → 80 [ACK] Seq=1
2085 134.275665148 192.168.32.100 192.168.32.103 TCP 68 46804 → 80 [RST, ACK]
2086 134.275896151 PcsCompu_9c:4c:27 ARP 44 Who has 102.168.32.1? T
Frame 1: 44 bytes on wire (352 bits), 44 bytes captured (35
Linux cooked capture v1
Address Resolution Protocol (request)
0000 00 04 00 01 00 06 08 00 27 9c 4c 27 0
0010 00 01 08 00 06 04 00 01 08 00 27 9c 4
0020 20 64 00 00 00 00 00 00 c0 a8 20 67
wireshark_anyW978Z1.pcapng
Packets: 4173 · Displayed: 4173 (100.0%)
Profile: Default


kali@kali: ~
File Actions Edit View Help
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
MAC Address: 08:00:27:83:A9:79 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
(kali㉿kali)-[~]
$ nmap -sT -p 0-1024 192.168.32.103
Starting Nmap 7.93 (https://nmap.org) at 2023-02-09 09:55 EST
Nmap scan report for 192.168.32.103
Host is up (0.00024s latency).
Not shown: 1013 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
Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds
(kali㉿kali)-[~]
$


Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
2066 13.137066779 192.168.32.103 192.168.32.100 TCP 62 315 → 38437 [RST, ACK] Seq=1
2067 13.137198804 192.168.32.100 192.168.32.103 TCP 60 38437 → 370 [SYN] Seq=0 Win=
2068 13.137207902 192.168.32.100 192.168.32.103 TCP 60 38437 → 928 [SYN] Seq=0 Win=
2069 13.137245770 192.168.32.100 192.168.32.103 TCP 60 38437 → 100 [SYN] Seq=0 Win=
2070 13.137255372 192.168.32.100 192.168.32.103 TCP 60 38437 → 232 [SYN] Seq=0 Win=
2071 13.137292631 192.168.32.103 192.168.32.100 TCP 62 370 → 38437 [RST, ACK] Seq=1
2072 13.137292687 192.168.32.103 192.168.32.100 TCP 62 928 → 38437 [RST, ACK] Seq=1
2073 13.137307992 192.168.32.100 192.168.32.103 TCP 60 38437 → 304 [SYN] Seq=0 Win=
2074 13.137345988 192.168.32.103 192.168.32.100 TCP 62 100 → 38437 [RST, ACK] Seq=1
2075 13.137346061 192.168.32.103 192.168.32.100 TCP 62 232 → 38437 [RST, ACK] Seq=1
2076 13.137403855 192.168.32.103 192.168.32.100 TCP 62 304 → 38437 [RST, ACK] Seq=1
Frame 1: 44 bytes on wire (352 bits), 44 bytes captured (35
Linux cooked capture v1
Address Resolution Protocol (request)
0000 00 04 00 01 00 06 08 00 27 9c 4c 27
0010 00 01 08 00 06 04 00 01 08 00 27 9c
0020 20 64 00 00 00 00 00 00 c0 a8 20 67
any: <live capture in progress>
Packets: 2079 · Displayed: 2079 (100.0%)
Profile: Default


kali@kali: ~
File Actions Edit View Help
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
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
(kali㉿kali)-[~]
$ sudo nmap -sS -p 0-1024 192.168.32.103
[sudo] password for kali:
Starting Nmap 7.93 (https://nmap.org) at 2023-02-09 09:53 EST
Nmap scan report for 192.168.32.103
Host is up (0.000092s latency).
Not shown: 1013 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
MAC Address: 08:00:27:83:A9:79 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
(kali㉿kali)-[~]
$

File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -p 0-1024 192.168.32.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 09:58 EST
Nmap scan report for 192.168.32.103
Host is up (0.00030s latency).
Not shown: 1013 closed tcp ports (conn-refused)
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 192.168.32.100
|      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
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8B
ITMIME, DSN
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      33674/tcp   mountd
|   100005  1,2,3      34230/udp   mountd
|   100021  1,3,4      32822/tcp   nlockmgr
```

File Actions Edit View Help

```
| 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      33674/tcp   mountd
|   100005  1,2,3      34230/udp   mountd
|   100021  1,3,4      32822/tcp   nlockmgr
|   100021  1,3,4      36294/udp   nlockmgr
|   100024  1          34015/udp   status
|_  100024  1          55232/tcp   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?
514/tcp open  shell       Netkit rshd
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 3h30m06s, deviation: 3h32m17s, median: 59m59s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-02-09T10:59:23-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 100.32 seconds

┌──(kali㉿kali)-[~]
└─$
```