

## Task 1 Scan Your Local Network for Open Ports - Screenshots

### 1. Attacker machine: Ip

```
(kali@kali)-[~]
$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

### 2. TCP SYN scan

```
(kali@kali)-[~]
$ nmap -sS 10.0.2.0/24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 13:24 EDT

Nmap scan report for 10.0.2.4
Host is up (0.0010s 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

Nmap done: 256 IP addresses (3 hosts up) scanned in 28.45 seconds
```

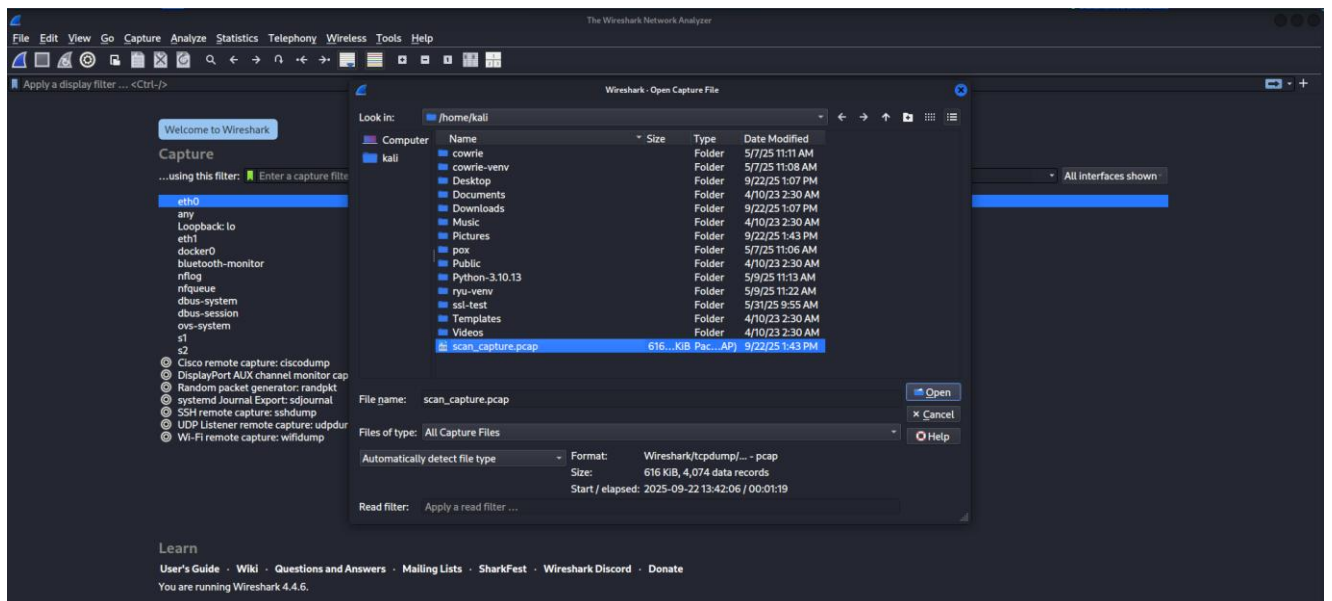
### 3. tcpdump packet\_capture.pcap

```
(kali㉿kali)-[~]
$ sudo tcpdump -i eth0 -w scan_capture.pcap

[sudo] password for kali:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C4074 packets captured
4076 packets received by filter
0 packets dropped by kernel

(kali㉿kali)-[~]
$
```

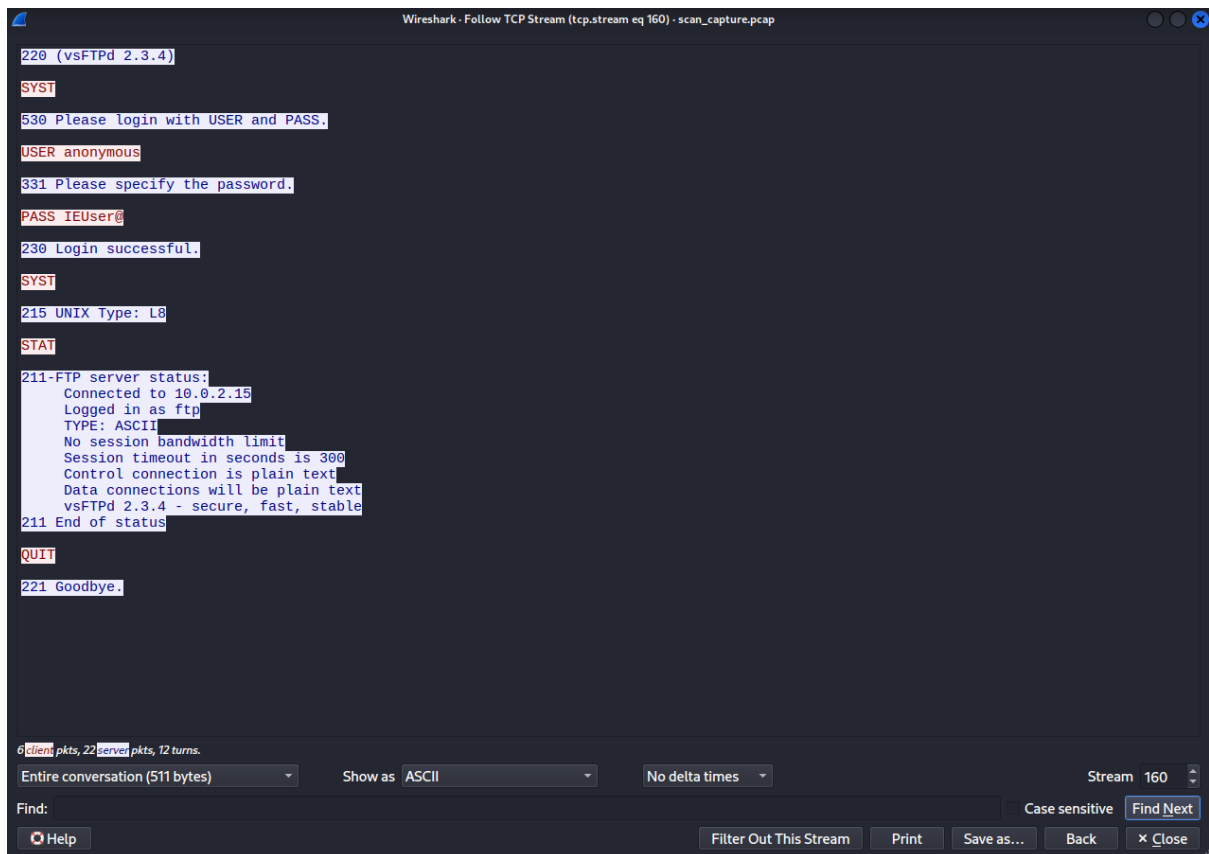
### 4. Analysis with Wireshark



### 5. Info: Login successful

No.	Date/Time	Source	Source Port	Destination	Dest Port	Protocol	Length	Info
1408	2025-09-22 13:42:46.569292	10.0.2.15	59148	10.0.2.4	21	TCP	74	59148 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2900706300 TSecr=0
1410	2025-09-22 13:42:46.570041	10.0.2.4	21	10.0.2.15	59148	TCP	74	21 → 59148 [SYN, ACK] Seq=9 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=22823 TSecr=22823
1411	2025-09-22 13:42:46.570967	10.0.2.15	59148	10.0.2.4	21	TCP	66	59148 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2900706301 TSecr=22823
1456	2025-09-22 13:42:46.648115	10.0.2.4	21	10.0.2.15	59148	FTP	86	Response: 220 (vsFTPd 2.3.4)
1457	2025-09-22 13:42:46.648143	10.0.2.15	59148	10.0.2.4	21	TCP	66	59148 → 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 TSval=2900706379 TSecr=22826
1472	2025-09-22 13:42:46.684864	10.0.2.15	59148	10.0.2.4	21	FTP	72	Request: SYST
1485	2025-09-22 13:42:46.694834	10.0.2.4	21	10.0.2.15	59148	TCP	66	21 → 59148 [ACK] Seq=21 Ack=7 Win=5792 Len=0 TSval=22828 TSecr=2900706416
1495	2025-09-22 13:42:46.709444	10.0.2.4	21	10.0.2.15	59148	FTP	104	Response: 530 Please login with USER and PASS.
1496	2025-09-22 13:42:46.709467	10.0.2.15	59148	10.0.2.4	21	TCP	66	59148 → 21 [ACK] Seq=7 Ack=59 Win=64256 Len=0 TSval=2900706440 TSecr=22828
1535	2025-09-22 13:42:46.793324	10.0.2.15	59148	10.0.2.4	21	FTP	82	Request: USER anonymous
1545	2025-09-22 13:42:46.802112	10.0.2.4	21	10.0.2.15	59148	FTP	100	Response: 331 Please specify the password.
1546	2025-09-22 13:42:46.802149	10.0.2.15	59148	10.0.2.4	21	TCP	66	59148 → 21 [ACK] Seq=23 Ack=93 Win=64256 Len=0 TSval=2900706533 TSecr=22831
1660	2025-09-22 13:42:53.071222	10.0.2.15	59148	10.0.2.4	21	FTP	80	Request: PASS IEUser@
1663	2025-09-22 13:42:53.093055	10.0.2.4	21	10.0.2.15	59148	FTP	63	Response: 230 Login successful
1664	2025-09-22 13:42:53.109834	10.0.2.15	59148	10.0.2.4	21	TCP	66	59148 → 21 [ACK] Seq=37 Ack=116 Win=64256 Len=0 TSval=2900706841 TSecr=23097
1735	2025-09-22 13:42:53.184681	10.0.2.15	59148	10.0.2.4	21	FTP	72	Request: SYST
1753	2025-09-22 13:42:53.197951	10.0.2.4	21	10.0.2.15	59148	FTP	85	Response: 215 UNIX Type: L8
1754	2025-09-22 13:42:53.197976	10.0.2.15	59148	10.0.2.4	21	TCP	66	59148 → 21 [ACK] Seq=43 Ack=135 Win=64256 Len=0 TSval=2900706928 TSecr=23100
1780	2025-09-22 13:42:53.291257	10.0.2.15	59148	10.0.2.4	21	FTP	72	Request: STAT
1780	2025-09-22 13:42:53.316811	10.0.2.4	21	10.0.2.15	59148	FTP	90	Response: 211-FTP server status:
1789	2025-09-22 13:42:53.316922	10.0.2.15	59148	10.0.2.4	21	TCP	66	59148 → 21 [ACK] Seq=49 Ack=159 Win=64256 Len=0 TSval=2900707048 TSecr=23104
1790	2025-09-22 13:42:53.318747	10.0.2.4	21	10.0.2.15	59148	FTP	84	Response: Connected to
1791	2025-09-22 13:42:53.318771	10.0.2.15	59148	10.0.2.4	21	TCP	66	59148 → 21 [ACK] Seq=49 Ack=177 Win=64256 Len=0 TSval=2900707050 TSecr=23104
1792	2025-09-22 13:42:53.319107	10.0.2.4	21	10.0.2.15	59148	FTP	75	Response: 10.0.2.15
1793	2025-09-22 13:42:53.319114	10.0.2.15	59148	10.0.2.4	21	TCP	66	59148 → 21 [ACK] Seq=49 Ack=186 Win=64256 Len=0 TSval=2900707050 TSecr=23104
1794	2025-09-22 13:42:53.319502	10.0.2.4	21	10.0.2.15	59148	FTP	68	Response: Logged in as
1795	2025-09-22 13:42:53.319553	10.0.2.15	59148	10.0.2.4	21	TCP	84	Response: 500
1796	2025-09-22 13:42:53.319566	10.0.2.15	59148	10.0.2.4	21	TCP	66	59148 → 21 [ACK] Seq=49 Ack=188 Win=64256 Len=0 TSval=2900707051 TSecr=23104
1797	2025-09-22 13:42:53.320623	10.0.2.15	59148	10.0.2.4	21	TCP	66	59148 → 21 [ACK] Seq=49 Ack=206 Win=64256 Len=0 TSval=2900707051 TSecr=23104
1798	2025-09-22 13:42:53.320763	10.0.2.4	21	10.0.2.15	59148	FTP	69	Response: ftp
1799	2025-09-22 13:42:53.320884	10.0.2.15	59148	10.0.2.4	21	TCP	66	59148 → 21 [ACK] Seq=49 Ack=209 Win=64256 Len=0 TSval=2900707052 TSecr=23104
1800	2025-09-22 13:42:53.321180	10.0.2.4	21	10.0.2.15	59148	FTP	68	Response: 211-FTP server status:
1801	2025-09-22 13:42:53.321187	10.0.2.15	59148	10.0.2.4	21	TCP	66	59148 → 21 [ACK] Seq=49 Ack=222 Win=64256 Len=0 TSval=2900707052 TSecr=23104
1802	2025-09-22 13:42:53.321913	10.0.2.4	21	10.0.2.15	59148	FTP	77	Response: TYPE:
1803	2025-09-22 13:42:53.321920	10.0.2.15	59148	10.0.2.4	21	TCP	66	59148 → 21 [ACK] Seq=49 Ack=222 Win=64256 Len=0 TSval=2900707053 TSecr=23104
1804	2025-09-22 13:42:53.322211	10.0.2.4	21	10.0.2.15	59148	FTP	73	Response: ASCII
1805	2025-09-22 13:42:53.322218	10.0.2.15	59148	10.0.2.4	21	TCP	66	59148 → 21 [ACK] Seq=49 Ack=229 Win=64256 Len=0 TSval=2900707053 TSecr=23104

## 6. TCP stream showcases



The image shows the 'Follow TCP Stream' window in Wireshark, displaying a text-based FTP session. The window title is 'Wireshark - Follow TCP Stream (tcp.stream eq 160) - scan\_capture.pcap'. The session details are as follows:

```
220 (vsFTPd 2.3.4)
SYST
530 Please login with USER and PASS.
USER anonymous
331 Please specify the password.
PASS IEUser@
230 Login successful.
SYST
215 UNIX Type: L8
STAT
211-FTP server status:
  Connected to 10.0.2.15
  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
211 End of status
QUIT
221 Goodbye.
```

At the bottom of the window, the status bar indicates '6 client pkts, 22 server pkts, 12 turns'. Below this, there are controls for 'Entire conversation (511 bytes)', 'Show as ASCII', 'No delta times', and 'Stream 160'. A 'Find:' search bar is also present, with 'Case sensitive' and 'Find Next' options. At the very bottom, there are buttons for 'Help', 'Filter Out This Stream', 'Print', 'Save as...', 'Back', and 'Close'.