

CT1406 Network Security Lab

Server IP is: 10.170.26.161

1. Perform a port scan that aims to check whether the Server machine is alive or not.

Command used:

2. Perform a Scan to the Server machine on the well-known ports.

Command used:

3. Perform a scan that the Server may not be able to detect on port 80.

Command used:

4. Perform a scan that the Server may not be able to detect on the DNS port.

Command used:

5. Perform a scan to discover the operating system of the target machine (server).

Command used:

No.	Time	Source	Destination	Protocol	Length	Info
193	9.910150000	10.170.25.101	10.170.25.102	TCP	66	2462->6112 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
194	9.911099000	10.170.25.102	10.170.25.101	TCP	54	6112->2462 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
207	10.410060000	10.170.25.101	10.170.25.102	TCP	66	[TCP Spurious Retransmission] 2462->6112 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
208	10.411687000	10.170.25.102	10.170.25.101	TCP	54	6112->2462 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
221	10.910155000	10.170.25.101	10.170.25.102	TCP	66	[TCP Spurious Retransmission] 2462->6112 [SYN] Seq=0 win=8192 Len=0 MSS=1460 SACK_PERM=1
222	10.910773000	10.170.25.102	10.170.25.101	TCP	54	6112->2462 [RST, ACK] Seq=1 Ack=1 win=0 Len=0

Based on the screenshot above determine the following:

- Scanner port no:
- Target scanned port no:
- Target port state:

No.	Time	Source	Destination	Protocol	Length	Info
10	3.775811000	10.170.25.101	10.170.25.102	TCP	66	2430->139 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
15	3.783826000	10.170.25.102	10.170.25.101	TCP	66	139->2430 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
19	3.783913000	10.170.25.101	10.170.25.102	TCP	54	2430->139 [ACK] Seq=1 Ack=1 win=65700 Len=0
23	3.784034000	10.170.25.101	10.170.25.102	TCP	54	2430->139 [RST, ACK] Seq=1 Ack=1 win=0 Len=0

- Scanner IP:
- Target IP:
- Scanning type:
- Target port state:

Determine the Version no. of ports 22,53,80,21