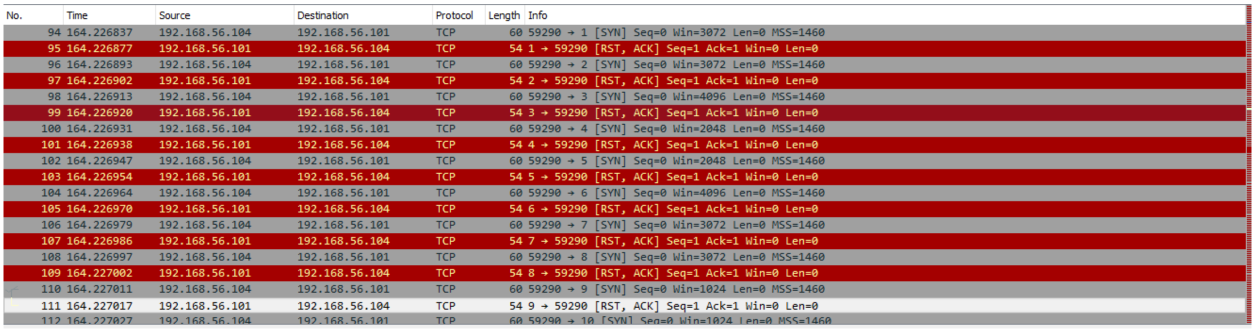
1-Abstract

Summary:

After a thorough analysis of the packet capture file named as Networkcapture1.pcap, Evidence of **Port Scanning attack** have been found by the attacking machine with the IP address 192.168.56.104 on to the victim machine with the IP address 192.168.56.101.

Capture Overview:

In the picture down below it can be seen that the Attacker is continuously sending SYN packets to the Victim's machine from port number 59290.



No.	Time	Source	Destination	Protocol	Length	Info
94	164.226837	192.168.56.104	192.168.56.101	TCP	60	59290 → 1 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
95	164.226877	192.168.56.101	192.168.56.104	TCP	54	1 → 59290 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
96	164.226893	192.168.56.104	192.168.56.101	TCP	60	59290 → 2 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
97	164.226902	192.168.56.101	192.168.56.104	TCP	54	2 → 59290 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
98	164.226913	192.168.56.104	192.168.56.101	TCP	60	59290 → 3 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
99	164.226920	192.168.56.101	192.168.56.104	TCP	54	3 → 59290 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
100	164.226931	192.168.56.104	192.168.56.101	TCP	60	59290 → 4 [SYN] Seq=0 Win=2048 Len=0 MSS=1460
101	164.226938	192.168.56.101	192.168.56.104	TCP	54	4 → 59290 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
102	164.226947	192.168.56.104	192.168.56.101	TCP	60	59290 → 5 [SYN] Seq=0 Win=2048 Len=0 MSS=1460
103	164.226954	192.168.56.101	192.168.56.104	TCP	54	5 → 59290 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
104	164.226964	192.168.56.104	192.168.56.101	TCP	60	59290 → 6 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
105	164.226970	192.168.56.101	192.168.56.104	TCP	54	6 → 59290 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
106	164.226979	192.168.56.104	192.168.56.101	TCP	60	59290 → 7 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
107	164.226986	192.168.56.101	192.168.56.104	TCP	54	7 → 59290 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
108	164.226997	192.168.56.104	192.168.56.101	TCP	60	59290 → 8 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
109	164.227002	192.168.56.101	192.168.56.104	TCP	54	8 → 59290 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
110	164.227011	192.168.56.104	192.168.56.101	TCP	60	59290 → 9 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
111	164.227017	192.168.56.101	192.168.56.104	TCP	54	9 → 59290 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
112	164.227027	192.168.56.104	192.168.56.101	TCP	60	59290 → 10 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

The port scan by the Attacker is done on 65,534 ports of Victim's machine.

Analysis Tool Used:

The PCAP file was analyzed using **Wireshark** desktop application.

2-Findings

Protocol Breakdown:

The protocols used in the file are the following:

HTTP (Hypertext transfer Protocol): HTTP (Hypertext Transfer Protocol) is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols (the foundation protocols for the Internet).

TCP (Transmission Control Protocol): TCP (Transmission Control Protocol) is an important network protocol that is used in the transmission of data over networks. A protocol, in the context of networks, is a set of rules and procedures that govern how the transmission of data is carried out so that everyone in the whole world, independent of the location, software or hardware used, does the thing the same way. TCP works together with IP (Internet Protocol) in a well-known duo called TCP/IP.

Actors Involved:

Victim: 192.168.56.101

Attacker: 192.168.56.104

Suspected machine: 192.168.56.1

Timeline of Events:

1. Some Suspected machine with the IP 192.168.56.1 accesses the machine 192.168.56.101(victim) and makes requests which are within the legal bounds of the protocol.

2. Attacker machine starts sending SYN packets to the victim’s machine and starts to scan the ports of the victim.
3. After the scanning is completed the normal request exchange starts taking place between 192.168.56.1 and 192.168.56.101.

Malicious Behavior:

Indicators of Compromise	**Indicators of Attack**
No compromisation of data was seen in the pcap file.	The attacker was using Port Scanning Attack.
	The intention could have been numerous involving transfer of malicious data through an Open port or gathering of vital information about the victim’s OS etc.

3-Mitigation

- The Port Scan attack can be effectively reduced (if not completely solved) by deploying Firewalls at critical locations of a network to filter un-wanted traffic and from iffy sources. There are many Port Scan detecting tools and products available on the market. For Linux systems, there is an open source program Port Scan Attack Detector (PSAD) available for free using.
- To detect the port scan attack, the security device should log the number of different port scan request coming from the remote source. The default settings for pre-defined interval of port scan attack (if a remote host scan 9 ports in 0.005 seconds) is used to identify the port scan attack.
- Depending on the severity of the attack, the default port scan interval and burst rate could be defined using the IP-Tables for countering such attack. If any source is found sending such packets then such packets needs to be flagged as a port scan attack and the security device would reject all further packets from the remote source. The security device would detect and drop the tenth packet that meets the port scan attack measure thus dropping all the subsequent packets of port scan.

4-Appendix

Table of carved files:

S.No	Filename
1.	Networkcapture1.pcap

Wireshark Filter Used:

TCP