

Lab-2 Report

AIM: Packet Capture and Network Traffic Analysis Using Wireshark & tcpdump

1. Introduction

The purpose of this lab is to provide hands-on experience in capturing and analyzing network traffic to identify potential security threats. Using tools like **Wireshark** and **tcpdump**, students will learn how to detect various types of attacks and security anomalies in a network, including **DoS attacks**, **port scanning**, **ARP spoofing**, **DNS spoofing**, and **cleartext data transmission**. These tools allow for detailed inspection of network traffic, providing insights into potential vulnerabilities and threats in a network environment.

2. Objective

- To use **Wireshark** and **tcpdump** for capturing and analyzing network traffic.
- To detect potential security threats and abnormal patterns such as SYN Floods, port scanning, ARP poisoning, DNS spoofing, and cleartext transmission of sensitive data.

3. Tools & Resources

- **Wireshark:** A graphical network protocol analyzer.
 - Official site: Wireshark
- **tcpdump:** A command-line network packet analyzer.
 - Installation for Linux: `sudo apt install tcpdump`
- **Kali Linux** (for simulating attacks)
- **Ubuntu/Windows** (for performing normal operations and being attacked)
- **Nmap** (for scanning and testing vulnerabilities)

4. Methodology

4.1. Installation & Setup

1. **Wireshark** was installed on the system, ensuring that the network interface was correctly selected for packet capture.
2. **tcpdump** was installed on both Kali Linux and Ubuntu systems to capture traffic from a command-line interface.
3. A **Virtual Lab Network** was created using virtual machines, assigning static IP addresses (e.g., Kali: 192.168.1.1, Ubuntu: 192.168.1.2) to allow safe and controlled testing of network behaviors.

5. Results

SYN Flood Attack

Capturing on Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.syn == 1 && tcp.flags.ack == 0

No.	Time	Source	Destination	Protocol	Length	Info
313053	96.399992	10.10.15.76	49.44.103.51	TCP	66	63703 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
313054	96.400383	10.10.15.76	49.44.103.51	TCP	66	63704 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
313055	96.400442	10.10.15.76	49.44.103.51	TCP	66	63705 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
313056	96.401199	10.10.15.76	49.44.103.51	TCP	66	63706 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
313057	96.401199	10.10.15.76	49.44.103.51	TCP	66	63707 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
313208	97.567779	10.10.15.76	204.79.197.222	TCP	66	63708 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
313339	100.718301	10.10.15.76	13.107.253.48	TCP	66	63709 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
313384	101.944042	10.10.15.76	52.149.152.135	TCP	66	63710 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
313424	103.989395	10.10.15.76	52.231.217.206	TCP	66	63711 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
313450	105.921345	10.10.15.64	10.10.15.76	TCP	66	56189 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
340356	112.445416	10.10.15.76	49.44.166.99	TCP	66	63712 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
601750	157.014368	10.10.15.76	23.45.47.89	TCP	66	63714 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
624435	158.533388	10.10.15.76	10.10.15.174	TCP	66	63715 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
680256	190.548547	10.10.15.76	10.10.15.86	TCP	66	63716 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
701917	225.943721	10.10.15.64	10.10.15.76	TCP	66	56214 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
732006	230.572160	10.10.15.76	10.10.15.113	TCP	66	63717 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
801338	278.596268	10.10.15.76	10.10.15.89	TCP	66	63718 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1001093	318.621060	10.10.15.76	10.10.15.164	TCP	66	63719 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1103212	345.965357	10.10.15.64	10.10.15.76	TCP	66	56229 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1150983	381.011265	10.10.15.76	52.182.143.214	TCP	66	63721 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1150924	384.609531	10.10.15.76	13.107.246.68	TCP	66	63722 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1150951	385.619766	10.10.15.76	52.191.219.104	TCP	66	63723 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1244427	398.655107	10.10.15.76	10.10.15.174	TCP	66	63724 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1543447	438.667276	10.10.15.76	10.10.15.86	TCP	66	63725 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1563920	478.689360	10.10.15.76	10.10.15.113	TCP	66	63726 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1578994	485.571907	10.10.15.76	52.109.124.29	TCP	66	63727 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1617056	513.091925	10.10.15.76	13.107.5.93	TCP	66	63728 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM

Frame 1150983: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface DeviceVNF (A2B1644D-C6A6)

Ethernet II, Src: HP_Gigaset9c (00:60:8b:9c:ee:9c), Dst: PaloAltoNet_80:8e:10 (3c:fa:30:00:0e:10)

Internet Protocol Version 4, Src: 10.10.15.76, Dst: 13.107.246.68

Transmission Control Protocol, Src Port: 63722, Dst Port: 443, Seq: 0, Len: 0

Source Port: 63722

Destination Port: 443

[Stream index: 30]

[Conversation completeness: Complete, WITH_DATA (63)]

... .. = RST: Present

... .. = FIN: Present

... .. = Data: Present

... .. = ACK: Present

... .. = SYN-ACK: Present

... .. = SYN: Present

[Completeness Flags: RSTACK]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 131735503

Window: 0

Source Port: 63722

Destination Port: 443

Bytes: 164057 - Displayed: 33.0 (0%)

Profile: Default

Port Scanning

Capturing on Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 443

No.	Time	Source	Destination	Protocol	Length	Info
68416	29.631953	10.10.15.76	142.250.183.200	TCP	55	63771 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1
68495	29.643194	142.250.183.200	10.10.15.76	TCP	66	443 → 63771 [ACK] Seq=1 Ack=2 Win=1047 Len=0 SLE=1 SRE=2
73849	30.315703	10.10.15.76	104.18.32.47	TCP	55	63772 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1
73950	30.327098	10.10.15.76	104.18.32.47	TCP	66	443 → 63772 [ACK] Seq=1 Ack=2 Win=11 Len=0 SLE=1 SRE=2
73907	30.821390	10.10.15.76	104.16.80.73	TCP	55	63780 → 443 [ACK] Seq=1 Ack=1 Win=251 Len=1
73908	30.835329	10.10.15.76	10.10.15.76	TCP	66	443 → 63780 [ACK] Seq=1 Ack=2 Win=11 Len=0 SLE=1 SRE=2
73909	30.964593	10.10.15.76	216.239.36.178	TCP	55	63782 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1
73910	30.977407	216.239.36.178	10.10.15.76	TCP	66	443 → 63782 [ACK] Seq=1 Ack=2 Win=1047 Len=0 SLE=1 SRE=2
73920	31.601201	10.10.15.76	104.18.41.158	TCP	55	63783 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1
73921	31.614907	104.18.41.158	10.10.15.76	TCP	66	443 → 63783 [ACK] Seq=1 Ack=2 Win=0 Len=0 SLE=1 SRE=2
75275	34.057180	10.10.15.76	142.250.70.74	TCP	55	63786 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1
75276	34.073030	142.250.70.74	10.10.15.76	TCP	66	443 → 63786 [ACK] Seq=1 Ack=2 Win=1047 Len=0 SLE=1 SRE=2
75281	34.611901	52.113.194.132	10.10.15.76	TCP	60	443 → 63787 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75286	37.219680	10.10.15.76	142.250.182.195	TCP	55	63791 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1
75287	37.230239	142.250.182.195	10.10.15.76	TCP	66	443 → 63791 [ACK] Seq=1 Ack=2 Win=1045 Len=0 SLE=1 SRE=2
75289	37.650436	10.10.15.76	104.18.32.47	TCP	55	63773 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
75290	37.660757	104.18.32.47	10.10.15.76	TCP	66	443 → 63773 [ACK] Seq=1 Ack=2 Win=19 Len=0 SLE=1 SRE=2
75291	37.720450	10.10.15.76	142.251.42.3	TCP	55	63793 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
75292	37.740510	142.251.42.3	10.10.15.76	TCP	66	443 → 63793 [ACK] Seq=1 Ack=2 Win=1012 Len=0 SLE=1 SRE=2
75293	39.015117	10.10.15.76	3.233.158.25	TCP	55	63794 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
75294	39.226225	3.233.158.25	10.10.15.76	TCP	66	443 → 63794 [ACK] Seq=1 Ack=2 Win=83 Len=0 SLE=1 SRE=2
76643	53.796241	3.233.158.25	10.10.15.76	TLSv1.2	93	Application Data
76644	53.796626	10.10.15.76	3.233.158.25	TCP	54	63794 → 443 [FIN, ACK] Seq=2 Ack=0 Win=255 Len=0
77908	54.007857	3.233.158.25	10.10.15.76	TLSv1.2	78	Application Data
77981	54.007857	3.233.158.25	10.10.15.76	TCP	66	443 → 63794 [FIN, ACK] Seq=64 Ack=3 Win=83 Len=0
77986	54.007942	10.10.15.76	3.233.158.25	TCP	54	63794 → 443 [RST, ACK] Seq=3 Ack=64 Win=0 Len=0
78413	60.701805	10.10.15.76	104.18.32.47	TCP	55	[TCP Keep-Alive] 63784 → 443 [ACK] Seq=1 Ack=1 Win=251 Len=1
78414	60.712627	104.18.32.47	10.10.15.76	TCP	66	[TCP Keep-Alive ACK] 443 → 63784 [ACK] Seq=1 Ack=2 Win=23 Len=0 SLE=1 SRE=2

Frame 5964: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface DeviceVNF (A2B1644D-C6A6)

Ethernet II, Src: PaloAltoNet_80:8e:10 (3c:fa:30:00:0e:10), Dst: HP_9c:ee:9c (00:60:8b:9c:ee:9c)

Internet Protocol Version 4, Src: 3.233.158.25, Dst: 10.10.15.76

Transmission Control Protocol, Src Port: 443, Dst Port: 63775, Seq: 1, Ack: 1, Len: 39

Source Port: 443

Destination Port: 63775

[Stream index: 0]

[Conversation completeness: Incomplete (60)]

[TCP Segment Len: 39]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 1697953420

[Next Sequence Number: 40 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment Number (raw): 1904936467

0101 ... = Header Length: 20 bytes (5)

Flags: 0010 (PSH, ACK)

Window: 363

Bytes: 99-92: Encrypted Application Data (tls_app_data)

Packets: 100428 - Displayed: 48 (0.0%)

Profile: Default

6. Conclusion

Packet capture and network traffic analysis using tools like Wireshark and tcpdump are essential for gaining deep insights into network performance, identifying issues, and ensuring security.