

EXPERIMENT: 24

NETWORK LAYER PROTOCOL HEADER ANALYSIS USING WIRE SHARK – SMTP AND ICMP

Aim:

To analyze capturing of Transport layer protocol header analysis using Wire shark- SMTP and ICMP.

SOFTWARE USED: Wire shark network analyzer

Procedure: 1. Open wire shark. 2. Click on list the available capture interface. 3. Choose the LAN interface. 4. Click on start button. 5. Active packets will be displayed. 6. Capture the packets & select any IP address from the source. 7. Click on the expression and select IPV4 →IP addr source address in the field name. 8. Select the double equals (==) from the selection and enter the selected IP source address. 9. Click on apply button. 10. All the packets will be filtered using source address.

Output:

The image displays a Wireshark network traffic capture. The top pane shows a list of captured packets, with the first 13 packets being SMTP traffic and the last two being ICMP Echo (ping) requests. The middle pane shows the details of the selected packet (No. 13, SMTP), including the SMTP envelope and the body of the email. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
786	64.166821	2409:40f4:3b:5360::c	2404:6800:4003:c11::	SMTP	76	C: DATA fragment, 10 bytes
788	64.243616	2409:40f4:3b:5360::c	2404:6800:4003:c11::	SMTP	76	C: DATA fragment, 2 bytes
790	64.481148	2409:40f4:3b:5360::c	2404:6800:4003:c11::	SMTP	76	C: DATA fragment, 2 bytes
791	64.500593	2404:6800:4003:c11::	2409:40f4:3b:5360::c	SMTP	240	S: 502-5.5.1 Unrecognized command. For more information, go to 5.5.1 https://support.google.com/a/answer/32216-
794	64.606486	2409:40f4:3b:5360::c	2404:6800:4003:c11::	SMTP	76	C: DATA fragment, 2 bytes
2742	118.065641	74.125.130.109	192.168.205.237	SMTP	129	S: 220 smtp.gmail.com ESMTP 41be93b00d2f7-7db498f9f28sm8690440a12.22 - gsmt
2788	130.343576	192.168.205.237	74.125.130.109	SMTP	56	C: DATA fragment, 16 bytes
2790	130.610782	74.125.130.109	192.168.205.237	SMTP	220	S: 502-5.5.1 Unrecognized command. For more information, go to 5.5.1 https://support.google.com/a/answer/32216-
2806	133.546796	192.168.205.237	74.125.130.109	SMTP	56	C: helo
2808	133.603122	74.125.130.109	192.168.205.237	SMTP	224	S: 501-5.5.4 Empty HELO/EHLO argument not allowed, closing connection. 5.5.4 https://support.google.com/mail/?
2970	148.895488	2404:6800:4003:c11::	2409:40f4:3b:5360::c	SMTP	148	S: 220 smtp.gmail.com ESMTP 98e67ed59e1d1-2dd58c109desm1867658a91.0 - gsmt
3176	166.722579	2409:40f4:3b:5360::c	2404:6800:4003:c11::	SMTP	76	C: helo
3178	166.975030	2404:6800:4003:c11::	2409:40f4:3b:5360::c	SMTP	243	S: 501-5.5.4 Empty HELO/EHLO argument not allowed, closing connection. 5.5.4 https://support.google.com/mail/?

Frame 2808: 324 bytes on wire (1792 bits), 324 bytes captured (1792 bits) on interface \Device\NPF{...} Ethernet II, Src: 2a:19:97:57:fb:7f:2a (2a:19:97:57:fb:7f:2a), Dst: Intel_deic3:e9 (f4:06:69:de:c3:e9) Internet Protocol Version 4, Src: 74.125.130.109, Dst: 192.168.205.237 Transmission Control Protocol, Src Port: 587, Dst Port: 53528, Seq: 242, Ack: 23, Len: 170 Source Port: 587 Destination Port: 53528 [Stream index: 46] [Stream Packet Number: 38] [Conversation completeness: Complete, WITH_DATA (31)] [TCP Segment Len: 170] Sequence Number: 242 (relative sequence number) Sequence Number (raw): 2714736421 [Next Sequence Number: 412 (relative sequence number)] Acknowledgment Number: 23 (relative ack number) Acknowledgment Number (raw): 1179687745 Window: 256 Window (raw): 256 [Calculated window size: 65536] Flags: 0x018 (PSH, ACK) Window: 256 [Calculated window size: 65536]

Packets: 3212 - Displayed: 13 (0.4%) - Dropped: 0 (0.0%) Profile: Default

Result: Hence, the capturing of packets using wire shark network analyzer was analyzed for SMTP and ICMP.