

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

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.

940	20.420843	172.24.36.230	142.251.221.142	ICMP	74 Echo (ping) request	id=0x0001, seq=1/256, ttl=128 (reply in 941)
941	20.425682	142.251.221.142	172.24.36.230	ICMP	74 Echo (ping) reply	id=0x0001, seq=1/256, ttl=115 (request in 940)
984	21.439987	172.24.36.230	142.251.221.142	ICMP	74 Echo (ping) request	id=0x0001, seq=2/512, ttl=128 (reply in 986)
986	21.446074	142.251.221.142	172.24.36.230	ICMP	74 Echo (ping) reply	id=0x0001, seq=2/512, ttl=115 (request in 984)
1054	22.459271	172.24.36.230	142.251.221.142	ICMP	74 Echo (ping) request	id=0x0001, seq=3/768, ttl=128 (reply in 1056)
1056	22.469587	142.251.221.142	172.24.36.230	ICMP	74 Echo (ping) reply	id=0x0001, seq=3/768, ttl=115 (request in 1054)
1129	23.479863	172.24.36.230	142.251.221.142	ICMP	74 Echo (ping) request	id=0x0001, seq=4/1024, ttl=128 (reply in 1133)
1133	23.488536	142.251.221.142	172.24.36.230	ICMP	74 Echo (ping) reply	id=0x0001, seq=4/1024, ttl=115 (request in 1129)
1425	29.855000	172.24.36.230	13.107.246.48	ICMP	74 Echo (ping) request	id=0x0001, seq=5/1280, ttl=128 (reply in 1448)
1448	29.962198	13.107.246.48	172.24.36.230	ICMP	74 Echo (ping) reply	id=0x0001, seq=5/1280, ttl=52 (request in 1425)
1477	30.868483	172.24.36.230	13.107.246.48	ICMP	74 Echo (ping) request	id=0x0001, seq=6/1536, ttl=128 (reply in 1488)
1488	30.980125	13.107.246.48	172.24.36.230	ICMP	74 Echo (ping) reply	id=0x0001, seq=6/1536, ttl=52 (request in 1477)
1495	31.886187	172.24.36.230	13.107.246.48	ICMP	74 Echo (ping) request	id=0x0001, seq=7/1792, ttl=128 (reply in 1501)
1501	31.944552	13.107.246.48	172.24.36.230	ICMP	74 Echo (ping) reply	id=0x0001, seq=7/1792, ttl=52 (request in 1495)

Frame 940: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface	0000	00 42 5a 4e e7 67 b0 47 e9 77 05 bf 08 00 45 00	BZN g G w ... E
Ethernet II, Src: Intel_77:05:bf (b0:47:e9:77:05:bf), Dst: Cisco_4e:e7:67 (00:4	0010	00 3c 65 a6 00 00 00 01 00 00 ac 18 24 e6 8e fb	<e \$
Internet Protocol Version 4, Src: 172.24.36.230, Dst: 142.251.221.142	0020	dd 8e 08 00 4d 5a 00 01 00 01 61 62 63 64 65 66	..MZ.. ..abcdef
Internet Control Message Protocol	0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
Type: 8 (Echo (ping) request)	0040	77 61 62 63 64 65 66 67 68 69	wabdefgh hi
Code: 0			
Checksum: 0x4d5a [correct]			
[Checksum Status: Good]			
Identifier (BE): 1 (0x0001)			
Identifier (LE): 256 (0x0100)			
Sequence Number (BE): 1 (0x0001)			
Sequence Number (LE): 256 (0x0100)			
[Response frame: 941]			
Data (32 bytes)			

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