

CONSEGNA S9/L3

Per l'esercizio pratico di oggi, troviamo in allegato una cattura di rete effettuata con Wireshark.

Analizzare la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco

SCANSIONE

The image shows a Wireshark network capture titled "Cattura_U3_W1_L3.pcapng". The packet list on the left shows a series of TCP SYN packets from 192.168.200.100 to 192.168.200.150, indicating a port scan. The packet details on the right show the structure of a TCP segment, including the source and destination IP addresses, ports, sequence number, and window size. The packet bytes pane at the bottom shows the raw data of the selected packet, including the Ethernet II header, Internet Protocol Version 4 header, and the TCP segment.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	256	256 Hosts Announcement: MEFASPOL1TABL1, Workstation, Server, Print Queue Server, Xenix server, NT Workstation, NT
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53860 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53860 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
5	23.764777427	192.168.200.150	192.168.200.100	TCP	66	443 → 33876 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
6	23.764919289	192.168.200.100	192.168.200.150	TCP	66	53860 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899991	192.168.200.100	192.168.200.150	TCP	66	53860 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
8	28.761629461	08:00:27:fd:87:1e	08:00:27:39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	08:00:27:39:7d:fe	08:00:27:fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	08:00:27:39:7d:fe	08:00:27:fd:87:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	08:00:27:fd:87:1e	08:00:27:39:7d:fe	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41384 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15	36.774366395	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
19	36.774685955	192.168.200.150	192.168.200.100	TCP	74	23 → 41384 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774708464	192.168.200.100	192.168.200.150	TCP	66	41384 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775337800	192.168.200.100	192.168.200.150	TCP	74	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128

Notiamo come appaiono molti protocolli TCP verso le porte della macchina con ip 192.168.200.150 da una macchina sorgente con ip 192.168.200.100.

Andiamo ad evidenziare le conversazioni:

The screenshot shows the Wireshark interface with the 'Statistics' pane open. The 'Conversations' tab is selected, displaying a table of network conversations. The table has columns for 'No.', 'Time', and 'Source'. The source IP address is consistently 192.168.200.100 for all entries. The destination IP address is 192.168.200.150. The table lists various protocols such as DHCP (BOOTP), NetPerfMeter, ONC-RPC, 29West, ANCP, BACnet, Collectd, DNS, Flow Graph, HART-IP, HPFEEDS, HTTP, HTTP2, Sametime, TCP Stream Graphs, UDP Multicast Streams, Reliable Server Pooling (RSerPool), SOME/IP, F5, IPv4 Statistics, and IPv6 Statistics. The 'Info' pane on the right shows details for the selected conversation, including 'Host Announcement' and 'Who has 192.168.200.150'.

No.	Time	Source
1	0.000000000	192.168.200.100
2	23.764214995	192.168.200.150
3	23.764287789	192.168.200.150
4	23.764777323	192.168.200.150
5	23.764777427	192.168.200.150
6	23.764815289	192.168.200.150
7	23.764899091	192.168.200.150
8	28.761629461	08:00:27:f
9	28.761644619	08:00:27:3
10	28.774852257	08:00:27:3
11	28.775230099	08:00:27:f
12	36.774143445	192.168.200.150
13	36.774218116	192.168.200.150
14	36.774257841	192.168.200.150
15	36.774366305	192.168.200.150
16	36.774405627	192.168.200.150
17	36.774535534	192.168.200.150
18	36.774614776	192.168.200.150
19	36.774685505	192.168.200.150
20	36.774685652	192.168.200.150
21	36.774685696	192.168.200.150
22	36.774685737	192.168.200.150
23	36.774685776	192.168.200.150
24	36.774700464	192.168.200.150
25	36.774711072	192.168.200.150
26	36.775141104	192.168.200.150
27	36.775141273	192.168.200.150
28	36.775174048	192.168.200.150
29	36.775337800	192.168.200.150

Quello che vediamo in atto è palesemente un port scanning:

Ethernet - 2	IPv4 - 2	IPv6	TCP - 1026	UDP - 1
Address A	Port A	Address B	Port B	Packets
192.168.200.100	37396	192.168.200.150	1	2 134 bytes
192.168.200.100	34748	192.168.200.150	2	2 134 bytes
192.168.200.100	58938	192.168.200.150	3	2 134 bytes
192.168.200.100	43056	192.168.200.150	4	2 134 bytes
192.168.200.100	54282	192.168.200.150	5	2 134 bytes
192.168.200.100	40874	192.168.200.150	6	2 134 bytes
192.168.200.100	52702	192.168.200.150	7	2 134 bytes
192.168.200.100	47720	192.168.200.150	8	2 134 bytes
192.168.200.100	41348	192.168.200.150	9	2 134 bytes
192.168.200.100	46014	192.168.200.150	10	2 134 bytes
192.168.200.100	37252	192.168.200.150	11	2 134 bytes
192.168.200.100	41700	192.168.200.150	12	2 134 bytes
192.168.200.100	58814	192.168.200.150	13	2 134 bytes
192.168.200.100	53648	192.168.200.150	14	2 134 bytes
192.168.200.100	42454	192.168.200.150	15	2 134 bytes
192.168.200.100	36316	192.168.200.150	16	2 134 bytes
192.168.200.100	39712	192.168.200.150	17	2 134 bytes
192.168.200.100	57066	192.168.200.150	18	2 134 bytes
192.168.200.100	49988	192.168.200.150	19	2 134 bytes
192.168.200.100	48812	192.168.200.150	20	2 134 bytes
192.168.200.100	41182	192.168.200.150	21	4 280 bytes
192.168.200.100	55656	192.168.200.150	22	4 280 bytes
192.168.200.100	41304	192.168.200.150	23	4 280 bytes
192.168.200.100	37888	192.168.200.150	24	2 134 bytes
192.168.200.100	60632	192.168.200.150	25	4 280 bytes
192.168.200.100	34782	192.168.200.150	26	2 134 bytes
192.168.200.100	52294	192.168.200.150	27	2 134 bytes

Come misure di prevenzione suggeriamo di chiudere le porte non utilizzate e filtrare le altre, impostare il firewall in modo tale che le porte comunichino solo con ip e protocolli prestabiliti.