

L'esercizio di oggi prevede l'analisi di una cattura effettuata con Wireshark per poi effettuare una Identificazione degli eventuali IOC (ovvero evidenze di attacchi in corso In base In base agli IOC trovati);

Fare delle ipotesi sui potenziali vettori di attacco utilizzati;

Consigliare un'azione per ridurre gli impatti dell'attacco.

Analizziamo la cattura dei pacchetti che EPICODE ci ha affidato, apriamo quindi il file su Kali linux utilizzando il programma "Wireshark":

No.	Time	Source	Destination	Protocol	Length	Info
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41	36.776095853	192.168.200.100	192.168.200.150	TCP	66	53662 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
42	36.776179338	192.168.200.100	192.168.200.150	TCP	74	50684 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
43	36.776233800	192.168.200.100	192.168.200.150	TCP	74	54220 → 999 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
44	36.776330610	192.168.200.100	192.168.200.150	TCP	74	34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
45	36.776385694	192.168.200.100	192.168.200.150	TCP	74	33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
46	36.776402500	192.168.200.100	192.168.200.150	TCP	74	49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
47	36.776451284	192.168.200.150	192.168.200.100	TCP	60	199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	36.776451357	192.168.200.150	192.168.200.100	TCP	60	995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	36.776478201	192.168.200.100	192.168.200.150	TCP	74	46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
50	36.776490366	192.168.200.100	192.168.200.150	TCP	74	33206 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
51	36.776512221	192.168.200.100	192.168.200.150	TCP	74	60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
52	36.776508606	192.168.200.100	192.168.200.150	TCP	74	49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
53	36.776671271	192.168.200.100	192.168.200.150	TCP	74	37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
54	36.776720715	192.168.200.100	192.168.200.150	TCP	74	54898 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
55	36.776813123	192.168.200.150	192.168.200.100	TCP	60	587 → 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56	36.776842423	192.168.200.100	192.168.200.150	TCP	74	51534 → 407 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
57	36.776904928	192.168.200.150	192.168.200.100	TCP	74	445 → 33042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64
58	36.776904922	192.168.200.150	192.168.200.100	TCP	60	256 → 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	36.776904961	192.168.200.150	192.168.200.100	TCP	74	139 → 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64
60	36.776905004	192.168.200.150	192.168.200.100	TCP	60	143 → 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	36.776905043	192.168.200.150	192.168.200.100	TCP	74	25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64
62	36.776905082	192.168.200.150	192.168.200.100	TCP	60	110 → 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63	36.776905123	192.168.200.150	192.168.200.100	TCP	74	53 → 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64
64	36.776905162	192.168.200.150	192.168.200.100	TCP	60	500 → 54898 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Possiamo notare che la macchina con indirizzo IP 192.168.200.100 ha inviato dei pacchetti TCP alla macchina 192.168.200.150, ed ogni pacchetto inviato ha una porta di destinazione diversa, quindi è sicuramente in atto una scansione delle porte sulla macchina vittima con Nmap.

l'attaccante ha sicuramente utilizzato lo switch -sT per effettuare una scansione tramite il Two-Hand-Shake visto l'utilizzo di Syn-Ack nei pacchetti analizzati.

Per evitare altre scansioni future è consigliata l'implementazione di un firewall configurato in modo da far risultare le porte scannerizzate come "Filtered" così da non fornire informazioni all'attaccante che effettua la scansione. Ricordiamo inoltre che solitamente la scansione delle porte attive è il primo passo verso un attacco informatico vero e proprio, per questo motivo è consigliato chiudere le porte superflue e utilizzare per i servizi installati sulla macchina porte oltre la 1024, solitamente scannerizzate solo in un secondo momento. Inoltre, visto che l'attaccante è entrato in possesso di informazioni importanti per un possibile attacco, è opportuno bloccare l'indirizzo ip dell'attaccante tramite firewall