

## THREAT INTELLIGENCE E IoC

L'esercizio di oggi ci chiede di analizzare il traffico catturato su Wireshark e di identificare eventuali IoC, ipotizzare i vettori di attacco e consigliare remediation.

Guardando il traffico catturato, si capisce fin da subito che l' IP 192.168.200.100 sta cercando di scansionare il bersaglio 192.168.200.150:

192.168.200.100	192.168.200.150	TCP	74 53060 → 80 [SYN] Seq=0 Win=64240
192.168.200.100	192.168.200.150	TCP	74 33876 → 443 [SYN] Seq=0 Win=64240
192.168.200.150	192.168.200.100	TCP	74 80 → 53060 [SYN, ACK] Seq=0 Ack=1

Riusciamo a capire questo guardando l'IP sorgente che invia una prima richiesta di connessione three way handshake (SYN) e il 192.168.200.150 che risponde con SYN, ACK.

Capiamo anche che il bersaglio della scansione è un server Metasploitable, perché quando si attiva, il server fa l'host announcement:

Host Announcement METASPLOITABLE, Workstation, Server

Analizzando più a fondo, vediamo come le richieste di connessione vengono fatte verso tutte le porte well-known, sono richieste di TCP connect (possiamo anche ipotizzare che sia una scansione Nmap con lo switch -sT) perché si conclude la three way handshake:

Qui un esempio con la porta 53

Source	Destination	Protocol	Length	Info
192.168.200.100	192.168.200.150	TCP	74	37282 → 53 [SYN] Seq=0 Win=64240
192.168.200.150	192.168.200.100	TCP	74	53 → 37282 [SYN, ACK] Seq=0 Ack=1
192.168.200.100	192.168.200.150	TCP	66	37282 → 53 [ACK] Seq=1 Ack=1 Win=6
192.168.200.100	192.168.200.150	TCP	66	37282 → 53 [RST, ACK] Seq=1 Ack=1

Nell'immagine sotto c'è anche la spiegazione del perché sia TCP connect e non uno scan version; nella parte sinistra possiamo vedere come, per scoprire la versione di un servizio, ci sia molto più traffico rispetto ad uno scan TCP:

No.	Time	Source	Destination	Protocol	Length	Info
59	13.004160763	192.168.32.100	192.168.32.102	TCP	74	42468 → 53 [SYN] Seq=0 Win=64240
64	13.004369396	192.168.32.102	192.168.32.100	TCP	74	53 → 42468 [SYN, ACK] Seq=0 Ack=1
68	13.004412216	192.168.32.100	192.168.32.102	TCP	66	42468 → 53 [ACK] Seq=1 Ack=1 Win=6
100	13.006310914	192.168.32.100	192.168.32.102	TCP	66	42468 → 53 [RST, ACK] Seq=1 Ack=1
2075	13.152138586	192.168.32.100	192.168.32.102	TCP	74	42470 → 53 [SYN] Seq=0 Win=64240
2081	13.152324631	192.168.32.102	192.168.32.100	TCP	74	53 → 42470 [SYN, ACK] Seq=0 Ack=1
2082	13.152346641	192.168.32.100	192.168.32.102	TCP	66	42470 → 53 [ACK] Seq=1 Ack=1 Win=6
2175	19.161124043	192.168.32.100	192.168.32.102	DNS	98	Standard query 0x0006 TXT v=1
2182	19.161470237	192.168.32.102	192.168.32.100	TCP	66	53 → 42470 [ACK] Seq=1 Ack=1 Win=6
2226	19.164170133	192.168.32.102	192.168.32.100	DNS	130	Standard query response 0x0006
2228	19.164176022	192.168.32.100	192.168.32.102	TCP	66	42470 → 53 [ACK] Seq=33 Ack=1
2230	19.164296107	192.168.32.100	192.168.32.102	TCP	66	42470 → 53 [FIN, ACK] Seq=33 Ack=1
2231	19.164623171	192.168.32.102	192.168.32.100	TCP	66	53 → 42470 [FIN, ACK] Seq=66 Ack=34
2232	19.164631653	192.168.32.100	192.168.32.102	TCP	66	42470 → 53 [ACK] Seq=34 Ack=66

Come azioni di remediation possiamo consigliare di attivare un firewall e impostare delle regole che impediscano la connessione, droppando i pacchetti che arrivano da indirizzi IP sconosciuti oppure non autorizzati ad effettuare Pentesting e Vulnerability Assessment.

Altra soluzione è quella di tenere sotto controllo il traffico con sistemi anti intrusione, come ad esempio IDS/IPS, collegati ad un SIEM in modo da monitorare il tutto da remoto.