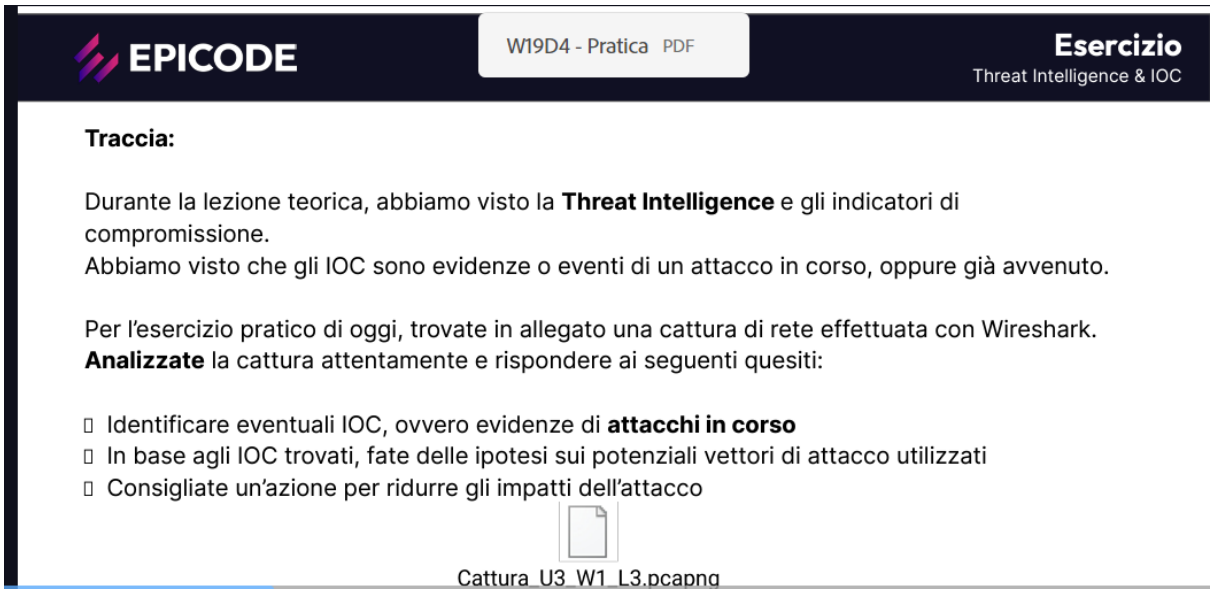
ESERCITAZIONE WEEK 19 DAY5



Dall'analisi del traffico catturato con WireShark si può ipotizzare che il target con indirizzo IP 192.168.200.150, che è una macchina Metasploitable, è vittima di una scansione in corso.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Serv
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8105224
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=810522
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSv
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr
8	28.761629461	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PcsCompu_fd:87:1e	PcsCompu_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	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8105354
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=810535
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535

I fattori di compromissione che danno evidenza di questo sono:

- Ci sono tantissime richieste dalla sorgente con IP 192.168.200.100 verso innumerevoli porte (intervallo ampio) del destinatario 192.168.200.150;
- Spesso le richieste, che hanno nel pacchetto il flag SYN attivo, sono una dopo l'altro verso porte differenti del target e provengono sempre da una porta sorgente assegnata randomicamente;
- Per ogni richiesta, viene completato il three way handshake che dimostra che si tratta di scansioni complete tcp;
- Se una porta del destinatario, risponde direttamente con il FLAG di reset, l'IP 192.168.200.100 continua con le richieste successive;

Dunque il sistema attaccante sta tentando di valutare quali porte siano aperte e quali chiuse. Si può ipotizzare che come vettore di attacco si stia usando un tool di scansione come nmap, oppure Nessus che nel fare Vulnerability Assessment, ricerca anche le porte aperte.

Per ridurre l'impatto, si elencano alcuni possibili azioni di rimedio:

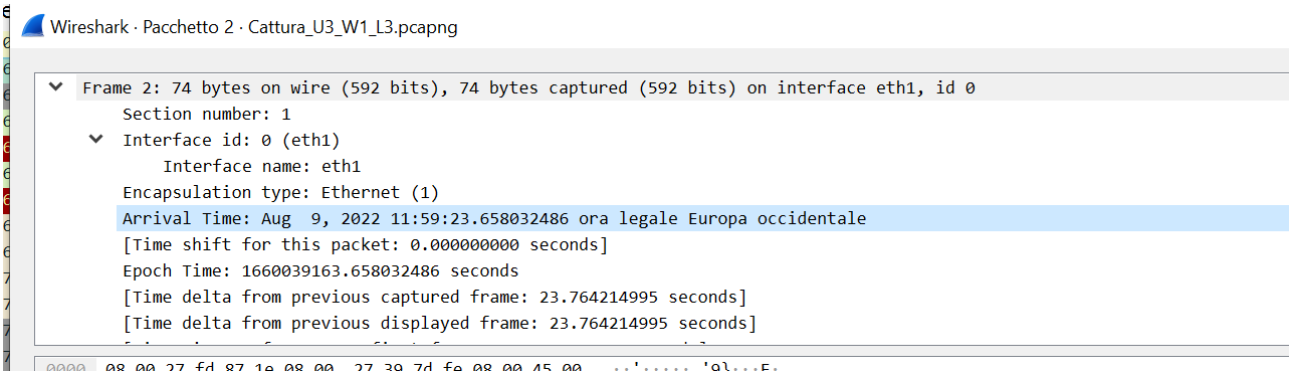
- **Bloccare l'IP 192.168.200.100** sul Firewall o sul computer di rete. Questo impedirà all'attaccante di continuare la scansione sulle porte;
- **Chiudere** le porte;
- **Verificare la configurazione del firewall**: valutare che il Firewall sia configurato correttamente per bloccare il traffico non autorizzato, oltre che l'IP sospetto;
- **Rafforzare la sicurezza delle password**: se l'attaccante sta cercando di accedere alle porte aperte, bisogna rafforzare le password dei servizi, usando password lunghe e complesse e considerando l'implementazione di autenticazione a più fattori;
- **Continuare a monitorare il traffico di rete**, in modo da valutare se ci sono altre attività sospette;
- **Mantenere il software aggiornato**: assicurarsi che il sistema operativo, il software di sicurezza e tutte le applicazioni siano aggiornate con gli ultimi patch di sicurezza. Le vulnerabilità non corrette possono essere sfruttate dagli attaccanti;
- Sul device target **monitorare anche i processi, le risorse e i log** per valutare azioni sospette e scongiurare una intrusione già in stato avanzato;
- Fare per sicurezza un **backup dei dati**, non conoscendo ancora lo stato dell'intrusione;
- Si può inoltre **segnalare l'attività sospetta** all'azienda o a organizzazioni competenti;

Altre informazioni utili:

- Dell'attaccante è noto il suo IP ed anche l'indirizzo MAC, visibili grazie ad esempio ai pacchetti generati durante la comunicazione ARP:

8	28.761629461	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60 Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42 192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42 Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60 192.168.200.150 is at 08:00:27:fd:87:1e

- Si evince che l'attaccante è all'interno della stessa rete;
- Ipotizzando che la scansione malevola sia ancora in corso, si ha evidenza dallo sniffing, di quali porte siano già state rilevate aperte (se è stato completato il 3WH) e si può iniziare ad agire su queste;
- Si ha di conseguenza evidenza delle porte che non è riuscito ad indivuare come aperte;
- Si può inoltre dai pacchetti conoscere data e ora degli eventi, utili per ricostruire gli eventi o correlarli;



- Poiché le richieste provengono sempre dalla sorgente con IP 192.168.200.100 e mai da altre, si esclude l'attacco DdoS;

Dubbio: perché la richiesta sulla porta 80 e sulla porta 443 la fa due volte a differenza di altre? Forse si è partiti con una scansione solo su quelle due porte per vedere se c'erano servizi HTTP/HTTPS attivi e poi è stata fatta la scansione più dettagliata su tutto. Essendo la 443 chiusa, il secondo tentativo ha senso.

Essendo la 80 aperta giò dall'inizio, forse è stato ripetuto ciò che è stato fatto sulla 443.