Threat Intelligence & IOC

Obiettivo:

Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare ed analizzare 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 attuale ed eventualmente un simile attacco futuro

Gestione Permessi

```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod ugo+rw Cattura_U3_W1_L5.pcapng
┌──(kali㉿kali)-[~/Desktop]
└─$ chown kali Cattura_U3_W1_L5.pcapng
```

Analisi pacchetti

Dopo un broadcast da parte della macchina .150 per comunicare la presenza del servizio web sulla rete, possiamo vedere la prima comunicazioni TCP che si muove sulla porta 80:

	Time	Source	Destination	Protocol	Length	Info
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 L
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=6
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1

E' presente il classico handshake TCP ma il client .100 ha chiuso la connessione subito, facendo sospettare di un operazione con nmap -sS, scansione silenziosa delle porte aperte.

Subito dopo il client prova la stessa operazione sulla porta 443 ma viene rifiutato probabilmente perché il servizio https non e' attivo.

	Time	Source	Destination	Protocol	Length	Info
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 A

Successivamente a un ARP-SCAN, sembrerebbe che l'attaccante stia facendo un secondo synscan sulle porte comuni:

12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=6424
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=6424
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=6424
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=6424
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=6424
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74	23 → 41304 [SYN, ACK] Seq=0 Ack=1
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=

tutte queste comunicazioni finiscono con un reset come quelle viste inizialmente.

Lista porte trovate aperte:

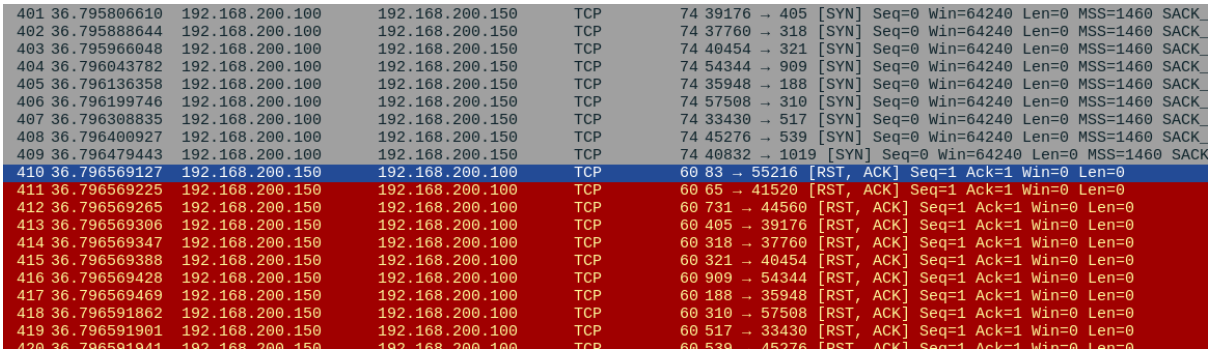
- 21
- 22
- 23
- 25
- 53
- 80
- 111
- 139
- 445
- 512
- 514

Considerazioni sui log:

I log iniziali presentano un chiaro segno di **nmap TCP SYN port scan,** una tecnica silenziosa per scannerizzare le porte aperte su una macchina.

La macchina target ha risposto con un SYN-ACK a molte porte facendo trapelare i servizi attivi e potenzialmente exploitabili.

Successivamente la macchina attaccante continua a scannerizzare tutte le altre porte utilizzando la stessa tecnica iniziale, molte di esse chiuse:



Macchina attaccante:

Dopo un'analisi di alcuni campi dei pacchetti si può dire che la macchina attaccante sta utilizzando linux come SO, questo è dovuto a campi come **Window_size = 64420** e **timestamp attivo** tipici di sistemi linux.

Il numero alto e casuale delle porte sorgente e' un probabile segno che si sta usando uno strumento avanzato per lo scan, come nmap.
Un altro segno di nmap e' l'ordinamento tipico delle opzioni TCP.

Azioni consigliate:

- **Attivare logging e alert su connessioni SYN anomale**
  Gli IP che effettuano connessioni di questo genere vanno RILEVATI e successivamente BLOCCATI per evitare possibili escalation.
  Un attaccante potrebbe passare alla fase di exploit dopo aver raccolto abbastanza informazioni sui servizi in esecuzione.

- **Limitare la superficie di attacco**
  Quindi chiudere tutte le porte non utili, come ftp o ssh, porte delicate su un web server.
  Questa azione riduce le possibilità d'attacco anche se avviene la scansione.

- **HoneyPot e fingerPrinting**
  Una honeyPot ben configurata puo' rallentare di molto un attaccante.
  Allo stesso tempo e' importante profilare l'attaccante per future attribuzioni e per capire se cambia strumenti o tecniche.