

THREAT INTELLIGENCE & IOC

TASK

Durante la lezione teorica, abbiamo visto la Threat Intelligence e gli indicatori di compromissione. Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.

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



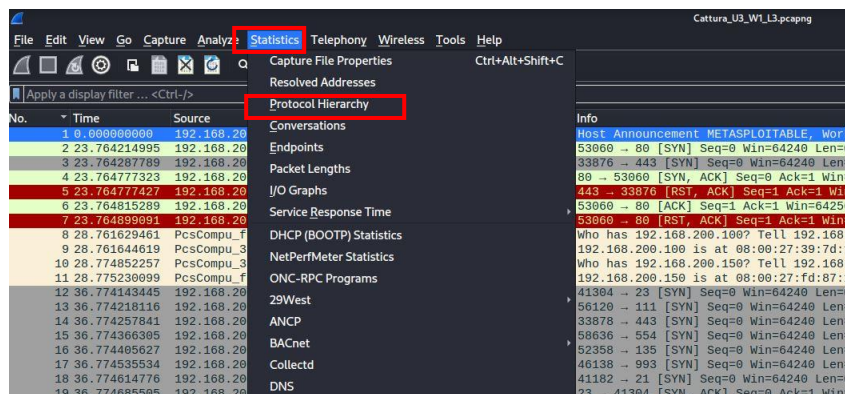
Cattura_U3_W1_L3.pcapng

ANALISI E VALUTAZIONE DEL FILE

Come prima cosa andiamo ad analizzare i file di Wireshark per andare a identificare eventuali IOC. Quest'ultimi "**indicatori di compromissione**" non sono altro che delle prove/indizi di una violazione dei dati. Questi indicatori infatti possono rilevare che si è verificato un attacco, quali strumenti sono stati utilizzati nell'attacco e chi c'è dietro.

Andando ad analizzare il file di wireshark come da esercizio ritroviamo che i pacchetti inviati sono tutti del tipo TCP, e lo si può notare andando nella sezione di wireshark che segue:

statistics → Protocol Hierarchy



Wireshark - Protocol Hierarchy Statistics - Cattura_U3_W1_L3.pcapng

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	2083	100.0	139872	30 k	0	0	0
Ethernet	100.0	2083	20.8	29162	6,326	0	0	0
Internet Protocol Version 4	99.8	2079	29.7	41580	9,019	0	0	0
User Datagram Protocol	0.0	1	0.0	8	1	0	0	0
NetBIOS Datagram Service	0.0	1	0.2	244	52	0	0	0
SMB (Server Message Block Protocol)	0.0	1	0.1	162	35	0	0	0
SMB MailSlot Protocol	0.0	1	0.0	25	5	0	0	0
Microsoft Windows Browser Protocol	0.0	1	0.1	76	16	1	76	16
Transmission Control Protocol	99.8	2078	44.8	62652	13 k	2078	62652	13 k
Address Resolution Protocol	0.2	4	0.1	148	32	4	148	32

Questo ci permette di intuire che tutti i pacchetti trasmessi sono del tipo TCP, i rimanenti invece sono:

- 1 BROWSER: Che instaura la connessione tra Source e Host server.
- 4 ARP: Che serve per conoscere l'indirizzo MAC una volta noto l'indirizzo IP di destinazione.

Analizzando il singolo pacchetto **Browser** si possono ottenere informazioni riguardante l'Host, andando nella sezione che segue come da immagine:

Wireshark - Packet 1 - Cattura_U3_W1_L3.pcapng

```

Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0
Ethernet II, Src: PcsCompu_fd:87:1e (08:00:27:fd:87:1e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.255
User Datagram Protocol, Src Port: 138, Dst Port: 138
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
Microsoft Windows Browser Protocol
  Command: Host Announcement (0x01)
  Update Count: 1
  Update Periodicity: 2 minutes
  Host Name: METASPLOITABLE
  Windows version:
  OS Major Version: 4
  OS Minor Version: 9
  Server Type: 0x00019a03, Workstation, Server, Print, Xenix, NT Workstation, NT Server, Potential Browser
  Browser Protocol Major Version: 15
  Browser Protocol Minor Version: 1
  Signature: 0xaa55
  Host Comment: metasploitable server (Samba 3.0.20-Debian)

```

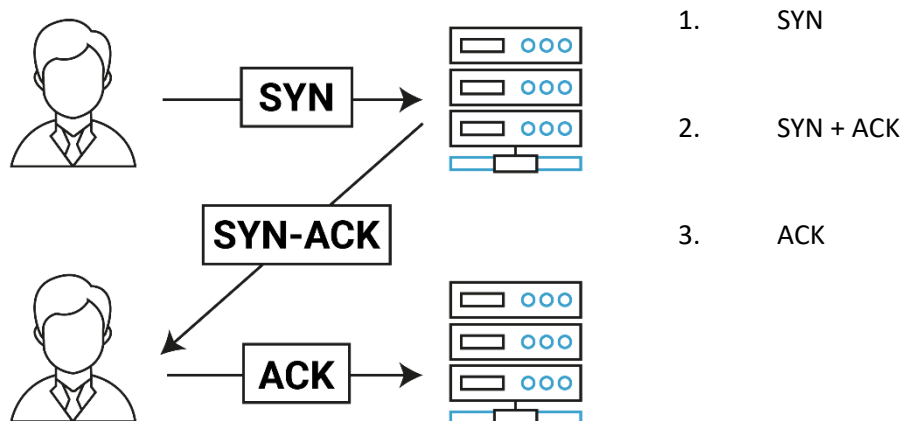
0000	ff ff ff ff ff ff 08 00	27 fd 87 1e 08 00 45 00E..
0010	01 10 00 00 40 00 40 11	26 f6 c0 a8 c8 96 c0 a8@.@.&....
0020	c8 ff 00 8a 00 8a 00 fc	4b 01 11 0a 75 b4 c0 a8K..U..
0030	c8 96 00 8a 00 e6 00 00	20 45 4e 45 46 46 45 45ENEFFEE
0040	42 46 44 46 41 45 4d 45	50 45 4a 46 45 45 42 45	BFDFAEME PEJFEEBE
0050	43 45 4d 45 46 43 41 41	41 00 20 46 48 45 50 46	CEMEFCAA A FHEPF
0060	43 45 4c 45 48 46 43 45	50 46 46 46 41 43 41 43	CELEHFCE PFFFACAC
0070	41 43 41 43 41 43 41 43	41 42 4e 00 ff 53 4d 42	ACACACAC ABN..SMB
0080	25 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	%.....
0090	00 00 00 00 00 00 00 00	00 00 00 00 11 00 00 4cL
00a0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00b0	00 00 00 4c 00 56 00 03	00 01 00 01 00 02 00 5d	...L.V.....]
00c0	00 5c 4d 41 49 4c 53 4c	4f 54 5c 42 52 4f 57 53	..MAILSL OT\BROWS
00d0	45 00 01 01 c0 d4 01 00	4d 45 54 41 53 50 4c 4f	E.....METASPLO

Quindi abbiamo scoperto in questo caso che la macchina vittima è METASPLOITABLE.

Analizzando i pacchetti TCP filtrando ad una porta (es. 23), con il comando `<<tcp.port == 23>>` i risultati ottenuti sono:

No.	Time	Source	Destination	Protocol	Length	Info
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=1 TSval=810535437 TSecr=0 WS=128
19	36.774685585	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=1 TSval=4294952466 TSecr=810535437 WS=64
24	36.774700464	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
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66	41384 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

Questo ci permette di intuire che è stata avviata una connessione tra le due macchine, con indirizzo IP dell'attaccante del tipo 192.168.200.100 e quello della vittima 192.168.200.150, il tutto dovuto al **Three-Way Handshake** il quale permette di instaurare la connessione inviando i pacchetti:



Nell'analisi dei pacchetti inviati ad una singola porta notiamo che la connessione è stata instaurata e dopo conclusa come si evince dall'ultimo pacchetto (RST, ACK). Il sospetto principale è che l'attaccante abbia voluto scansionare la nostra macchina vittima, attraverso esempio con il tool **nmap** dovuto a delle multiple richieste TCP su ampi intervalli di porte.

Possiamo ora ipotizzare che tipo di scansione abbia potuto sfruttare l'attaccante. Tra quelle conosciute, sappiamo che:

- **sS**: è una scansione che non instaura la connessione e che quindi dopo il primo SYN + ACK la connessione si conclude
- **sT**: è una scansione che instaura la connessione e che quindi conclude il Three-way Handshake
- **sV**: è una scansione molto più invasiva delle ultime due con risultato finale simile ad esse con aggiunta delle versioni dei servizi.
- **A**: anch'essa scansione invasiva simile alla precedente fornendo anche informazioni del dispositivo vittima.

Andando per esclusione: -sS nell'analisi con Wireshark non avrebbe dovuto fornire l'ACK finale di avvenuta connessione e quindi scartata. Pertanto le uniche opzioni sarebbero potuto essere -sT, -sV e -A.

Quindi possiamo supporre che il nostro attaccante avrebbe voluto avere informazioni sulla nostra macchina per andare a sfruttare, tra i risultati della scansione, le porte aperte. Ad esempio potrebbe sfruttare il tool Nessus per andare ad analizzare le vulnerabilità più critiche tra le porte aperte e utilizza Metasploit per entrarci.

RISOLUZIONE DEL PROBLEMA:

Supponiamo in questo esempio di essere noi la vittima, come avremmo potuto evitare che un utente esterno possa scansionare il nostro dispositivo?

1. Tra le soluzioni la prima mi sembrerebbe la più ovvia, ovvero inserimento di un firewall che permetta di evitare questa scansione. Essendo Host Metasploitable la soluzione sarebbe quella di sfruttare **iptables** e creare di conseguenza una regola che non permetta la comunicazione con altre macchine.
2. Un'altra soluzione è quella di inserire l'IP sorgente dell'attaccante all'interno di una **blacklist** e di conseguenza non permettere a quest'ultimo di avere alcuna comunicazione con la nostra macchina. Di seguito una guida per come bloccare un indirizzo IP:
https://verytech.smartworld.it/come-bloccare-un-indirizzo-ip-274978.html#steps_3