THREAT INTELLIGENCE & IOC

TRACCIA

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

REQUISITI

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

PASSAGGI ESERCIZIO

PRIMI PASSI

andiamo a scaricare il file che poi andremo ad analizzare la cattura, spostate il file sulla vostra Kali Linux, Vi basterà creare la cartella sul vostro sistema operativo, e configurare la cartella sulla macchina virtuale, specificando il percorso della cartella sul vostro Host ed il nome della cartella. Configurate la cartella

```
┌──(kali㉿kali)-[/media]
└─$ cd ..

┌──(kali㉿kali)-[/]
└─$ cd /home/kali

┌──(kali㉿kali)-[~]
└─$ cd /media

┌──(kali㉿kali)-[/media]
└─$ ls
sf_Cattura_U3_W1_L3

┌──(kali㉿kali)-[/media]
└─$ cd sf_Cattura_U3_W1_L3

┌──(kali㉿kali)-[/media/sf_Cattura_U3_W1_L3]
└─$ ls
Cattura_U3_W1_L3.pcapng

┌──(kali㉿kali)-[/media/sf_Cattura_U3_W1_L3]
└─$
```

Da Kali potete accedere alla cartella (ed ai file in essa contenuti) navigando il file system alla directory /media come da figura seguente. Come vedete il nostro file è nella cartella condivisa. Da qui possiamo spostare il file sul desktop con il comando «mv» specificando il nome del file ed il path di destinazione, come visto nelle lezioni sul file system di Linux (il comando che abbiamo usato noi è nella figura a destra). Successivamente assicuratevi che l'utente Kali possa aprire il file assegnando i permessi necessari - riferimento figura in a destra. A questo punto fate doppio click per analizzare la cattura.

```
┌──(root㉿kali)-[/media/sf_vm_shared]
└─# ls -la
total 272
drwxrwx─── 1 root vboxsf   4096 Aug  9 06:31 .
drwxr-xr-x 4 root root     4096 May 20 03:00 ..
-rwxrwx─── 1 root vboxsf    708 Jul 24 06:46 BW_D3_BOF.c
-rwxrwx─── 1 root vboxsf 209024 Aug  9 06:26 Cattura_U3_W1_L3.pcapng
-rwxrwx─── 1 root vboxsf   1242 May 31 06:38 Esercizio_10_Epicode.c
-rwxrwx─── 1 root vboxsf  46382 Jun  4 06:34 GameShell_lv10.txt

┌──(root㉿kali)-[/media/sf_vm_shared]
└─# mv Cattura_U3_W1_L3.pcapng /home/kali/Desktop

┌──(root㉿kali)-[/media/sf_vm_shared]
└─# cd /home/kali/Desktop

┌──(root㉿kali)-[~kali/Desktop]
└─# chmod ugo+rw Cattura_U3_W1_L3.pcapng

┌──(root㉿kali)-[~kali/Desktop]
└─# chown kali Cattura_U3_W1_L3.pcapng

┌──(root㉿kali)-[~kali/Desktop]
└─#
```

ANALISI E SOLUZIONI

Per la identificazione di eventuali ICO, ovvero evidenzia di attacchi in corso abbiamo visto che ci sono delle richieste TCP ripetute.
invece In base agli IOC trovati, ho fato delle ipotesi sui potenziali vettori di attacco utilizzati. e ho notato che ci possano essere stati delle scansioni sulla macchina target 192.168.200.150 dalla machina attaccante 192.168.200.100

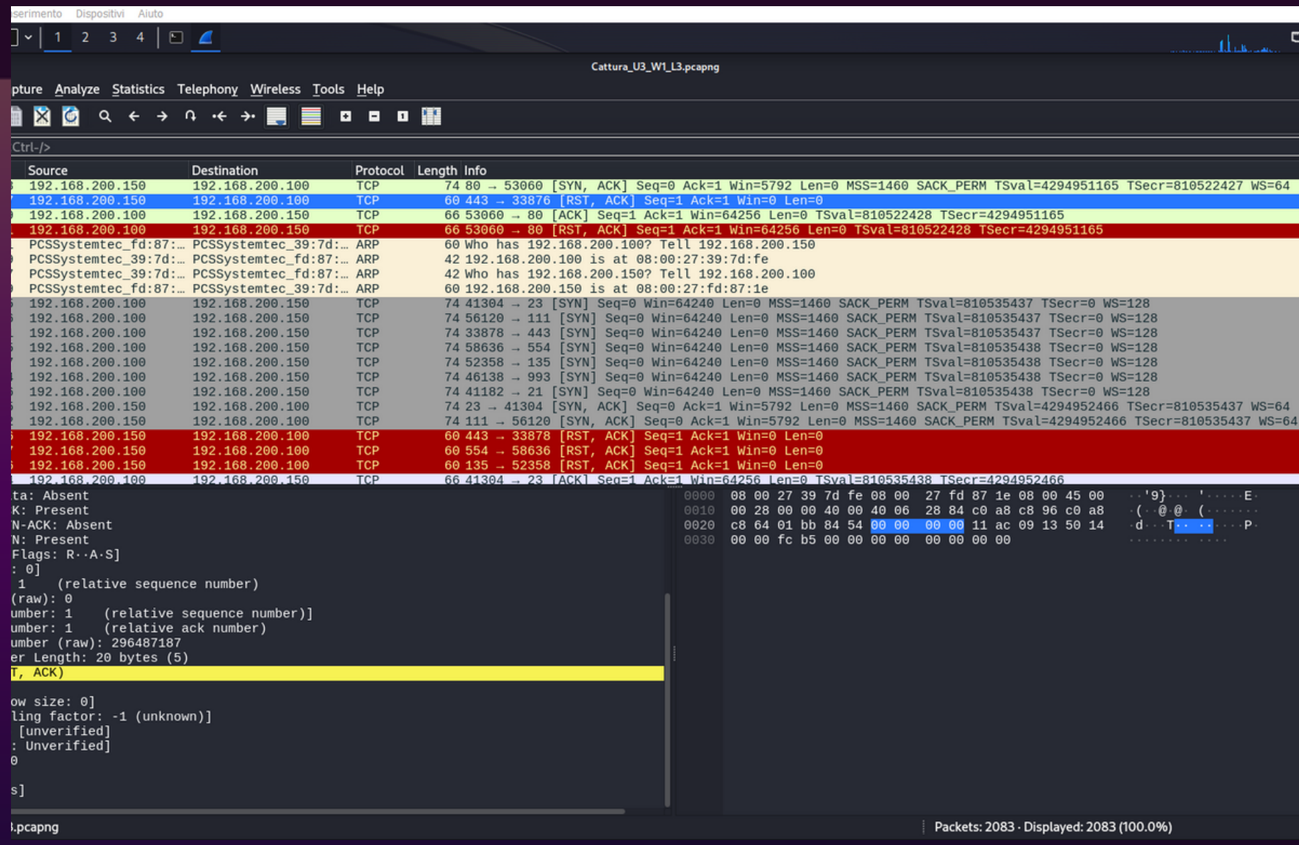
Un consiglio per ridurre gli impatti dell'attacco possono essere impostare delle regole nel firewall per negare l'accesso a tutte le porte da parte di quell'attaccante specifico. Questo impedirebbe all'attaccante di ottenere informazioni riguardanti le porte e i servizi attivi, proteggendo così il sistema da potenziali minacce.

SPIEGAZIONE

Dall'analisi dei dati catturati, emerge un pattern di numerose richieste TCP (SYN) provenienti dall'host 192.168.200.100 e dirette verso l'host target 192.168.200.150, con le porte di destinazione che variano costantemente. Questo suggerisce la possibilità di una scansione in corso da parte dell'host 192.168.200.100 per individuare porte aperte sul target. Tale ipotesi trova conferma nel fatto che alcune risposte del target sono [SYN+ACK], indicando porte aperte, mentre altre sono [RST+ACK], a indicare porte chiuse.

Come possiamo vedere dalla figura alla destra ci sono richieste SYN da parte dello scanner (le richieste evidenziane in grigio)

Invece evidenziati in rosso troviamo le risposte negative da parte dell'host. E la porta è chiusa




THANK YOU