

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. Configurare la cartella

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.

```
(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]
$
```

```
(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

(kali@kali)-[/media/sf_vm_shared]
# mv Cattura_U3_W1_L3.pcapng /home/kali/Desktop

(kali@kali)-[/media/sf_vm_shared]
# cd /home/kali/Desktop

(kali@kali)-[~kali/Desktop]
# chmod ugo+rw Cattura_U3_W1_L3.pcapng

(kali@kali)-[~kali/Desktop]
# chown kali Cattura_U3_W1_L3.pcapng

(kali@kali)-[~kali/Desktop]
#
```

ANALISI E SOLUZIONI

Per la identificazione di eventuali IOC, ovvero evidenza di attacchi in corso abbiamo visto che ci sono delle richieste TCP ripetute.

invece In base agli IOC trovati, ho fatto 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 macchina 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

serimentoDispositiviAiuto

1234

Cattura_U3_W1_L3.pcapng

ptureAnalyzeStatisticsTelephonyWirelessToolsHelp

Ctrl-/>

Source	Destination	Protocol	Length	Info
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 TSval=4294951165 TSecr=810522427 WS=64
192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
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=4294951165
PCSSystemtec_fd:87:...	PCSSystemtec_39:7d:...	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
PCSSystemtec_39:7d:...	PCSSystemtec_fd:87:...	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
PCSSystemtec_39:7d:...	PCSSystemtec_fd:87:...	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
PCSSystemtec_fd:87:...	PCSSystemtec_39:7d:...	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
192.168.200.150	192.168.200.100	TCP	74	23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466

ta: Absent
K: Present
N-ACK: Absent
N: Present
Flags: R·A·S]
: 0]
1 (relative sequence number)
(raw): 0
umber: 1 (relative sequence number)]
umber: 1 (relative ack number)
umber (raw): 296487187
er Length: 20 bytes (5)
T, ACK)

ow size: 0]
ling factor: -1 (unknown)]
[unverified]
: Unverified]
0
s]

l.pcapngPackets: 2083 · Displayed: 2083 (100.0%)



THANK YOU