

PROGETTO

S9L5

Presented by
Gabriele Turazza

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 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



PRIME IPOTESI

```
kali@kali: ~/Desktop
$ tshark -r Cattura_U3_W1_L5.pcapng -c 20
1 0.000000000 192.168.200.150 > 192.168.200.255 BROWSER 286 Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential Browser
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 TStamp=810522427 TSectr=0 WS=128
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 TStamp=810522428 TSectr=0 WS=128
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 TStamp=810522427 TSectr=810522427 WS=64
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 TStamp=810522428 TSectr=4294951165
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 TStamp=810522428 TSectr=4294951165
8 28.761629461 PCSSystemtec_fd:87:1e > PCSSystemtec_39:7d:fe ARP 60 Who has 192.168.200.100? Tell 192.168.200.150
9 28.761644619 PCSSystemtec_39:7d:fe > PCSSystemtec_fd:87:1e ARP 42 192.168.200.100 is at 08:00:27:39:7d:fe
10 28.774852257 PCSSystemtec_39:7d:fe > PCSSystemtec_fd:87:1e ARP 42 Who has 192.168.200.150? Tell 192.168.200.100
11 28.775230099 PCSSystemtec_fd:87:1e > PCSSystemtec_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 TStamp=810535437 TSectr=0 WS=128
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 TStamp=810535437 TSectr=0 WS=128
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 TStamp=810535437 TSectr=0 WS=128
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 TStamp=810535437 TSectr=0 WS=128
16 36.774405627 192.168.200.100 > 192.168.200.150 TCP 74 52358 > 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=810535438 TSectr=0 WS=128
17 36.774535534 192.168.200.100 > 192.168.200.150 TCP 74 46138 > 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=810535438 TSectr=0 WS=128
18 36.774614776 192.168.200.100 > 192.168.200.150 TCP 74 41182 > 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=810535438 TSectr=0 WS=128
19 36.774685505 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 TStamp=810535438 TSectr=4294951166 WS=64
20 36.774685652 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 TStamp=810535438 TSectr=810535437 WS=64
```

Azioni consigliate per mitigare l'attacco:

Bloccare l'IP 192.168.200.100 sul firewall del target, attivare IDS/IPS come Snort o Suricata per rilevare port scanning, segmentare la rete: la macchina vulnerabile dovrebbe essere isolata, limitare le porte aperte solo ai servizi strettamente necessari, utilizzare firewall host-based per rifiutare connessioni non autorizzate

in primis ho analizzato il file utilizzando il comando tshark -r Cattura_U3_W1_L5.pcapng -c 20, questo comando legge il file e mostra i primi 20 pacchetti. Utile per capire il traffico presente. Dal output ho potuto vedere un tentativo di port scanning, nel log vediamo numerosi pacchetti TCP con flag [SYN] verso varie porte sul sistema 192.168.200.150, provenienti da 192.168.200.100

La presenza di molte richieste SYN su porte diverse, in rapida sequenza, suggerisce:

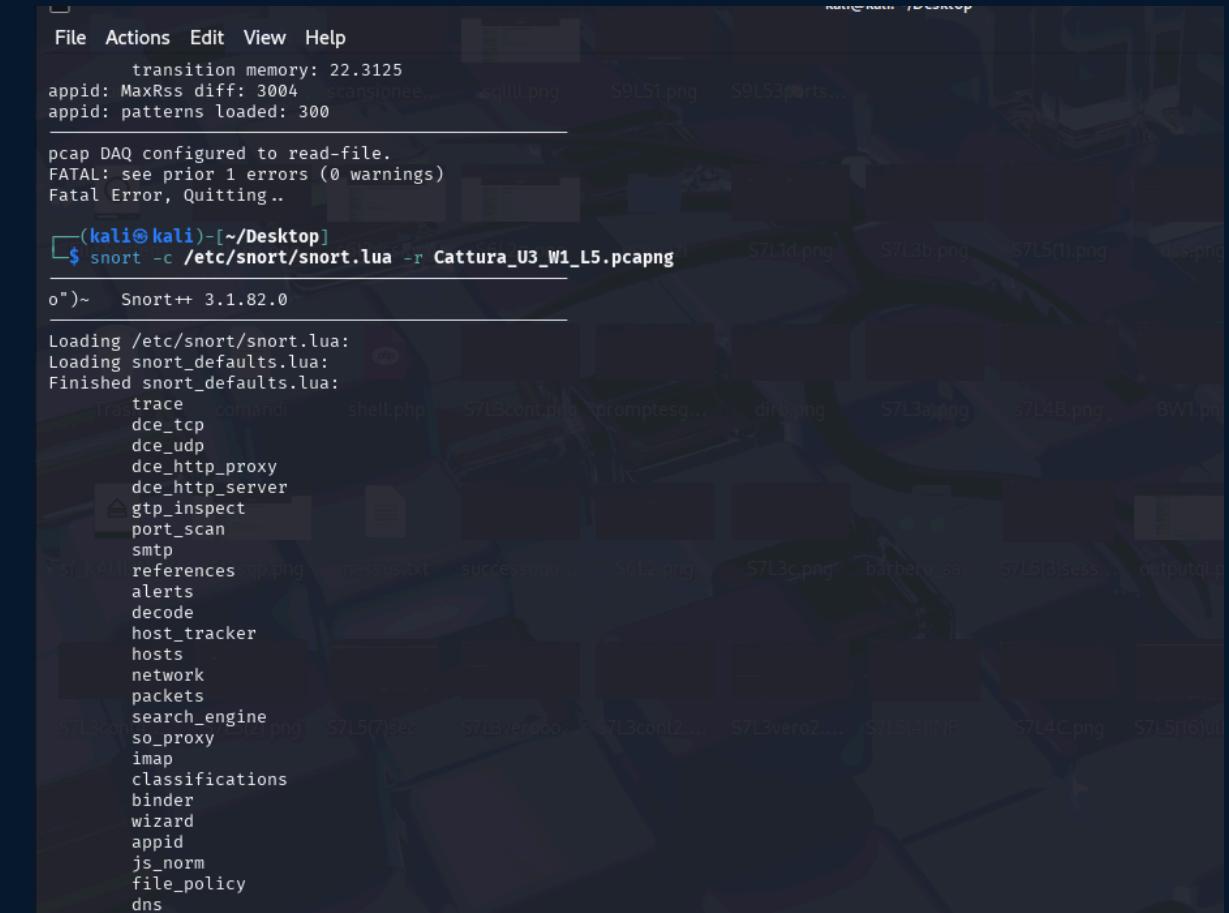
- Fase di ricognizione da parte di un attaccante (probabile scansione automatizzata)
- Potenziale utilizzo di strumenti come Nmap o moduli scanner di Metasploit

La riga 1 mostra: Host Announcement METASPLOITABLE, quindi il target 192.168.200.150 sembra essere una macchina Metasploitable, questo rafforza l'ipotesi di un attacco didattico simulato.

SECONDO TEST

Per un ulteriore verifica (dopo una ricerca approfondita) ho utilizzato SNORT, un IDS/IPS (Intrusion Detection/Prevention System), per analizzare un file di cattura di traffico di rete. Ecco una spiegazione breve:

- snort: Il comando per avviare Snort.
- -c /etc/snort/snort.lua: Specifica il file di configurazione di Snort (in formato LUA). Questo file contiene le regole e le impostazioni per l'analisi del traffico.
- -r Cattura_U3_W1_L5.pcapng: Analizza il file Cattura_U3_W1_L5.pcapng (un dump di traffico di rete in formato PCAPNG) in modalità offline (cioè senza monitorare la rete in tempo reale).



```
File Actions Edit View Help
transition memory: 22.3125
appid: MaxRss diff: 3004
appid: patterns loaded: 300
pcap DAQ configured to read-file.
FATAL: see prior 1 errors (0 warnings)
Fatal Error, Quitting..
(kali㉿kali)-[~/Desktop]
$ snort -c /etc/snort/snort.lua -r Cattura_U3_W1_L5.pcapng
o")~ Snort++ 3.1.82.0
Loading /etc/snort/snort.lua:
Loading snort_defaults.lua:
Finished snort_defaults.lua:
trace
dce_tcp
dce_udp
dce_http_proxy
dce_http_server
gtp_inspect
port_scan
smtp
references
alerts
decode
host_tracker
hosts
network
packets
search_engine
so_proxy
imap
classifications
binder
wizard
appid
js_norm
file_policy
dns
```

💡 Vettori di attacco rilevati da Snort		
Vettore Identificato	Evidenza nell'output	Spiegazione tecnica
ARP Spoofing	arp_spoof_packets: 4	Tentativo di manipolazione della cache ARP per sniffare il traffico o eseguire attacchi MITM.
Back Orifice	back_orifice_packets: 1	Presenza di un pacchetto associato a un trojan storico, spesso usato per controllo remoto.
Port Scanning (TCP)	port_scan_packets: 2079 , trackers: 8	Esecuzione di scansione di porte per identificare servizi attivi su un host.
UDP Scan	wizard_udp_scans: 1 , udp_misses: 1	Un tentativo di scansione su porta UDP, spesso usato per rilevare servizi vulnerabili.
Bad TCP Checksum	bad_tcp4_checksum: 1052	Potenziale evasione IDS o traffico manipolato. Può anche indicare un attacco o un replay.

Minaccia rilevata	Contromisura concreta
ARP Spoofing	- Abilitare ARP inspection dinamico su switch - Usare static ARP per host critici
Port scanning	- Implementare un firewall con filtraggio delle porte - Utilizzare tool di port knocking
Back Orifice (trojan)	- Utilizzare antivirus aggiornati - Segmentare la rete per isolamento dei dispositivi infetti
Checksum TCP errati	- Attivare verifiche IDS approfondite - Usare switch gestiti con monitoraggio integrità pacchetti
UDP scans	- Bloccare porte non utilizzate via firewall - Attivare rate limiting su pacchetti UDP sospetti

CONCLUSIONE

In conclusione, dopo i vari test (alcuni fallimentari) sono giunto alla conclusione che il file condiviso per questa esercitazione sia un brute force port scanning con nmap -sT, inoltre ho potuto notare anche tentativi di arp spoofing e un trojan di tipo backdoor per favorire gli attacchi MITM.

