

THREAT INTELLIGENCE & IOC

ANALISI DEL TRAFFICO DI RETE CON WIRESHARK

Tasks:

1. Identificazione di eventuali IOC e potenziali vettori d'attacco utilizzati
2. Azioni consigliate per ridurre gli impatti dell'attacco

Analisi del traffico di rete

Oggetto di analisi odierna è l'analisi del traffico di rete catturato nel seguente record di Wireshark:



Analizzeremo dunque il file di cattura utilizzando il tool menzionato. Una volta aperto il file, notiamo per prima cosa che l'indirizzo IP **192.168.200.150** corrisponde all'host name **Metasploitable**:

The screenshot shows the Wireshark interface with the file 'Cattura_U3_W1_L3.pcapng' open. The packet list pane shows a list of packets, with packet 1 selected. The packet details pane shows the following information:

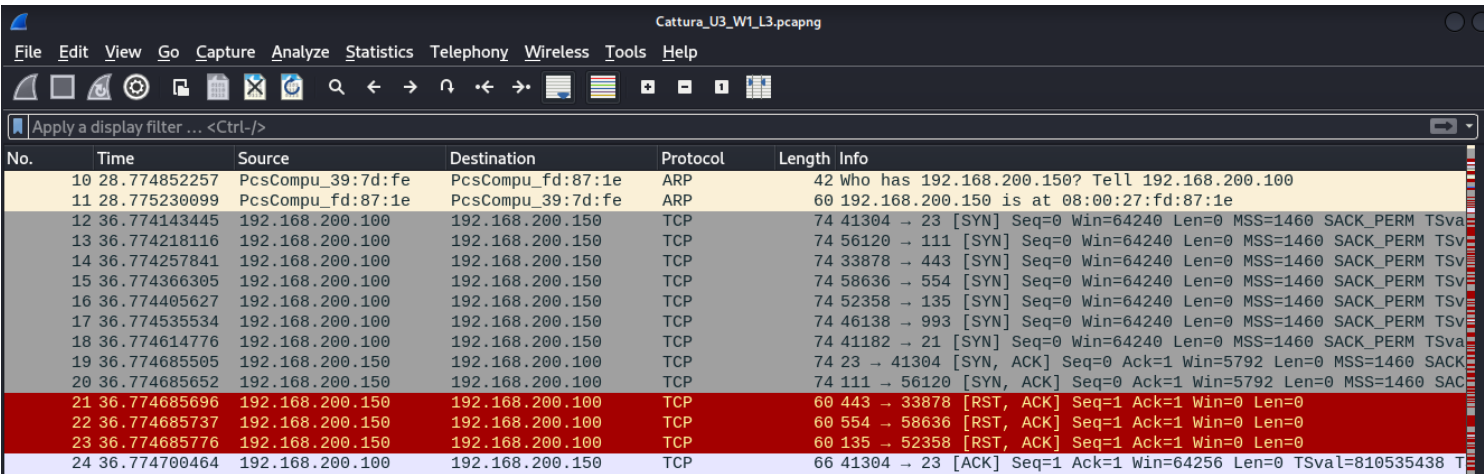
- Size: 93
- Mailslot Name: \MAILSLOT\BROWSE
- Microsoft Windows Browser Protocol
- Command: Host Announcement (0x01)
- Update Count: 1
- Update Periodicity: 2 minutes
- Host Name: METASPLOITABLE
- Windows version:
- OS Major Version: 4
- OS Minor Version: 9

The packet bytes pane shows the raw data of the packet, including the Host Name 'METASPLOITABLE' in the command field.

1. Identificazione di eventuali IOC e potenziali vettori d'attacco utilizzati

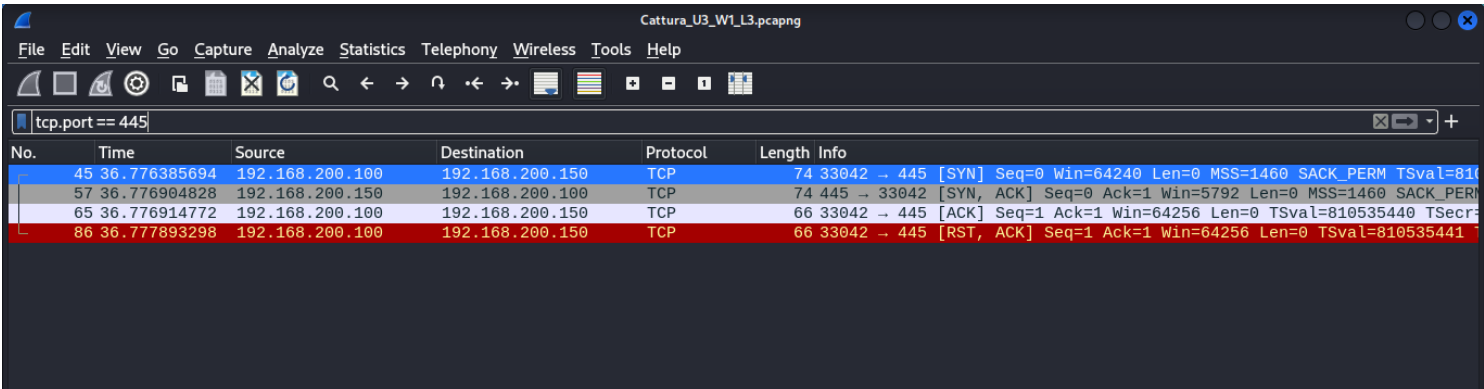
Analizzando la cattura, possiamo notare che:

- La comunicazione si svolge tra i due indirizzi IP **192.168.200.100** e **192.168.200.150** (Metasploitable)
- Risultano multiple richieste TCP su ampi intervalli di porte, il che è evidenza di un **port scanning** in corso al momento della cattura. Tali richieste risultano provenienti dalla macchina con IP 192.168.200.100 e hanno come target le porte dell'host con IP 192.168.200.150 (Metasploitable). Possiamo ipotizzare che il tool utilizzato sia stato nmap, per la sua estrema popolarità.



No.	Time	Source	Destination	Protocol	Length	Info
10	28.774852257	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PcsCompu_fd:87:1e	PcsCompu_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 TSval=810535440 TSecr=810535441
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 TSval=810535440 TSecr=810535441
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 TSval=810535440 TSecr=810535441
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 TSval=810535440 TSecr=810535441
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 TSval=810535440 TSecr=810535441
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 TSval=810535440 TSecr=810535441
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 TSval=810535440 TSecr=810535441
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 TSval=810535440 TSecr=810535441
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 TSval=810535440 TSecr=810535441
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=810535441

In dettaglio, possiamo dire che si tratta di una scansione con **three-way handshake completo**: nella figura sottostante ho preso in esame una delle porte aperte rilevate dalla scansione, ossia la numero 445. Come possiamo vedere nella figura sottostante, vengono completati tutti i passaggi del three-way handshake. Ciò ci fa pensare ad una scansione di tipo **TCP Connect (switch -sT)**, o una semplice scansione senza particolari switch, in quanto di default le scansioni effettuate con nmap completano il three-way handshake con la macchina target, ove possibile (= in caso di porte aperte).



No.	Time	Source	Destination	Protocol	Length	Info
45	36.776385694	192.168.200.100	192.168.200.150	TCP	74	33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=810535441
57	36.776904828	192.168.200.150	192.168.200.100	TCP	74	445 → 33042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=810535441
65	36.776914772	192.168.200.100	192.168.200.150	TCP	66	33042 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=810535441
86	36.777893298	192.168.200.100	192.168.200.150	TCP	66	33042 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=810535441

Inoltre, applicando i dovuti filtri al file di cattura (ossia andando alla ricerca di pacchetti con flag SYN, ACK) possiamo ricavare che le porte aperte sono in tutto 12:

No.	Time	Source	Destination	Protocol	Length	Info
4	23764777323	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
19	36774685505	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
20	36774685652	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
27	36775141273	192.168.200.150	192.168.200.100	TCP	74	21 > 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
35	36775796938	192.168.200.150	192.168.200.100	TCP	74	22 > 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
36	36775797004	192.168.200.150	192.168.200.100	TCP	74	80 > 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
57	36776904828	192.168.200.150	192.168.200.100	TCP	74	445 > 33042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
59	36776904961	192.168.200.150	192.168.200.100	TCP	74	139 > 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
61	36776905043	192.168.200.150	192.168.200.100	TCP	74	25 > 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
63	36776905123	192.168.200.150	192.168.200.100	TCP	74	53 > 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
164	36781487210	192.168.200.150	192.168.200.100	TCP	74	512 > 45648 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535445 WS=64
267	36788805940	192.168.200.150	192.168.200.100	TCP	74	514 > 51390 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952467 TSecr=810535452 WS=64
994	36825722553	192.168.200.150	192.168.200.100	TCP	74	513 > 42048 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952471 TSecr=810535489 WS=64

Porta 21 - ftp

Porta 22 - ssh

Porta 23 - telnet

Porta 25 - smtp

Porta 53 - domain

Porta 80 - http

Porta 111 - rpcbind

Porta 139 - netbios-ssn

Porta 445 - microsoft-ds

Porta 512 - exec

Porta 513 - remote login

Porta 514 - shell

2. Azioni consigliate per ridurre gli impatti dell'attacco

Alla luce delle vulnerabilità esposte, le azioni preventive consigliate sono:

- Chiudere le porte *critiche*, ossia maggiormente vulnerabili ad eventuali tentativi di accesso non autorizzati, qualora i corrispondenti servizi in ascolto non siano strettamente necessari (ad es. ftp, telnet, netbios, smb, remote login)
- Proteggere l'accesso ai servizi esposti tramite l'impostazione di policy mirate sul Firewall, ad esempio consentendovi l'accesso solo ad indirizzi IP autorizzati