

Per l'esercizio pratico di oggi, analizzare la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare eventuali IoC
- Fare delle ipotesi sui vettori d'attacco utilizzati
- Consigliare un'azione per ridurre gli impatti dell'attacco

Dalle analisi del file che ci è stato fornito si può notare come ci sia una serie di connessioni che partono da una macchina avente indirizzo IP 192.168.200.100 verso un'altra macchina avente indirizzo IP 192.168.200.150. Nella foto qua sotto possiamo vedere i primi pacchetti che sono stati sniffati tramite il tool Wireshark:

No.	T	Source	Destination	Protocol	Length	Info
1	8	698809880	192.168.200.150	192.168.200.255	BROWSER	288 M00! Announcement METASPLOITABLES, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potent
2	23	764214995	192.168.200.100	192.168.200.150	TCP	74 538606 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=180522427 Tscsr=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 Tsva=180522428 Tscsr=0 WS=128
4	23	764777323	192.168.200.150	192.168.200.100	TCP	74 80 - 538606 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsva=180522427 Tscsr=0 WS=64
5	23	764777457	192.168.200.150	192.168.200.100	TCP	74 80 - 538606 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsva=180522427 Tscsr=0 WS=64
6	23	764515209	192.168.200.100	192.168.200.150	TCP	66 538606 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=180522428 Tscsr=429495105
7	23	764899891	192.168.200.100	192.168.200.150	TCP	66 538606 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=180522428 Tscsr=429495105
8	28	761629461	PcsCompu-fd:87:1e	PcsCompu-39:7d:fe	ARP	60 Who has 192.168.200.100? Tell 192.168.200.150
9	28	761641401	PcsCompu-39:7d:fe	PcsCompu-fd:87:1e	ARP	42 192.168.200.100 is at 08:00:27:39:7d:fe
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	30	775230099	PcsCompu-39:7d:fe	PcsCompu-fd:87:1e	ARP	60 192.168.200.150 is at 08:00:27:fd:87:1e
12	38	774134345	192.168.200.100	192.168.200.150	TCP	74 41304 - 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=180535437 Tscsr=0 WS=128
13	76	774218116	192.168.200.100	192.168.200.150	TCP	74 56120 - 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=180535437 Tscsr=0 WS=128
14	38	774257841	192.168.200.100	192.168.200.150	TCP	74 33878 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=180535437 Tscsr=0 WS=128
15	76	774366395	192.168.200.100	192.168.200.150	TCP	74 58836 - 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=180535438 Tscsr=0 WS=128
16	76	774405627	192.168.200.100	192.168.200.150	TCP	74 52928 - 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=180535438 Tscsr=0 WS=128
17	76	774355354	192.168.200.100	192.168.200.150	TCP	74 46138 - 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=180535438 Tscsr=0 WS=128
18	38	774614776	192.168.200.100	192.168.200.150	TCP	74 41182 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=180535438 Tscsr=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 Tsva=180535437 WS=64
20	76	774685052	192.168.200.150	192.168.200.100	TCP	74 111 - 56120 [ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsva=180535437 WS=64
21	30	774655996	192.168.200.150	192.168.200.100	TCP	66 538606 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=180535437 Tscsr=429495246 Tscsr=180535437 WS=64
22	76	774685737	192.168.200.150	192.168.200.100	TCP	66 538606 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=180535437 Tscsr=429495246 Tscsr=180535437 WS=64
23	30	774685776	192.168.200.150	192.168.200.100	TCP	66 935 - 52358 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=180535437 Tscsr=429495246 Tscsr=180535437 WS=64

Nella prima riga possiamo vedere l'host announcement, messaggio che viene inviato dal server quando il suo servizio viene avviato, per annunciarsi. Nelle righe successive possiamo vedere come l'IP 192.168.200.100 faccia una serie di connessioni usando il protocollo TCP. Nelle immagini successive ho selezionato alcune tra le principali porte well known:

No.	Time	Source	Destination	Protocol	Length	Info
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=9 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
27	36.774121273	192.168.200.150	192.168.200.100	TCP	74	21 → 41182 [SYN, ACK] Seq=9 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
39	36.775861964	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

No.	Time	Source	Destination	Protocol	Length	Info
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=810535437 TSecr=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 TSval=4294952466 TSecr=810535437 WS=64
24	36.774709464	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
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

No.	Time	Source	Destination	Protocol	Length	Info
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 TSval=810522428 TSecr=0 WS=128
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
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=810535437 TSecr=0 WS=128
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

No.	Time	Source	Destination	Protocol	Length	Info
352	36.793242024	192.168.208.108	192.168.280.150	TCP	74	49592 → 515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=818535456 TSecr=0 WS=128
355	36.793442026	192.168.208.158	192.168.280.100	TCP	60	515 → 49592 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

No.	Time	Source	Destination	Protocol	Length	Info
1655	36.855989752	192.168.200.100	192.168.200.150	TCP	74	35216 → 700 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535519 TSecr=0 WS=128
1659	36.856118782	192.168.200.150	192.168.200.100	TCP	60	700 → 35216 [RST] ACK1 Seq=1 Ack=1 Win=0 Len=0

any tcp.port ==1050

No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

La mia ipotesi è che quanto intercettato da Wireshark sia una scansione con Nmap, o comunque un altro tool di scansione, per andare a vedere quali siano le porte aperte e i relativi servizi della macchina con indirizzo IP 192.168.200.150. Possiamo notare la differenza tra le porte aperte e quelle chiuse dal fatto che nelle prime viene completato il three way handshake (es porta 21, 23, 443). Per le porte chiuse non viene completato il three way handshake (es porta 515, 700). invece notiamo come andando oltre la porta 1024 non vi è alcun tentativo di connessione (es porta 1050). Questo rientra tra gli indicatori di compromissione, poiché multiple richieste TCP su ampi intervalli di porte indicano una scansione in corso.

Il mio consiglio per andare a ridurre l'impatto d'attacco è quello di configurare il firewall in modo tale che solo indirizzi IP scelti possano andare a comunicare con la nostra macchina, andando ad impedire così che una macchina estranea possa andare ad eseguire delle scansioni per scoprire le porte aperte e i relativi servizi per cercare una vulnerabilità da sfruttare e causare danni alla nostra macchina.