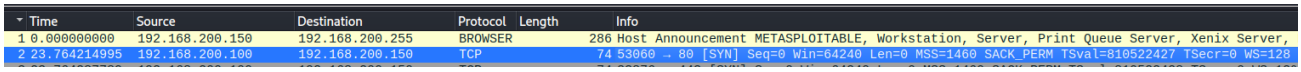
Threat Intelligence & IOC - Wireshark

Gli **IOC** (Indicatori di compromissione) sono evidenze degli attacchi e vengono usati per capire cosa è successo e fare una ricostruzione degli attacchi subiti.

Fornisco anzitutto l'analisi di un singolo pacchetto intercettato da Wireshark. Prendo ad esempio il secondo.

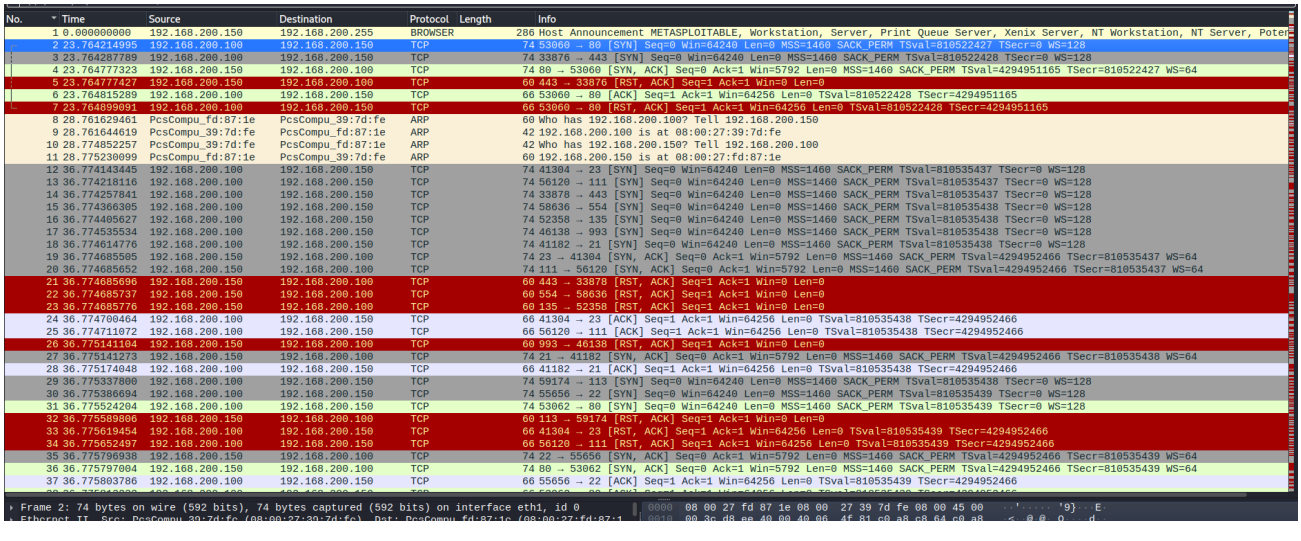


	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server,
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128

- 2: è il numero di sequenza del pacchetto, che indica l'ordine dei pacchetti intercettati
- 23.764214995: è il timestamp e indica il momento in cui il pacchetto è stato catturato.
- **192.168.200.100: è l'indirizzo IP sorgente del pacchetto**
- **192.168.200.150: è l'indirizzo IP destinazione del pacchetto**
- **TCP: il pacchetto utilizza il protocollo TCP**
- 74: è la dimensione del pacchetto in byte.
- **53060 → 80: il pacchetto viaggia dalla porta TCP 53060 sorgente alla TCP 80 di destinazione**.
- **[SYN]: il pacchetto è usato per avviare una sessione di comunicazione TCP.**
- Seq=0: il numero di sequenza iniziale del pacchetto, utilizzato per sincronizzare la comunicazione tra i dispositivi.
- Win=64240: la finestra di ricezione, ovvero la quantità di dati che il dispositivo destinazione è in grado di accettare in una volta sola.
- Len=0: la lunghezza del carico utile del pacchetto, che in questo caso è pari a zero.
- MSS=1460: indica la dimensione massima del segmento TCP che il dispositivo mittente è in grado di accettare.
- SACK_PERM: indica che la comunicazione supporta l'uso di opzioni di conferma di ricezione selettiva (SACK).
- TSval=810522427: il valore del timestamp TCP del pacchetto mittente.
- TSecr=0: il valore del timestamp TCP del pacchetto destinazione.
- WS=128: indica la quantità di dati che il mittente è in grado di inviare prima di ricevere una conferma di ricezione dal destinatario.

Identifcazione IOC

Di seguito uno screen dei primi 37 pacchetti, sebbene in totale siano 2083:



No.	Time	Source	Destination	Protocol	Length	Info
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, Poter
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 TSval=810522427 TSecr=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 TSval=810522428 TSecr=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 TSval=4294951165 TSecr=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 TSval=810522428 TSecr=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 TSval=810522428 TSecr=4294951165
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	28.761644619	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	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=810535437 TSecr=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 TSval=810535437 TSecr=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 TSval=810535437 TSecr=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 TSval=810535438 TSecr=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 TSval=810535438 TSecr=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 TSval=810535438 TSecr=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 TSval=810535438 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
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=4294952466 TSecr=810535437 WS=64
21	36.774685690	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=4294952466
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	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
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
29	36.775337800	192.168.200.100	192.168.200.150	TCP	74	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30	36.775386604	192.168.200.100	192.168.200.150	TCP	74	55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
32	36.775589806	192.168.200.150	192.168.200.100	TCP	60	113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
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
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35	36.775796938	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	36.775797004	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
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

Dall'analisi complessiva di tutti i pacchetti si denota che:

- Gli indirizzi sorgenti e di destinazione sono solo 2, il che vuol dire che la comunicazione intercettata è probabilmente

avvenuta su una rete interna tra due macchine virtuali
- Le porte di destinazione dei vari pacchetti sono moltissime, diverse tra loro e in molti casi, poco comuni. Da questo si deduce che il traffico intercettato è quello di una scansione.
Dall' 8° all 11° pacchetto (nello screen su) ci sono dei pacchetti ci sono delle richieste ARP. Sappiamo che nmap usa questo protocollo per individuare i dispositivi attivi nella rete. Da ciò deduciamo che il traffico intercettato è quello di una scansione nmap.
- I pacchetti usati per avviare la comunicazione TCP sono quasi tutti SYN e RST ACK. Quelli con sfondo bianco sono ACK e ce ne sono diversi SYN ACK. Ciò ci suggerisce che la scansione avviata con nmap sia stata usata con -sT. Se fosse stata una scansione -sS non ci sarebbero stati risultati ACK.

Ricostruzione dell'attacco subito

L'attaccante ha inviato una scansione con una serie di pacchetti SYN ai diversi numeri di porta dell'ip target, cercando di stabilire una connessione TCP:

- Se la porta è aperta, il dispositivo target invia un pacchetto SYN ACK in risposta, indicando che è pronto ad accettare la connessione. L'attaccante può quindi inviare un pacchetto ACK per completare la connessione TCP e avviare la comunicazione.
- Se la porta è chiusa, il dispositivo target invia un pacchetto RST ACK.

Pertanto concludiamo che la presenza dei molti pacchetti SYN e dei molti pacchetti RST ACK, ci indica che qualcuno sta effettuando una scansione delle porte sul dispositivo destinazione. La presenza di alcuni pacchetti SYN ACK e ACK, ci indica che alcune porte sono aperte e che l'attaccante ha identificato quelle porte.

Soluzioni per ridurre gli impatti dell'attacco

1. Aggiornare il software e il sistema operativo: è importante mantenere il software e il sistema operativo della macchina aggiornati con le ultime patch di sicurezza per correggere eventuali vulnerabilità.
2. Installare un firewall: un firewall può aiutare a impedire l'accesso non autorizzato alla macchina bloccando il traffico di rete indesiderato.
3. Configurare le porte: se le porte aperte sulla tua macchina non sono necessarie, è possibile chiuderle o disattivarle per ridurre il rischio di attacchi.
4. Monitorare il traffico di rete piu frequentemente