Threat Intelligence & IOC

INDICE

1. **Traccia**
2. **Wireshark**
3. **Cattura di rete**
4. **SYN scan**
5. **Analisi**
6. **Conclusioni - azioni di mitigazione**

EPICODE

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 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

EPICODE

Wireshark

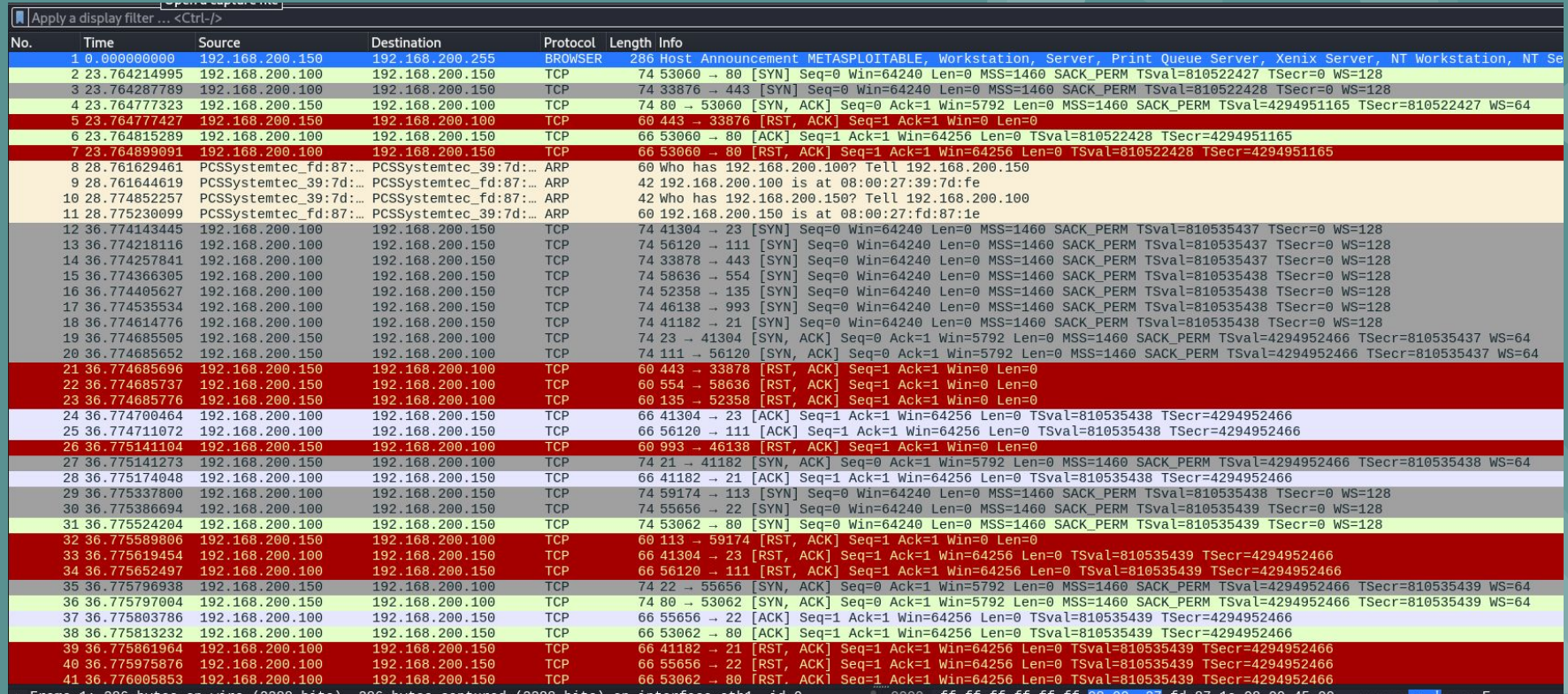
Wireshark è uno degli analizzatori di pacchetti più conosciuto e utilizzato; è open source ed è disponibile per Windows, MAC OS X e Linux. Il software può catturare, salvare, importare ed esportare i pacchetti di rete; include un sistema di filtraggio completo e colori diversificati in base al tipo di pacchetto catturato.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host

- **No**: numero del pacchetti, sono ordinati in base al tempo di arrivo;
- **Time**: tempo di arrivo del pacchetto;
- **Source**: l'indirizzo da cui il pacchetto arriva;
- **Destination**: l'indirizzo a cui è andato il pacchetto;
- **Protocol**: il tipo di protocollo che sta utilizzando, in questo caso è una richiesta HTTP;
- **Lenght**: lunghezza del pacchetto;
- **Info**: informazioni aggiuntive, in questo caso mostra che è una richiesta GET.

Cattura di rete

Andando ad analizzare la cattura di rete eseguita con Wireshark, possiamo notare la presenza di molteplici richieste TCP, questo può condurci a pensare ad un'attività di scansione da parte di un client remoto.

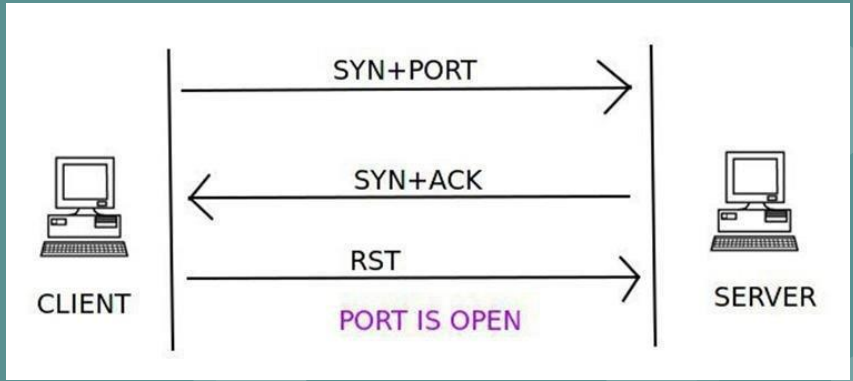

Apply a display filter ... <Ctrl-/>

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 Se
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	PCSSystemtec_fd:87:…	PCSSystemtec_39:7d:…	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d:…	PCSSystemtec_fd:87:…	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PCSSystemtec_39:7d:…	PCSSystemtec_fd:87:…	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PCSSystemtec_fd:87:…	PCSSystemtec_39:7d:…	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	36.774685696	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=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	36.775386694	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
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 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
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41	36.776005853	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announc
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [
8	28.761629461	PCSSystemtec_fd:87:…	PCSSystemtec_39:7d:…	ARP	60	Who has 192.

Buona parte delle tecniche più comuni tentano di colpire porte TCP, poiché quest'ultime utilizzano un protocollo connection-oriented, per la quale si ottiene un feedback utile all'attaccante. Questa tipologia di attacchi viene definita come TCP scanning e si basano sull'instaurazione di una connessione TCP, anche se in pochi casi verrà effettivamente completamente stabilita. Alcuni tipi di TCP scan sono: TCP connect, SYN, FIN, ACK, XMAS, NULL.

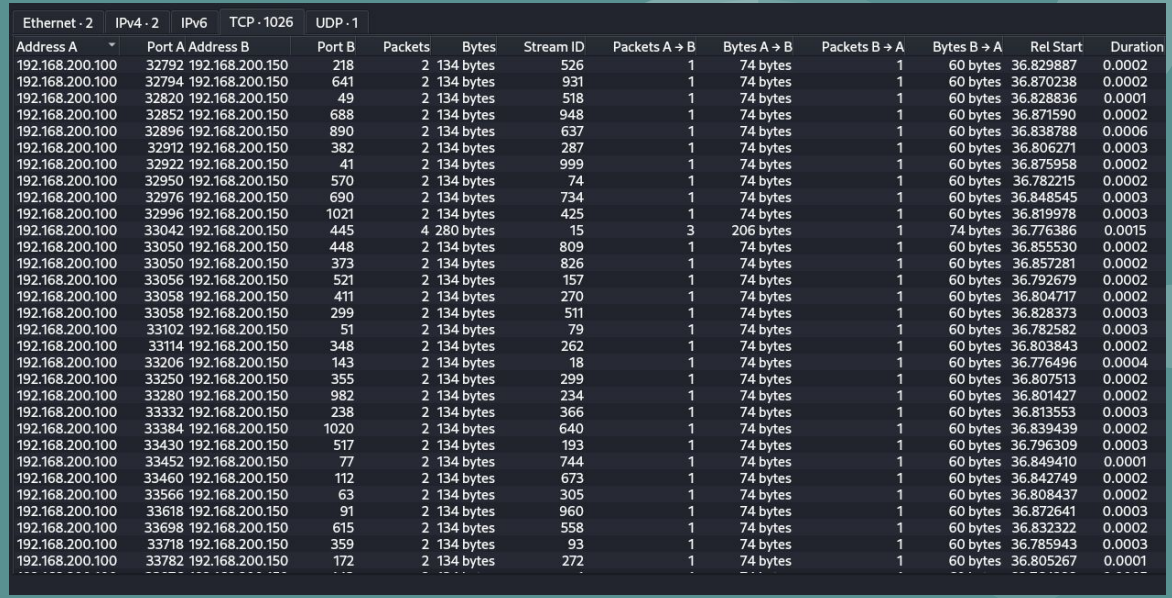
SYN Scan



Il SYN scan è tra le tecniche di port scanning più utilizzate, questo grazie alla velocità infatti è possibile scansionare migliaia di porte per secondo. L'attaccante quindi controlla ogni singola porta inviando un pacchetto SYN, quelle aperte risponderanno con un SYN|ACK, mentre quelle chiuse con un RST, di conseguenza non verrà completato l'handshake a 3-vie necessaria per stabilire una connessione TCP, ma bensì essa cadrà nel momento in cui la vittima invierà la risposta. Mentre nel caso non si riceva alcun riscontro, o si riceva un messaggio ICMP di tipo 3 (Porta non raggiungibile), ciò implica che la porta sarà probabilmente filtrata da un packet filter.

Analisi

Ci spostiamo sul tab *Statistics*, posizioniamoci su *Protocol*, ed infine su *Conversation* per poter controllare tutte le informazioni sui protocolli in modo più dettagliato. Possiamo notare che vengono inviati pacchetti TCP a tutte le porte fino alla porta 1024, questo ci porta a realizzare che sta avvenendo un *port scanning*.
Tuttavia le porte sono quasi tutte chiuse perché il three-way-handshake non viene completato.



Ethernet · 2 | IPv4 · 2 | IPv6 | TCP · 1026 | UDP · 1

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
192.168.200.100	32792	192.168.200.150	218	2	134 bytes	526	1	74 bytes	1	60 bytes	36.829887	0.0002
192.168.200.100	32794	192.168.200.150	641	2	134 bytes	931	1	74 bytes	1	60 bytes	36.870238	0.0002
192.168.200.100	32820	192.168.200.150	49	2	134 bytes	518	1	74 bytes	1	60 bytes	36.828836	0.0001
192.168.200.100	32852	192.168.200.150	688	2	134 bytes	948	1	74 bytes	1	60 bytes	36.871590	0.0002
192.168.200.100	32896	192.168.200.150	890	2	134 bytes	637	1	74 bytes	1	60 bytes	36.838788	0.0006
192.168.200.100	32912	192.168.200.150	382	2	134 bytes	287	1	74 bytes	1	60 bytes	36.806271	0.0003
192.168.200.100	32922	192.168.200.150	41	2	134 bytes	999	1	74 bytes	1	60 bytes	36.875958	0.0002
192.168.200.100	32950	192.168.200.150	570	2	134 bytes	74	1	74 bytes	1	60 bytes	36.782215	0.0002
192.168.200.100	32976	192.168.200.150	690	2	134 bytes	734	1	74 bytes	1	60 bytes	36.848545	0.0003
192.168.200.100	32996	192.168.200.150	1021	2	134 bytes	425	1	74 bytes	1	60 bytes	36.819978	0.0003
192.168.200.100	33042	192.168.200.150	445	4	280 bytes	15	3	206 bytes	1	74 bytes	36.776386	0.0015
192.168.200.100	33050	192.168.200.150	448	2	134 bytes	809	1	74 bytes	1	60 bytes	36.855530	0.0002
192.168.200.100	33050	192.168.200.150	373	2	134 bytes	826	1	74 bytes	1	60 bytes	36.857281	0.0002
192.168.200.100	33056	192.168.200.150	521	2	134 bytes	157	1	74 bytes	1	60 bytes	36.792679	0.0002
192.168.200.100	33058	192.168.200.150	411	2	134 bytes	270	1	74 bytes	1	60 bytes	36.804717	0.0002
192.168.200.100	33058	192.168.200.150	299	2	134 bytes	511	1	74 bytes	1	60 bytes	36.828373	0.0003
192.168.200.100	33102	192.168.200.150	51	2	134 bytes	79	1	74 bytes	1	60 bytes	36.782582	0.0003
192.168.200.100	33114	192.168.200.150	348	2	134 bytes	262	1	74 bytes	1	60 bytes	36.803843	0.0002
192.168.200.100	33206	192.168.200.150	143	2	134 bytes	18	1	74 bytes	1	60 bytes	36.776496	0.0004
192.168.200.100	33250	192.168.200.150	355	2	134 bytes	299	1	74 bytes	1	60 bytes	36.807513	0.0002
192.168.200.100	33280	192.168.200.150	982	2	134 bytes	234	1	74 bytes	1	60 bytes	36.801427	0.0002
192.168.200.100	33332	192.168.200.150	238	2	134 bytes	366	1	74 bytes	1	60 bytes	36.813553	0.0003
192.168.200.100	33384	192.168.200.150	1020	2	134 bytes	640	1	74 bytes	1	60 bytes	36.839439	0.0002
192.168.200.100	33430	192.168.200.150	517	2	134 bytes	193	1	74 bytes	1	60 bytes	36.796309	0.0003
192.168.200.100	33452	192.168.200.150	77	2	134 bytes	744	1	74 bytes	1	60 bytes	36.849410	0.0001
192.168.200.100	33460	192.168.200.150	112	2	134 bytes	673	1	74 bytes	1	60 bytes	36.842749	0.0002
192.168.200.100	33566	192.168.200.150	63	2	134 bytes	305	1	74 bytes	1	60 bytes	36.808437	0.0002
192.168.200.100	33618	192.168.200.150	91	2	134 bytes	960	1	74 bytes	1	60 bytes	36.872641	0.0003
192.168.200.100	33698	192.168.200.150	615	2	134 bytes	558	1	74 bytes	1	60 bytes	36.832322	0.0002
192.168.200.100	33718	192.168.200.150	359	2	134 bytes	93	1	74 bytes	1	60 bytes	36.785943	0.0003
192.168.200.100	33782	192.168.200.150	172	2	134 bytes	272	1	74 bytes	1	60 bytes	36.805267	0.0001

Abbiamo tracciato un tentativo di port scanning eseguito sulla macchina 192.168.200.100 verso la macchina 192.168.200.150.

Conclusioni -azioni di mitigazione

Una tecnica di prevenzione contro questa potenziale minaccia è sicuramente la configurazione di alcune regole nel firewall. In questo modo, le regole configurate andrebbero a bloccare le scansione che provengono dall'IP attaccante, andando a contrastarlo e quindi negandogli l'accesso e l'acquisizione delle informazioni sulle porte aperte all'interno del nostro sistema.
Per limitare l'accesso, lasciamo accessibili solo le porte necessarie, chiudiamo quelle che non vengono utilizzate
Eseguiamo sempre un sistema di monitoraggio per poter identificare le attività sospette e altri port scanning.