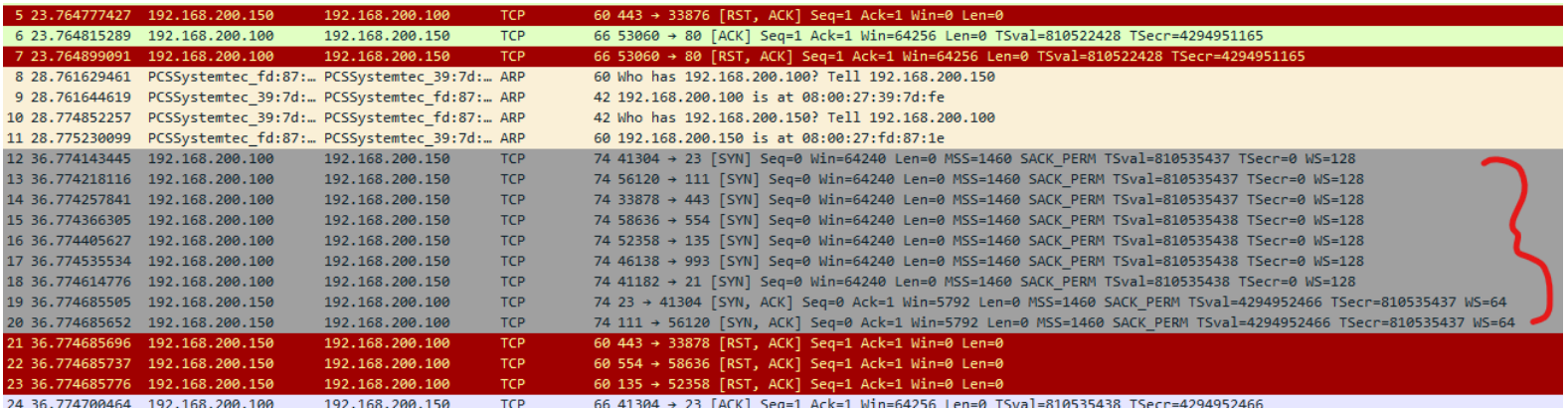
S9/L3

L’esercizio di oggi prevede di analizzare un file di Wireshark , cercando di individuare richieste o pacchetti sospetti.
Wireshark è un software per analisi di protocollo o *packet sniffer* utilizzato per la soluzione di problemi di rete, per l'analisi e lo sviluppo di protocolli o di software di comunicazione e per la didattica, possedendo tutte le caratteristiche di un analizzatore di protocollo standard.

La traccia è la seguente:
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.

Dopo aver scaricato il file e unzippato , lo apriamo in Wireshark e cerchiamo le anomalie.
Di seguito ci saranno 2 immagini allegate.



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

398	36.795684369	192.168.200.150	192.168.200.100	TCP	60 814 → 53828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
399	36.795684428	192.168.200.150	192.168.200.100	TCP	60 683 → 56982 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
400	36.795726078	192.168.200.100	192.168.200.150	TCP	74 44560 → 731 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535459 TSecr=0 WS=128
401	36.795806610	192.168.200.100	192.168.200.150	TCP	74 39176 → 405 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535459 TSecr=0 WS=128
402	36.795888644	192.168.200.100	192.168.200.150	TCP	74 37760 → 318 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535459 TSecr=0 WS=128
403	36.795966048	192.168.200.100	192.168.200.150	TCP	74 40454 → 321 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535459 TSecr=0 WS=128
404	36.796043782	192.168.200.100	192.168.200.150	TCP	74 54344 → 909 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535459 TSecr=0 WS=128
405	36.796136358	192.168.200.100	192.168.200.150	TCP	74 35948 → 188 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535459 TSecr=0 WS=128
406	36.796199746	192.168.200.100	192.168.200.150	TCP	74 57508 → 310 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535459 TSecr=0 WS=128
407	36.796308835	192.168.200.100	192.168.200.150	TCP	74 33430 → 517 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535460 TSecr=0 WS=128
408	36.796400927	192.168.200.100	192.168.200.150	TCP	74 45276 → 539 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535460 TSecr=0 WS=128
409	36.796479443	192.168.200.100	192.168.200.150	TCP	74 40832 → 1019 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535460 TSecr=0 WS=12
410	36.796569127	192.168.200.150	192.168.200.100	TCP	60 83 → 55216 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
411	36.796569225	192.168.200.150	192.168.200.100	TCP	60 65 → 41520 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
412	36.796569265	192.168.200.150	192.168.200.100	TCP	60 731 → 44560 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
413	36.796569306	192.168.200.150	192.168.200.100	TCP	60 405 → 39176 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
414	36.796569347	192.168.200.150	192.168.200.100	TCP	60 318 → 37760 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
415	36.796569388	192.168.200.150	192.168.200.100	TCP	60 321 → 40454 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
416	36.796569428	192.168.200.150	192.168.200.100	TCP	60 909 → 54344 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

La prima cosa che salta all'occhio sono le ripetute richieste TCP (in grigio) su diverse porte. Si evince che sia in corso una scansione delle porte sulla macchina interessata, probabilmente l'attaccante **(192.168.200.100)** sta cercando delle porte aperte in modo da sfruttare delle vulnerabilità ed entrare all'interno della macchina vittima **(192.168.200.150)**.

Per evitare di farci attaccare potremmo configurare il firewall bloccando tutte le richieste dall'indirizzo IP dell'attaccante.