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.

Questa era la traccia dell' esercizio odierno.

Premettiamo dicendo che un **IOC** è un Indicator Of Compromise (Indicatore di Compromissione), ovvero un segnale di un' anomalia all' interno di un sistema informatico, che indica che c'è un attacco in corso.

Per l' esercizio dovevamo analizzare una schermata di cattura eseguita con Wireshark, trovare evidenze di un IOC e consigliare un' azione per ridurre l' impatto dell' attacco sul target.

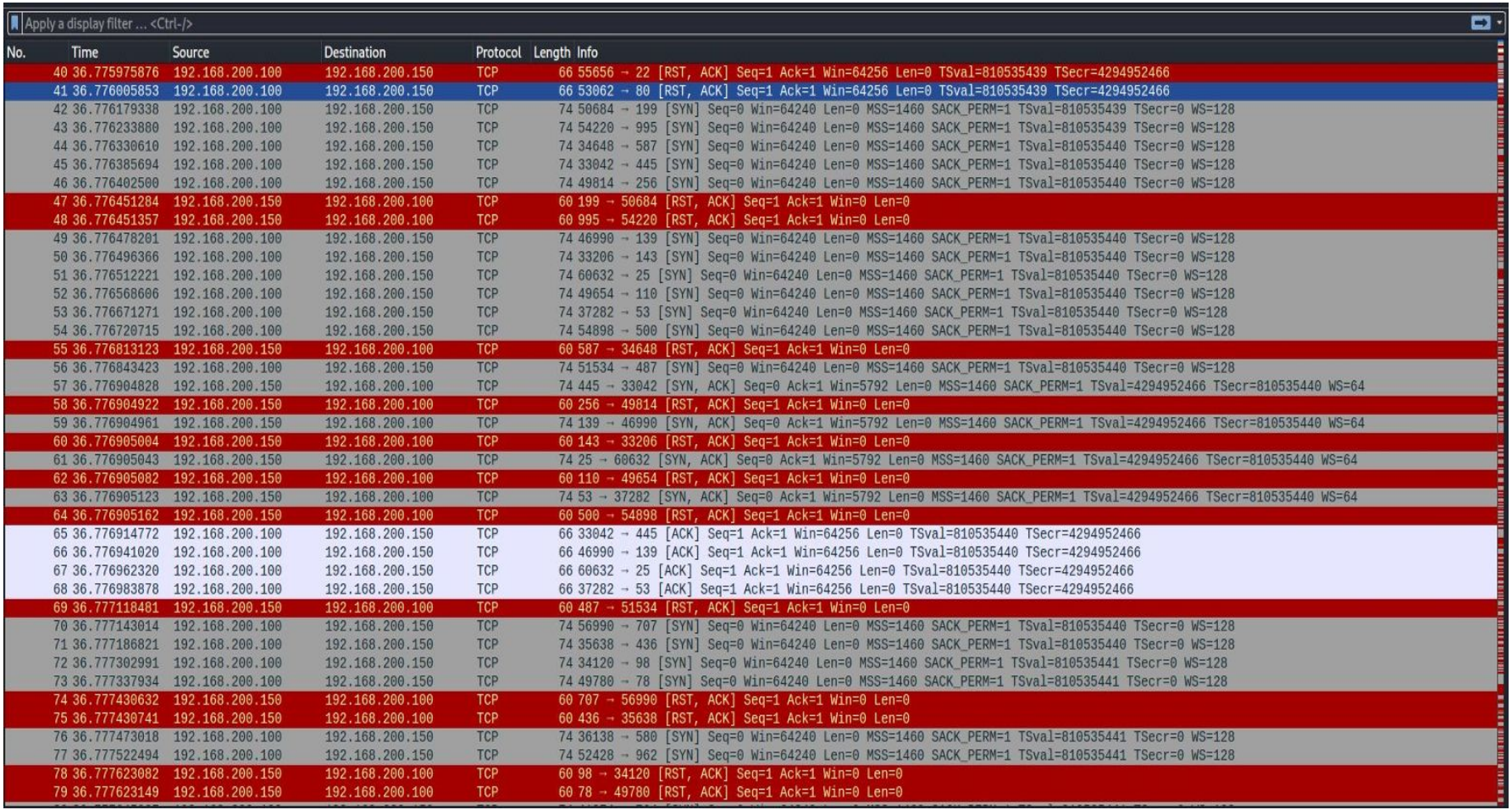
La prima cosa che salta all' occhio dalla cattura è la presenza di un elevatissimo numero di richieste **TCP** (**T**ransfer **C**ontrol **P**rotocol) su porte differenti. Gli indirizzi IP sono solo due, quello dell' Host da cui partono le richieste (**192.168.200.100**) e quello del Target (**192.168.200.150**).

Il motivo principale per questo elevatissimo numero di pacchetti su un singolo host e su più porte diverse da parte di un solo indirizzo IP è quasi certamente una **scansione del sistema** da parte di un potenziale criminale informatico.

Infatti, come vediamo dalla cattura, l' host sta inviando delle richieste **SYN** al target e, lì dove una specifica porta risulta aperta, il target risponde con il **SYN ACK**, mentre dove la porta risulta essere chiusa risponde con un **RST ACK**.

Molto probabilmente si tratta quindi di una scansione di sistema e porte sul target 192.168.200.150;

A prima vista potrebbe sembrare un attacco **Ddos**, anche se generalmente questo tipo di attacco è rivolto piuttosto ad una singola porta per riuscire a bloccare e rendere inutilizzabile uno specifico servizio, non a più porte come in questo caso.


Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
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
42 36.776179338 192.168.200.100 192.168.200.150 TCP 74 50684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
43 36.776233880 192.168.200.100 192.168.200.150 TCP 74 54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
44 36.776330610 192.168.200.100 192.168.200.150 TCP 74 34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
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=1 TSval=810535440 TSecr=0 WS=128
46 36.776402500 192.168.200.100 192.168.200.150 TCP 74 49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
47 36.776451284 192.168.200.150 192.168.200.100 TCP 60 199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48 36.776451357 192.168.200.150 192.168.200.100 TCP 60 995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49 36.776478201 192.168.200.100 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
50 36.776496366 192.168.200.100 192.168.200.150 TCP 74 33206 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
51 36.776512221 192.168.200.100 192.168.200.150 TCP 74 60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
52 36.776568606 192.168.200.100 192.168.200.150 TCP 74 49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
54 36.776720715 192.168.200.100 192.168.200.150 TCP 74 54898 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
55 36.776813123 192.168.200.150 192.168.200.100 TCP 60 587 → 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56 36.776843423 192.168.200.100 192.168.200.150 TCP 74 51534 → 487 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
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=1 TSval=4294952466 TSecr=810535440 WS=64
58 36.776904922 192.168.200.150 192.168.200.100 TCP 60 256 → 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59 36.776904961 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=1 TSval=4294952466 TSecr=810535440 WS=64
60 36.776905004 192.168.200.150 192.168.200.100 TCP 60 143 → 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61 36.776905043 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=1 TSval=4294952466 TSecr=810535440 WS=64
62 36.776905082 192.168.200.150 192.168.200.100 TCP 60 110 → 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63 36.776905123 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=1 TSval=4294952466 TSecr=810535440 WS=64
64 36.776905162 192.168.200.150 192.168.200.100 TCP 60 500 → 54898 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
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=4294952466
66 36.776941020 192.168.200.100 192.168.200.150 TCP 66 46990 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
67 36.776962320 192.168.200.100 192.168.200.150 TCP 66 60632 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
68 36.776983878 192.168.200.100 192.168.200.150 TCP 66 37282 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
69 36.777118481 192.168.200.150 192.168.200.100 TCP 60 487 → 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
70 36.777143014 192.168.200.100 192.168.200.150 TCP 74 56990 → 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
71 36.777186821 192.168.200.100 192.168.200.150 TCP 74 35638 → 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
72 36.777302991 192.168.200.100 192.168.200.150 TCP 74 34120 → 98 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
73 36.777337934 192.168.200.100 192.168.200.150 TCP 74 49780 → 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
74 36.777430632 192.168.200.150 192.168.200.100 TCP 60 707 → 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75 36.777430741 192.168.200.150 192.168.200.100 TCP 60 436 → 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76 36.777473018 192.168.200.100 192.168.200.150 TCP 74 36138 → 580 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
77 36.777522494 192.168.200.100 192.168.200.150 TCP 74 52428 → 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
78 36.777623082 192.168.200.150 192.168.200.100 TCP 60 98 → 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79 36.777623149 192.168.200.150 192.168.200.100 TCP 60 78 → 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Una volta interpretato il tipo di problema possiamo adottare delle contromisure immediate per evitare un' intrusione all' interno del nostro sistema.

In questo caso una soluzione potrebbe essere impostare il **Firewall** in modo che blocchi l' accesso all' indirizzo IP dell' attaccante ad ogni porta, in modo che ciò che riguarda queste ultime ed i servizi che vi sono in ascolto non siano recuperabili dal potenziale criminale informatico.