



# CYBER SECURITY



# Threat Intelligence

&

## IOC

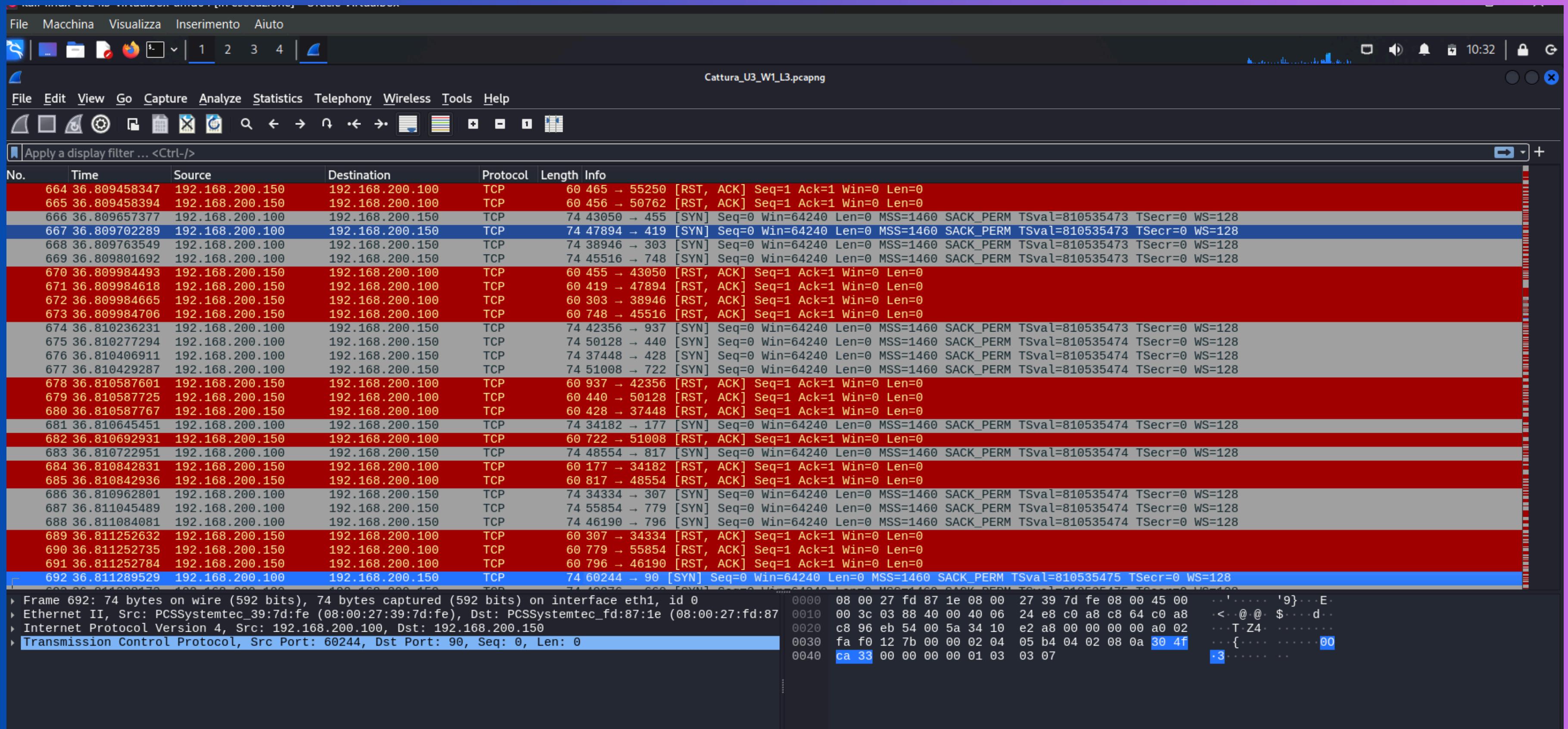


Nel compito di oggi era richiesto di analizzare ed identificare eventuali IOC ,(evidenze di attacchi in corso),nella cattura di rete effettuata su wireshark fornитaci. Da questa base sono andato a fare delle ipotesi sui potenziali vettori di attacco utilizzati e sono andato a dare un mio parere e consiglio su come mitigare l'impatto dell'attacco in corso e prevenire attacchi futuri .

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential ...
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 TStamp=810522427 TSectr=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 TStamp=810522428 TSectr=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 TStamp=4294951165 TSectr=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 TStamp=810522428 TSectr=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 TStamp=810522428 TSectr=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 TStamp=810535437 TSectr=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 TStamp=810535437 TSectr=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 TStamp=810535437 TSectr=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 TStamp=810535438 TSectr=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 TStamp=810535438 TSectr=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 TStamp=810535438 TSectr=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 TStamp=810535438 TSectr=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 TStamp=4294952466 TSectr=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 TStamp=4294952466 TSectr=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 TStamp=810535438 TSectr=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 TStamp=810535438 TSectr=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 TStamp=4294952466 TSectr=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 TStamp=810535438 TSectr=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 TStamp=810535438 TSectr=0 WS=128
30	36.775386941	192.168.200.100	192.168.200.150	TCP	74	55656 → 99 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=810535438 TSectr=0 WS=128

Come si evince dalle slide di wireshark abbiamo molteplici segnalazioni e ripetizioni di pacchetti con il flag (RST,ACK). In un contesto TCP, i pacchetti con i flag RST e ACK indicano la chiusura di una connessione o l'annullamento di una comunicazione. Il flag RST viene utilizzato per forzare la chiusura di una connessione TCP ,quindi questo pacchetto viene inviato da un dispositivo quando desidera annullare immediatamente la connessione , ad esempio per segnalare per l'appunto che la connessione non è riconosciuta o comunque illegale non autorizzata .





## IPOTESI DEI POTENZIALI VETTORI DI ATTACCO

Flag ACK, questo flag viene utilizzato per confermare la ricezione di dati. Se un pacchetto ACK è presente insieme a RST, significa che la parte che invia il pacchetto sta confermando la ricezione del pacchetto precedente mentre contemporaneamente chiude la connessione.

A questo punto ho stilato una serie di possibili attacchi da parte di un attaccante :

- TCP Reset Attack ,in questo caso l'attaccante invia pacchetti RST a entrambe le parti di una connessione TCP, il suo obiettivo è interrompere la comunicazione tra due dispositivi in modo forzato. Questo tipo di attacco può essere utilizzato per interrompere le sessioni legittime tra client e server.

- Man in the Middle (MitM), un attaccante che si trova nel mezzo della comunicazione potrebbe intercettare i pacchetti TCP e inviare un pacchetto RST per chiudere la connessione tra due parti legittime, reindirizzando così il traffico o modificandolo.

- Flooding di pacchetti RST, qui l'attaccante può inondare un server o un dispositivo di pacchetti RST, terminando forzatamente molte connessioni TCP legittime e creando interruzioni di servizio.

# AZIONI PER MITIGARE

A questo punto ho pensato a come poter mitigare questa problematica in corso , la prima cosa a cui ho pensato è stata quella di bloccare l'indirizzo IP interessato, ma pensandoci meglio potrebbe anche essere un dipendente curioso oppure un pc infetto e bloccandolo completamente avrei una perdita di operatività in azienda . La mossa più giusta da seguire in questo caso è quella di limitarne l'operatività cosicché si possa tamponare l'emergenza eseguire un report da far analizzare ad una figura superiore in azienda che se ne andrà ad occupare .

Eseguirei un controllo dei log di sistema , questo mi serve per identificare eventuali attività sospette o errori di connessione.

Dopo aver verificato l'integrità della rete , andrei a rafforzarla tramite le tecniche a noi conosciute come le TLS ( transport layer security) che va a proteggere le comunicazioni sensibili da attacchi MITM ed evita l'entrata di pacchetti maliziosi. Oppure seguire le linee guida aziendali di riferimento a queste criticità.

Matteo Piccinini