

Threat Intelligence & IOC

07/02/2025

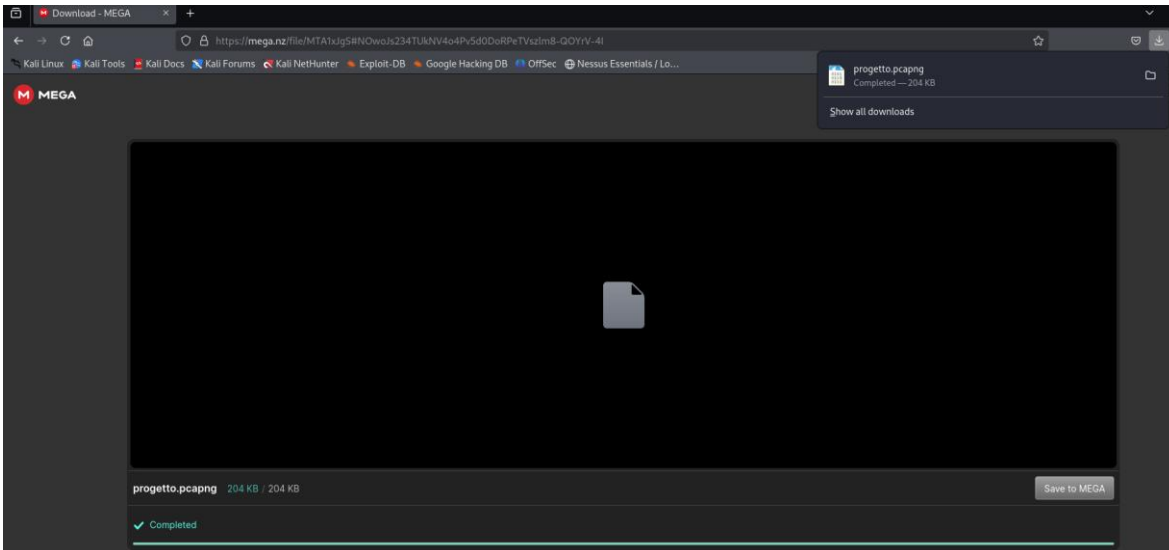
TRACCIA:

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:

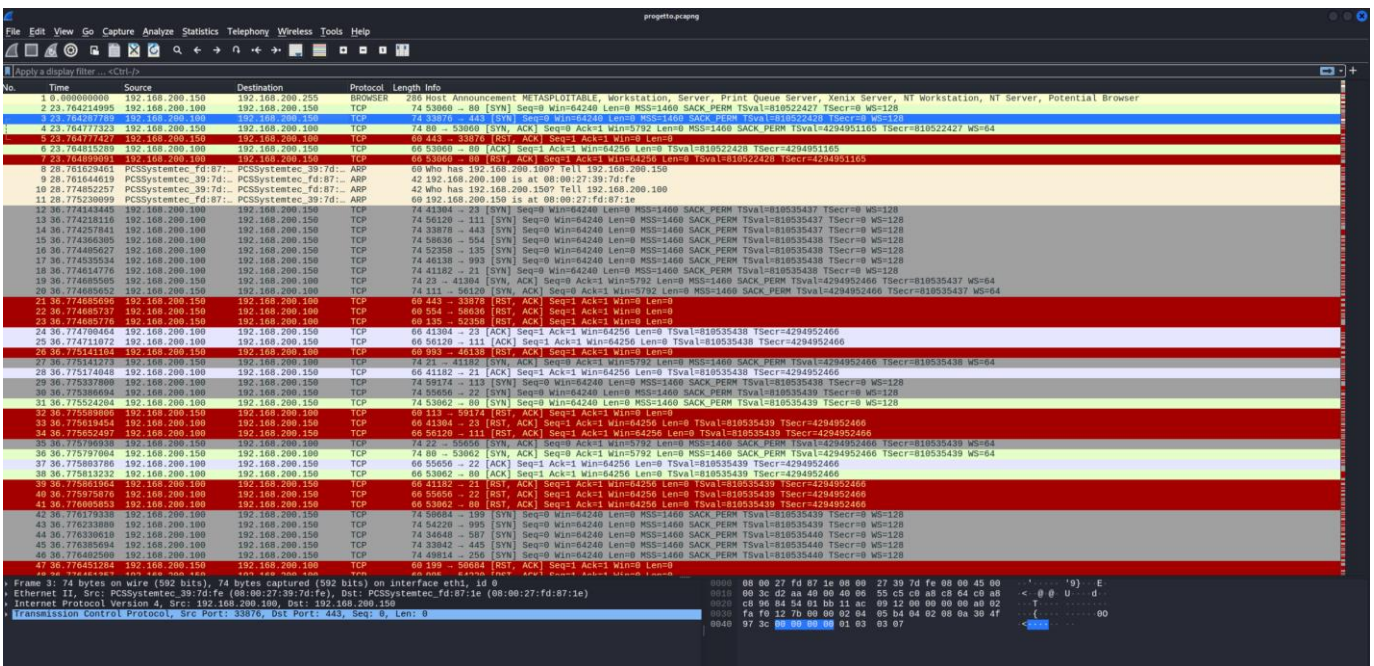
- Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso.
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati.
- Consigliate un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro.

SVOLGIMENTO



Apriamo la nostra macchina kali e scarichiamo il file con la cattura di rete effettuata tramite Wireshark.

Una volta fatto lo apriamo e avremo una schermata di questo tipo:



- Come primo punto dobbiamo identificare ed analizzare eventuali IOC. Gli indicatori IOC.

Gli Indicatori di Compromissione (IOC) sono informazioni che indicano la possibilità di un'attività malevola su una rete o un sistema informatico. Gli IOC possono includere indirizzi IP sospetti, hash di file dannosi, nomi di dominio maligni, firme di virus e altro. Essi vengono utilizzati per rilevare e rispondere rapidamente a incidenti di sicurezza, contribuendo a proteggere sistemi e dati da minacce informatiche.

Per prima cosa notiamo che la comunicazione avviene tra 2 host interni con indirizzo IP di:

- 192.168.200.100
- 192.168.200.150

Nella prima riga vediamo come l'host 192.168.200.150 invia un Host Announcement per informare gli altri dispositivi della sua presenza e dei servizi che offre. In risposta, i dispositivi inviano annunci contenenti i loro nomi, tipi (ad esempio, workstation, server) e altre informazioni.

Gli altri dispositivi usano queste informazioni per aggiornare le loro tabelle di risoluzione dei nomi interne, permettendo loro di comunicare con il nuovo dispositivo tramite nome anziché indirizzo IP.

| Time | Source | Destination | Protocol | Length | Info |
|----------------|-----------------|-----------------|----------|--------|---|
| 1 0.000000000 | 192.168.200.150 | 192.168.200.255 | BROWSER | 280 | Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential Browser |
| 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 | 60 | 53060 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165 |
| 7 23.764839991 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 53060 -> 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165 |

Dalla riga 2 e 3 parte la comunicazione; a farla partire è **192.168.200.100** che manda 2 <syn>; di risposta nella riga 4 e 5 l'altro host risponde con 1 syn-ack e 1 rst-ack.

RST,ACK= Questo flag viene utilizzato per interrompere una connessione TCP. Quando un dispositivo riceve un pacchetto con il flag RST, chiude immediatamente la connessione. Questo può accadere per vari motivi,

come un errore di connessione, un pacchetto non riconosciuto o un tentativo di connessione a un servizio non attivo.

Infine l'host che ha fatto partire la comunicazione chiude l'hand-way shake con un 1 ack e 1 rst,ack.

IOC

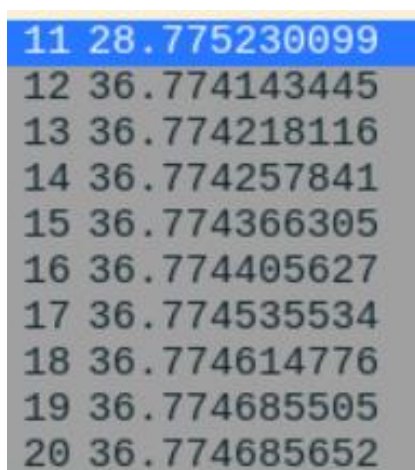
Parto analizzando le prime 40 righe:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|----------------------|----------------------|----------|--------|---|
| 1 | 0.00000000 | 192.168.200.150 | 192.168.200.255 | BROWSER | 286 | Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT S |
| 2 | 23.764214995 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 53660 → 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 → 53660 [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 | 53660 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165 |
| 7 | 23.764899691 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 53660 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 TSval=810522428 TSecr=4294951165 |
| 8 | 28.761628401 | 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 | 36.774366395 | 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 | 36.774495627 | 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 | 36.774685595 | 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=810535438 TSecr=4294952466 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 | 36.774780464 | 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 | 36.775337808 | 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 | 53662 → 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 → 53662 [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 | 53662 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466 |
| 39 | 36.775861904 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 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 |

Già da queste prime catture possiamo notare alcuni possibili Indicatori di Compromissione (IOC):

- **Pacchetti con Flag RST e ACK:** La presenza di pacchetti con flag [RST, ACK] potrebbe indicare tentativi di interruzione delle connessioni, potrebbero far parte di un attacco DoS (Denial of Service) o di una scansione di rete.
- **Host Announcement da "METASPLOITABLE":** L'annuncio dell'host "METASPLOITABLE" è molto indicativo, poiché Metasploitable è una piattaforma comunemente utilizzata per test di vulnerabilità. Questo potrebbe indicare che qualcuno sta eseguendo test di penetrazione sulla rete o che c'è un sistema compromesso.

- **Traffico TCP Sospetto tra 192.168.200.150 e 192.168.200.100:** Le comunicazioni su porte alte, come le porte 33876 e 53060, potrebbero indicare traffico non usuale. Gli attaccanti spesso utilizzano porte non comuni per evitare il rilevamento.
- **Tanti pacchetti SYN** (righe 12-20): La presenza di numerosi pacchetti con il flag SYN può indicare un possibile attacco SYN flood, che è una forma di attacco Denial of Service (DoS). In un attacco SYN flood, l'attaccante invia un alto volume di pacchetti SYN per saturare le risorse del server di destinazione, impedendo così alle connessioni legittime di essere stabilite.
- **Tempi ravvicinati:** I tempi di invio dei pacchetti sono estremamente ravvicinati. Questo potrebbe indicare traffico generato automaticamente o un attacco SYN flood. Potrebbe anche essere una scansione di rete; gli attaccanti possono utilizzare strumenti di scansione automatizzati per esplorare la rete e identificare dispositivi e servizi attivi. Questi strumenti inviano pacchetti in rapida successione per mappare la rete il più velocemente possibile.



A screenshot of a network capture showing a sequence of 9 packets. The first packet (line 11) is highlighted in blue and shows a SYN flag. The subsequent packets (lines 12-20) show a rapid succession of SYN packets with different source ports, indicating a SYN flood attack. The source IP is 36.774... and the destination IP is 192.168.200.100.

| Line | Source IP | Destination IP | Flag |
|------|--------------|-----------------|------|
| 11 | 28.775230099 | 192.168.200.100 | SYN |
| 12 | 36.774143445 | 192.168.200.100 | SYN |
| 13 | 36.774218116 | 192.168.200.100 | SYN |
| 14 | 36.774257841 | 192.168.200.100 | SYN |
| 15 | 36.774366305 | 192.168.200.100 | SYN |
| 16 | 36.774405627 | 192.168.200.100 | SYN |
| 17 | 36.774535534 | 192.168.200.100 | SYN |
| 18 | 36.774614776 | 192.168.200.100 | SYN |
| 19 | 36.774685505 | 192.168.200.100 | SYN |
| 20 | 36.774685652 | 192.168.200.100 | SYN |

Possiamo notare questo trend proseguendo con l'analisi della cattura, notiamo come a molte richieste SYN dell'attaccante, ci sono altrettante RST-ACK della macchina target che interrompono la connessione. Alcuni pacchetti però riescono a passare chiudendo la 3 hand-way shake.

| | | | | | | | | | | | | | | | | | |
|----|--------------|-----------------|-----------------|-----|----|-------|---------|------------|-------|-----------|-----------|----------|-----------------|------------------|------------------|-----------------|-------|
| 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 | TSval=810535439 | TSecr=0 | WS=128 | |
| 43 | 36.776233889 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 54220 | → 995 | [SYN] | Seq=0 | Win=64240 | Len=0 | MSS=1460 | SACK_PERM | 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 | TSval=810535440 | TSecr=0 | WS=128 | |
| 45 | 36.776395694 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 33842 | → 445 | [SYN] | Seq=0 | Win=64240 | Len=0 | MSS=1460 | SACK_PERM | TSval=810535440 | TSecr=0 | WS=128 | |
| 46 | 36.776492500 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 49814 | → 256 | [SYN] | Seq=0 | Win=64240 | Len=0 | MSS=1460 | SACK_PERM | 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 | TSval=810535440 | TSecr=0 | WS=128 | |
| 50 | 36.776496360 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 33200 | → 143 | [SYN] | Seq=0 | Win=64240 | Len=0 | MSS=1460 | SACK_PERM | 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 | TSval=810535440 | TSecr=0 | WS=128 | |
| 52 | 36.776500606 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 49654 | → 110 | [SYN] | Seq=0 | Win=64240 | Len=0 | MSS=1460 | SACK_PERM | 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 | 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 | 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 | TSval=810535440 | TSecr=0 | WS=128 | |
| 57 | 36.776964828 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 445 | → 33842 | [SYN, ACK] | Seq=0 | Ack=1 | Win=5792 | Len=0 | MSS=1460 | SACK_PERM | TSval=4294952466 | TSecr=810535440 | WS=64 |
| 58 | 36.776949222 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 256 | → 49814 | [RST, ACK] | Seq=1 | Ack=1 | Win=0 | Len=0 | | | | | |
| 59 | 36.776949061 | 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 | TSval=4294952466 | TSecr=810535440 | WS=64 |
| 60 | 36.776905004 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 143 | → 33200 | [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 | TSval=4294952466 | TSecr=810535440 | WS=64 |
| 62 | 36.776905082 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 110 | → 49654 | [SYN, ACK] | Seq=0 | 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 | 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 | 33842 | → 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 | | | |

Notiamo come nelle righe: 57, 59, 61 e 63 la macchina target ha risposto con una SYN-ACK, permettendo poi alla macchina attaccante di chiudere la comunicazione tramite 4 ACK (righe 65, 66, 67, 68).

Qui invece possiamo vedere un altro numero elevato di richieste con altrettante interruzioni:

| | | | | | | | | | | | | | | | | |
|-----|--------------|-----------------|-----------------|-----|----|-------|---------|------------|-------|-----------|-------|----------|-----------|-----------------|---------|--------|
| 129 | 36.780149473 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 57552 | → 58 | [SYN] | Seq=0 | Win=64240 | Len=0 | MSS=1460 | SACK_PERM | TSval=810535443 | TSecr=0 | WS=128 |
| 130 | 36.780170333 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 40822 | → 266 | [SYN] | Seq=0 | Win=64240 | Len=0 | MSS=1460 | SACK_PERM | TSval=810535443 | TSecr=0 | WS=128 |
| 131 | 36.780215176 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 42 | → 40522 | [RST, ACK] | Seq=1 | Ack=1 | Win=0 | Len=0 | | | | |
| 132 | 36.780301750 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 58 | → 57552 | [RST, ACK] | Seq=1 | Ack=1 | Win=0 | Len=0 | | | | |
| 133 | 36.780325837 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 37252 | → 11 | [SYN] | Seq=0 | Win=64240 | Len=0 | MSS=1460 | SACK_PERM | TSval=810535444 | TSecr=0 | WS=128 |
| 134 | 36.780346429 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 40648 | → 235 | [SYN] | Seq=0 | Win=64240 | Len=0 | MSS=1460 | SACK_PERM | TSval=810535444 | TSecr=0 | WS=128 |
| 135 | 36.780409818 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 36548 | → 739 | [SYN] | Seq=0 | Win=64240 | Len=0 | MSS=1460 | SACK_PERM | TSval=810535444 | TSecr=0 | WS=128 |
| 136 | 36.780427899 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 38866 | → 55 | [SYN] | Seq=0 | Win=64240 | Len=0 | MSS=1460 | SACK_PERM | TSval=810535444 | TSecr=0 | WS=128 |
| 137 | 36.780472830 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 52136 | → 999 | [SYN] | Seq=0 | Win=64240 | Len=0 | MSS=1460 | SACK_PERM | TSval=810535444 | TSecr=0 | WS=128 |
| 138 | 36.780490897 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 38022 | → 317 | [SYN] | Seq=0 | Win=64240 | Len=0 | MSS=1460 | SACK_PERM | TSval=810535444 | TSecr=0 | WS=128 |
| 139 | 36.780577800 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 266 | → 40822 | [RST, ACK] | Seq=1 | Ack=1 | Win=0 | Len=0 | | | | |
| 140 | 36.780577981 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 11 | → 37252 | [RST, ACK] | Seq=1 | Ack=1 | Win=0 | Len=0 | | | | |
| 141 | 36.780578026 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 235 | → 40648 | [RST, ACK] | Seq=1 | Ack=1 | Win=0 | Len=0 | | | | |
| 142 | 36.780578074 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 739 | → 36548 | [RST, ACK] | Seq=1 | Ack=1 | Win=0 | Len=0 | | | | |
| 143 | 36.780578119 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 55 | → 38866 | [RST, ACK] | Seq=1 | Ack=1 | Win=0 | Len=0 | | | | |
| 144 | 36.780578158 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 999 | → 52136 | [RST, ACK] | Seq=1 | Ack=1 | Win=0 | Len=0 | | | | |
| 145 | 36.780578198 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 317 | → 38022 | [RST, ACK] | Seq=1 | Ack=1 | Win=0 | Len=0 | | | | |

Questo trend prosegue per tutta la cattura.

POTENZIALI VETTORI DI ATTACCO

Identificati gli IOC possiamo passare a ipotizzare quali siano i vettori di attacco utilizzati.

Attacco SYN Flood

- Gli attaccanti inviano un gran numero di pacchetti SYN in rapida successione per saturare le risorse del server, impedendo alle connessioni legittime di essere stabilite. La presenza di numerosi pacchetti SYN e SYN, ACK in rapida successione senza una corrispondente risposta ACK è un forte indicatore di questo tipo di attacco.

Attacco Denial of Service (DoS)

- Attacchi volti a rendere un servizio non disponibile agli utenti legittimi sovraccaricando il server con richieste inutili. La presenza di pacchetti RST, ACK in rapida successione e la saturazione delle risorse di rete sono indicatori di un possibile attacco DoS.

TCP Reset Attack

- In un attacco di tipo TCP Reset Attack l'attaccante invia pacchetti RST falsificati a una o entrambe le estremità di una connessione TCP attiva, costringendola a terminare. L'interruzione improvvisa delle connessioni può causare perdite di dati, interruzione di servizi critici e disservizi per gli utenti.

Host compromesso

- L'host 192.168.200.100 potrebbe essere stato infettato tramite un malware. In questo caso potrebbe essere usato inconsapevolmente dentro una rete di bot (botnet) per attacchi Ddos. Questo tipo di compromissione potrebbe avvenire quando vengono scaricati dei file infetti, cliccando su link presenti in e-mail phishing, o quando il dispositivo non è adeguatamente protetto.

Azioni per ridurre impatto dell'attacco

Per ridurre gli impatti dell'attacco attuale e prevenire attacchi simili in futuro, possiamo adottare diverse soluzioni, quali:

Azioni Immediate

Isolare l'Host Compromesso:

- Isolare l'host 192.168.200.100 dalla rete per evitare che l'attacco si propaghi ulteriormente e per contenere il danno.

Verifica e Pulizia:

- Eseguire una scansione approfondita con software antivirus/antimalware aggiornato.
- Rimuovere eventuali malware individuati.
- Controllare i processi in esecuzione e i file sospetti sull'host compromesso.

Monitoraggio del Traffico di Rete:

- Monitorare attentamente il traffico di rete per individuare attività sospette.
- Utilizzare strumenti di analisi del traffico per identificare ulteriori indicatori di compromissione.

Aggiornamento delle Patch di Sicurezza:

- Aggiornare tutti i sistemi con le ultime patch di sicurezza disponibili per correggere eventuali vulnerabilità note.

Azioni Preventive per il futuro

Implementare SYN Cookies:

- Configura il server per utilizzare SYN cookies, che aiutano a prevenire gli attacchi SYN flood senza consumare risorse eccessive.

Rate Limiting:

- Impostare delle limitazioni di frequenza per il numero di richieste di connessione che il server può accettare in un determinato periodo di tempo.

Utilizzare Firewall e IDS/IPS:

- Configurare firewall per bloccare traffico sospetto e potenzialmente malevolo e implementare sistemi di rilevazione e prevenzione delle intrusioni (IDS/IPS) per monitorare e bloccare attività anomale.

Segmentazione della Rete:

- Dividere la rete in segmenti più piccoli per limitare l'accesso e contenere eventuali attacchi.

Backup Regolari:

- Eseguire backup regolari dei dati critici per garantire che siano recuperabili in caso di compromissione.

Esecuzione di Audit di Sicurezza:

- Periodicamente eseguire audit di sicurezza per valutare la robustezza delle difese della rete.

BONUS

Azienda Mak produce dei macchinari e il cliente vuole mettere in sicurezza tutto l'ecosistema. Abbiamo da una parte l'azienda Mak, poi c'è il macchinario e dall'altra parte c'è il cliente che lo utilizza. Il macchinario è bastato su Windows 10, ha porta di rete (usata solo per gli aggiornamenti e

la diagnostica remota), porta USB (sono disabilitate le pendrive, ovviamente) La diagnostica remota è fatta attraverso la VPN del cliente Il macchinario è sostanzialmente bloccato – La partizione del sistema operativo non è scrivibile mentre c'è una seconda partizione per il software di gestione del macchinario. Il software di gestione è realizzato con il linguaggio C99. Il macchinario è installato nelle varie aziende dei clienti.

TRACCIA

1. Valutare le eventuali vulnerabilità e punti di attacco
2. Proporre al cliente soluzioni di sicurezza
3. Progettare un sistema di monitoraggio del traffico (Windows 10 è bloccato dalla casa madre, non è modificabile)

Proponente al cliente due soluzioni, una economica (massimo 500 euro) e una più costosa (massimo 2500 euro).

VALUTAZIONE DELLE VULNERABILITÀ E PUNTI DI ATTACCO

Sistema Operativo Windows 10

Il sistema operativo Windows 10 può presentare diverse vulnerabilità come:

- **Patch di sicurezza non aggiornate:** Se il sistema operativo non riceve regolarmente aggiornamenti di sicurezza, potrebbe diventare vulnerabile a exploit conosciuti.
- **Driver vulnerabili:** Driver non aggiornati o mal configurati possono essere sfruttati per attacchi.
- **Software di terze parti:** Applicazioni aggiuntive installate sul sistema operativo potrebbero contenere vulnerabilità.

Porta di Rete

La porta di rete del macchinario potrebbe essere un punto di attacco poichè ci potrebbero essere alcune vulnerabilità come:

- **Configurazioni errate:** Configurazioni di rete non sicure potrebbero consentire accessi non autorizzati.
- **Accessi non monitorati:** La porta di rete è usata per aggiornamenti e diagnostica remota, quindi potrebbe essere sfruttata se non adeguatamente monitorata.
- **Possibili exploit:** Vulnerabilità nei protocolli utilizzati per gli aggiornamenti e la diagnostica remota possono essere sfruttate da attaccanti.

Porta USB

Sebbene le pendrive siano disabilite, la porta USB può ancora rappresentare un rischio per:

- **Attacchi fisici:** Altri dispositivi USB potrebbero essere usati per attacchi fisici, come keylogger hardware.

VPN del Cliente

La VPN utilizzata per la diagnostica remota può avere vulnerabilità, eccone alcune:

- **Configurazioni non sicure:** Configurazioni VPN non corrette possono permettere accessi non autorizzati.
- **Gestione inadeguata delle chiavi di sicurezza:** Se le chiavi di sicurezza non sono gestite correttamente, potrebbero essere compromesse, consentendo accessi non autorizzati.
- **Possibili attacchi MITM (Man-In-The-Middle):** Vulnerabilità nella VPN possono esporre i dati a intercettazioni.

Macchinario Bloccato

Anche se il sistema operativo del macchinario è bloccato, ci sono ancora punti di attacco potenziali:

- **Seconda partizione:** La partizione scrivibile per il software di gestione potrebbe essere un punto di attacco se non adeguatamente protetta.

SOLUZIONI DI SICUREZZA

Di seguito riporterò alcune soluzioni di sicurezza che proporrei al cliente:

Aggiornamenti di Sicurezza Regolari

- Assicurarsi che il sistema operativo Windows 10 sia sempre aggiornato con le ultime patch di sicurezza. Questo previene vulnerabilità che potrebbero essere sfruttate da attacchi informatici.

Utilizzo di VPN Sicura

- Garantire che tutte le connessioni remote per la diagnostica vengano effettuate tramite una VPN sicura. Questo assicura che i dati trasmessi siano criptati e protetti da accessi non autorizzati.

Firewall e Controllo del Traffico di Rete

- Implementare un firewall robusto per monitorare e controllare il traffico di rete in entrata e in uscita.

Autenticazione Forte

- Implementare l'autenticazione a due fattori (2FA) per accedere alla diagnostica remota e al software di gestione. Questo garantisce che solo gli utenti autorizzati possano accedere.

Crittografia dei Dati Sensibili

- Cifrare i dati sensibili. Questo aggiunge un ulteriore livello di protezione contro possibili accessi non autorizzati.

Monitoraggio e Logging

- Implementare un sistema di monitoraggio continuo e registrazione dei log per tracciare tutte le attività sul macchinario. Questo aiuta a rilevare tempestivamente eventuali attività sospette.

Isolamento della Rete

- Segmentare la rete per isolare i macchinari da altre parti della rete aziendale. Questo riduce il rischio di propagazione di eventuali minacce informatiche.

Whitelisting delle Applicazioni

- Implementare una politica di whitelisting delle applicazioni per garantire che solo il software approvato possa essere eseguito sul macchinario. Questo previene l'esecuzione di applicazioni non autorizzate o potenzialmente dannose.

Sistemi di Rilevamento delle Intrusioni (IDS)

- Implementare sistemi di rilevamento delle intrusioni (IDS) per monitorare il traffico di rete e rilevare attività sospette o non autorizzate.

Sicurezza Fisica

- Garantire che i macchinari siano fisicamente protetti contro accessi non autorizzati. Questo include l'utilizzo di serrature fisiche e controllo degli accessi ai locali dove i macchinari sono installati.

Analisi delle Vulnerabilità

- Condurre regolarmente analisi delle vulnerabilità per identificare e correggere potenziali punti deboli nel sistema e nel software di gestione.

Backup e Ripristino

- Implementare una strategia di backup regolare e sicuro dei dati. Poi garantire che i backup siano protetti e testare periodicamente il processo di ripristino per assicurarsi che funzioni correttamente.

SISTEMA MONITORAGGIO DI RETE

Soluzione economica (max 500 euro)

Mini PC con Software Open Source

Mini PC (ad esempio, Intel NUC):

- Prezzo: circa **300 euro**.

Software di Monitoraggio Open Source:

- **Wireshark:** gratuito.

Totale Stimato:

- Mini PC (Intel NUC): circa 300 euro
- Software di Monitoraggio Open Source: gratuito

Totale: circa 300 euro

Soluzione più costosa (max 2500 euro)

Acquisto di un'Appliance Dedicata:

Fortinet FortiGate 40F:

- Prezzo attuale: circa **500 euro**.

Software di Monitoraggio Professionale:

SolarWinds Network Performance Monitor:

- Prezzo attuale: circa **1500 euro** per una licenza annuale.

Totale Stimato:

- Fortinet FortiGate 40F: circa **500 euro**
- SolarWinds Network Performance Monitor: **1500 euro**
- Totale: circa **2000 euro**