

Threat Intelligence & IOC

Introduzione:

Il compito di oggi, prevedere attraverso una cattura di **Wireshark** di controllare le richieste ricevute e di risolvere o mitigare il potenziale danno, sul nostro dispositivo con **IP 192.168.200.100**, in comunicazione con l'**IP anomalo 192.168.200.150**.

Attraverso le competenze sviluppate in **Malware Analysis** e **Cyber Threat Intelligence**;

Cos'è Wireshark:

Wireshark è un software open-source per l'analisi del traffico di rete. Permette di catturare e ispezionare i pacchetti di dati che transitano su una rete, decodificando vari protocolli come TCP, HTTP, DNS, e molti altri. È utilizzato principalmente per diagnosticare problemi di rete, analizzare la sicurezza, monitorare il traffico e raccogliere prove in caso di attacchi informatici.

Cos'è la Malware Analysis:

La **Malware Analysis** è il processo di esaminare un software sospetto o dannoso (malware) per comprenderne il funzionamento, l'origine e gli obiettivi. Serve a identificare come il malware si diffonde, quali danni provoca e come mitigarne gli effetti.

Si divide in due approcci principali:

- 1. **Analisi statica**: Studio del codice senza eseguirlo, analizzando file, firme e comportamenti potenziali.
- 2. **Analisi dinamica**: Esecuzione del malware in un ambiente controllato (sandbox) per osservarne direttamente le azioni.

Cos'è la Cyber Threat Intelligence:

La Threat Intelligence è la raccolta, analisi e condivisione di informazioni su minacce attuali e potenziali alla sicurezza informatica. Queste informazioni provengono da diverse fonti e includono dettagli sui cyber attacchi, sulle vulnerabilità dei sistemi, sulle tattiche e sugli indicatori di compromissione (IoC). Tutto ciò serve per comprendere, prevenire e rispondere a potenziali minacce;

Policy di Sicurezza:

Le **policy** sono **linee guida** in materia di sicurezza seguite all'interno di un'azienda, è compito del **responsabile** della sicurezza **stabilire queste regole**, in accordo con i valori e gli obiettivi aziendali, e convincere il management a implementarle, affrontando i relativi costi. Seguendo **le principali tipi di policy**:

- Policy Amministrative;
- Piani di Disaster Recovery;
- Policy dei Dati (chi può accedere a cosa):
- Policy di Sicurezza;
- Requisiti del Software:
- Policy di Utilizzo:
- Policy di Gestione degli Utenti:

Pratica:

Da questa prima cattura notiamo come l'IP sospetto provi a mandare molte **richieste TCP**, che come sappiamo per essere completato ha bisogno del **3-way handshake**, ma in questo caso l'IP sospetto manda solo una richiesta **SYN** senza rispondere con l'**ACK** una volta ricevuto il **SYN/ACK** dal mio dispositivo, da questa cosa possiamo dedurre 2 cose:

- 1. **Scansione porte**: l'attaccante scansione le porte, per trovare un punto di accesso per il nostro dispositivo;
- 2. Denial of service (DOS): interruzione di un determinato servizio;

2 23.764214995 192.168.200.100 192.168.200.150 TCP 74 53006 98 [57N] Seq=0 Wins04240 Len=0 MSS=1460 SACK_PERM TSVal=016522427 TSecr=0 WS=128 4 23.764777323 192.168.200.150 192.168.200.100 TCP 74 80 = 53060 [57N, ACK] Seq=0 Ack=1 Wins5192 Len=0 MSS=1460 SACK_PERM TSVal=016522427 MS=64 5 23.764877427 192.168.200.100 192.168.200.100 TCP 60 434 = 33876 [Ack] Wins5192 Len=0 MSS=1460 SACK_PERM TSVal=016522427 MS=64 5 23.7648717427 192.168.200.100 TCP 60 434 = 33876 [Ack] Wins5192 Len=0 MSS=1460 SACK_PERM TSVal=016522427 MS=64 6 23.764815280 192.168.200.100 192.168.200.150 TCP 66 53060 = 80 [ACK] Seq=1 Ack=1 Wins6256 Len=0 TSVal=016522428 TSecr=4294951165 TSecr=016522427 WS=64 6 23.764815280 192.168.200.100 TCP 60 53000 = 80 [ACK] Seq=1 Ack=1 Wins6256 Len=0 TSVal=016522428 TSecr=4294951105 TSecr=01652427 WS=64 6 23.764815280 PSSystemate_G.39.761 ARP 92.7648.200.100 TCP 60 53000 = 80 [ACK] Seq=1 Ack=1 Wins6256 Len=0 TSVal=016522428 TSecr=4294951105 TSecr=0.000 TSPAL=01652427 WS=64 6 23.764815280 PSSystemate_G.39.761 ARP 92.7648.200.100 TCP 60 93000 = 80 [ACK] Seq=1 Ack=1 Wins6256 Len=0 TSVal=016522428 TSecr=4294951105 TSecr=0.000 TSPAL=01652428 TSecr=4294951105 TSecr=0.000 TSPAL=01652428 TSecr=4294951105 TSecr=0.000 TSPAL=01652428 TSecr=4294951105 TSecr=0.000 TSPAL=01652428 TSecr=4294951105 TSPAL=01652428 TSPA	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
4 23.764777327 192.168.209.150 192.168.209.109 TCP 74 80 - 53000 [SYN, ACK] Seq=0 Ack=1 Win=5*P92 Len=0 MSS=1400 SACK PERM TSVal=4294951105 TSecr=810522427 WS=64 5 23.764815289 192.168.209.100 192.168.209.150 TCP 66 53060 - 80 [ACK] Seq=1 Ack=1 Win=04250 Len=0 TSVal=810522428 TSecr=4294951105 TCP 72 37.764815289 192.168.209.100 192.168.209.150 TCP 66 53060 - 80 [RS1, ACK] Seq=1 Ack=1 Win=04250 Len=0 TSVal=810522428 TSecr=4294951105 TCP 66 53060 - 80 [RS1, ACK] Seq=1 Ack=1 Win=04250 Len=0 TSVal=810522428 TSecr=4294951105 TCP 72 37.76481528 TSecr=0.39:7d: PCSSystemtec_0.39:7d: PCSSystemtec	2 23.764214995	192.168.200.100	192.168.200.150	TCP	
5 23.764777427 192.168.209.150 192.168.209.150 192.168.209.150 TCP 65 53306 8.0K) Segri Ackil Wins-04256 Lens-0 TSval=810522428 Tsecr=4294951165 7 23.764899991 192.168.209.100 192.168.209.150 TCP 65 53306 8.0K) Segri Ackil Wins-04256 Lens-0 TSval=810522428 Tsecr=4294951165 9 28.761644619 PCSSystemtec_03:7d:. PCSSystemtec_61:87:. APB 92.8761644619 PCSSystemtec_03:7d:. PCSSystemtec_07:7d:. APB 92.8761644619 PCSSystemtec_03:7d:. PCSSystemtec_07:7d:. APB 92.8776320909 PCSSystemtec_07:7d:. PCSSystemtec_07:7d:. APB 92.168.200.150 Inc. PCSSystemtec_07:7d:. APB 92.168.200.150 Inc. PCSSystemtec_07:7d:. APB 96.192.168.200.150 I	3 23.764287789	192.168.200.100	192.168.200.150		
6 23.764815289 192.168.209.100 192.168.209.150 TCP 66 5380980 [RST, AKK] SeqT AKK=1 Win=64256 Len=0 TSVal=810522428 TSecr=4294951165 8 28.761629461 PCSSystemtec di 87: PCSSystemtec gi 87: ARP 92 8.761644619 PCSSystemtec gi 87: ARP 19 28.761644619 PCSSystemtec gi 87: ARP 19 28.76164619 PCSSystemtec gi 87: ARP 19 28.76167619 PCSSystemtec gi 88: ARP 19 28:			192.168.200.100		
7 23.764899991 192.168.209.199 192.168.209.199 1CP 66 97. MRX Seq 1.4 MRX 1.0 1.0 1.0 1.0 1.0 1.0 1.0 1.0 1.0 1.0					
8 28.761629461 PCSSystemtec fd:87: PCSSystemtec 3:7d: PCSSystemtec 3:7d: ARP 98.76168.209.109 Tell 192.168.209.109 19					
9 28. 761644619 PCSSystemtec_39:7di					
182.8774852257 PCSSystemtec_39:7di PCSSystemtec_fd:87: CSSystemtec_fd:87: ARP 69 12.88.729099 PCSSystemtec_fd:87: PCSSystemtec_fd:87: ARP 69 12.168.209.159 is at 08:00:27:fd:87: aRP 69 12.168.209.109					60 Who has 192.168.200.100? Tell 192.168.200.150
11 28.775230099 PCSSystemtec_fd:87: PCSSystemtec_39:7d:_ARP					
12 36.774143445 192.168.200.100 192.168.200.150 TCP 74 41304 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535437 TSecr=0 WS=128 13 6.774257841 192.168.200.100 192.168.200.150 TCP 74 55120 - 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535437 TSecr=0 WS=128 15 36.774365305 192.168.200.100 192.168.200.150 TCP 74 53878 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535437 TSecr=0 WS=128 16 36.774465507 192.168.200.100 192.168.200.150 TCP 74 52356 - 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 52356 - 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535438 TSecr=0 WS=128 17 36.774685505 192.168.200.100 192.168.200.100 TCP 74 46138 - 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535438 TSecr=0 WS=128 17 36.774685505 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 17 36.774685505 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 17 36.774685505 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 17 36.774685505 192.168.200.150 TCP 74 46138 - 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535438 TSecr=8 WS=128 17 36.774685505 192.168.200.150 TCP 74 23 - 41304 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535437 WS=64 192.168.200.150 TCP 74 23 - 41304 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535437 WS=64 192.168.200.150 TCP 60 554 - 58036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 192.168.200.150 TCP 60 543 - 58036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 192.168.200.150 TCP 60 41380 - 22 [ACK] Seq=1 Ack=1 Win=0 Len=0 192.168.200.150 TCP 60 54182 - 21 [ACK] Seq=1 Ack=1 Win=0 Len=0 192.168.200.150 TCP 60 41380 - 22 [ACK] Seq=1 Ack=1 Win=0 Len=0 192.168.200.150 TCP 74 5505 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535438 TSecr=805354	10 28.774852257	PCSSystemtec_39:7d:	. PCSSystemtec_fd:87:	ARP	42 Who has 192.168.200.150? Tell 192.168.200.100
13 6.774218116 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 15 36.774356345 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 36.774405637 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 17 36.774535534 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 18 36.774614776 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 19 36.774685555 192.168.200.100 192.168.200.100 TCP 74 4118 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535438 TSecr=0 WS=128 19 36.774685555 192.168.200.150 192.168.200.100 TCP 74 4118 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535438 TSecr=0 WS=128 19 36.774685565 192.168.200.150 192.168.200.100 TCP 74 4118 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535438 TSecr=0 WS=128 19 36.774685656 192.168.200.150 192.168.200.100 TCP 74 4118 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535438 TSecr=0 WS=128 19 36.774685767 192.168.200.150 192.168.200.100 TCP 60 943 - 33678 [RST, ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSVal=4294952466 TSecr=810535437 WS=64 192.168.200.150 192.168.200.150 TCP 60 943 - 33678 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 192.168.200.150 192.168.200.150 TCP 60 943 - 54636 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSVal=810535438 TSecr=4294952466 TSecr=810535438 WS=64 192.168.200.150 192.168.200.150 TCP 66 41304 - 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSVal=810535438 TSecr=4294952466 TSecr=810535438 WS=64 192.168.200.150 192.168.200.150 TCP 66 41304 - 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSVal=810535438 TSecr=4294952466 TSecr=810535438 WS=64 192.168.200.150 192.168.200.150 TCP 66 41304 - 23 [ACK] Seq=1 Ack=1 Win=64256			PCSSystemtec_39:7d:	ARP	
14 36.774257841 192.168.200.100 192.168.200.150 TCP 74 38878 - 443 \$\text{SYN}\$ \text{Seq=0}\$ \text{win=64240}\$ \text{Len=0}\$ \text{MSS=1460}\$ \text{SACK}\$ \text{PERM}\$ \text{TSVal=810535438}\$ \text{TSecr=0}\$ \text{wS=128}\$ \text{15} 36.774366305 192.168.200.100 192.168.200.150 TCP 74 \$6836 - 554 \$\text{SYN}\$ \text{Seq=0}\$ \text{win=64240}\$ \text{Len=0}\$ \text{MSS=1460}\$ \text{SACK}\$ \text{PERM}\$ \text{TSVal=810535438}\$ \text{TSecr=0}\$ \text{wS=128}\$ \text{17} 36.774535534 192.168.200.100 192.168.200.150 TCP 74 \$46138 - 993 \$\text{SYN}\$ \text{Seq=0}\$ \text{win=64240}\$ \text{Len=0}\$ \text{MSS=1460}\$ \text{SACK}\$ \text{PERM}\$ \text{TSVal=810535438}\$ \text{TSecr=0}\$ \text{wS=128}\$ \text{18} 36.774685555 192.168.200.100 192.168.200.100 TCP 74 \$41182 - 21 \$\text{SYN}\$ \text{Seq=0}\$ \text{win=64240}\$ \text{Len=0}\$ \text{MSS=1460}\$ \text{SACK}\$ \text{PERM}\$ \text{TSVal=810535438}\$ \text{TSecr=0}\$ \text{wS=128}\$ \text{19} 36.774685555 192.168.200.150 192.168.200.100 TCP 74 \$41182 - 21 \$\text{SYN}\$ \text{Seq=0}\$ \text{Ack=1}\$ \text{win=5792}\$ \text{Len=0}\$ \text{MSS=1460}\$ \text{SACK}\$ \text{PERM}\$ \text{TSVal=810535437}\$ \text{wS=64}\$ \text{23} \text{.41304}\$ \text{SYN}\$ \text{Seq=0}\$ \text{Ack=1}\$ \text{win=5792}\$ \text{Len=0}\$ \text{MSS=1460}\$ \text{SACK}\$ \text{PERM}\$ \text{TSVal=810535437}\$ \text{WS=64}\$ \text{23} \text{.41304}\$ \text{Len=0}\$ \text{MSS=1460}\$ \text{SACK}\$ \text{PERM}\$ \text{TSVal=810535438}\$ \text{TSecr=0}\$ \text{wS=128}\$ \text{17} \text{36} \text{.74685565}\$ \text{192.168.200.150}\$ \text{192.168.200.100}\$ \text{TCP}\$ \text{74} \text{4113} \text{.56128}\$ \text{SYN}\$ \text{Seq=0}\$ \text{Ack=1}\$ \text{win=5792}\$ \text{Len=0}\$ \text{MSS=1460}\$ \text{SACK}\$ \text{PERM}\$ \text{TSVal=810535437}\$ \text{WS=64}\$ \text{23} \text{.41304}\$ \text{Len=0}\$ \text{MSS=1460}\$ \text{SACK}\$ \text{PERM}\$ \text{TSVal=810535437}\$ \text{WS=64}\$ \text{23} \text{.41304}\$ \text{Len=0}\$ \text{MS=1460}\$ \text{SACK}\$ \text{PERM}\$ \text{TSVal=810535437}\$ \text{WS=64}\$ \text{23} \text{.41304}\$ \text{Len=0}\$ \text{MS=1460}\$	12 36.774143445	192.168.200.100	192.168.200.150	TCP	
15 63.774366365 192.168.200.100 192.168.200.150 TCP 74 58636 - 554 \$\begin{array}{c} \text{SYN} \end{array} \text{Seq=0 Min=64240 Len=0 MSS=1460 SACK_PERN TSVal=810535438 TSecr=0 MS=128 TCP 74 52358 - 135 \$\text{SYN} \end{array} \text{Seq=0 Min=64240 Len=0 MSS=1460 SACK_PERN TSVal=810535438 TSecr=0 MS=128 TCP 74 46138 - 993 \$\text{SYN} \end{array} \text{Seq=0 Min=64240 Len=0 MSS=1460 SACK_PERN TSVal=810535438 TSecr=0 MS=128 TCP 74 46138 - 993 \$\text{SYN} \end{array} \text{Seq=0 Min=64240 Len=0 MSS=1460 SACK_PERN TSVal=810535438 TSecr=0 MS=128 TCP 74 46138 - 993 \$\text{SYN} \end{array} \text{Seq=0 Min=64240 Len=0 MSS=1460 SACK_PERN TSVal=810535438 TSecr=0 MS=128 TCP 74 46138 - 993 \$\text{SYN} \end{array} \text{Seq=0 Min=64240 Len=0 MSS=1460 SACK_PERN TSVal=810535438 TSecr=0 MS=128 TCP 74 41182 - 21 \$\text{SYN} \end{array} \text{Seq=0 MCS=1460 SACK_PERN TSVal=810535438 TSecr=0 MS=128 TCP 74 111 - 50120 \$\text{SYN} \end{array} \text{ACK} \end{array} \text{Seq=0 Ack=1 Min=5792 Len=0 MSS=1460 SACK_PERN TSVal=829452466 TSecr=810535437 WS=64 23 36.774685769 \$\text{192.168.200.150} \text{192.168.200.150} \text{192.168.200.190} \text{TCP} \text{60 554 } 58036 [RST, ACK] Seq=1 Ack=1 Min=5 Len=0 Seq=0 Ack=1 Min=5 Le	13 36.774218116	192.168.200.100	192.168.200.150		
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 18 36.77461876 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 36.774685552 192.168.200.150 192.168.200.150 TCP 74 41182 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535438 TSecr=0 WS=128 19 36.774685555 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 21 36.774685573 192.168.200.150 192.168.200.100 TCP 60 443 - 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 MSS=1460 SACK_PERM TSVal=4294952466 TSecr=810535437 WS=64 22 36.774685737 192.168.200.150 192.168.200.100 TCP 60 443 - 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 MSS=1460 SACK_PERM TSVal=4294952466 TSecr=810535437 WS=64 22 36.774685737 192.168.200.150 192.168.200.100 TCP 60 135 - 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 MSS=1460 SACK_PERM TSVal=8494952466 MS=1408.800 MS=1408.8	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
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 36.774685505 192.168.200.150 192.168.200.150 TCP 74 11304 [SYN] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64 20 36.774685605 192.168.200.150 192.168.200.100 TCP 74 111 - 56120 [SYN] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64 1136.774685606 192.168.200.150 192.168.200.100 TCP 74 111 - 56120 [SYN] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64 12 36.774685696 192.168.200.150 192.168.200.100 TCP 60 554 - 58036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 S36.77468576 192.168.200.150 192.168.200.100 TCP 60 135 - 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 S36.774608576 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [ACK] Seq=1 Ack=1 Win=0 Len=0 S40.77460464 192.168.200.100 192.168.200.150 TCP 66 541304 - 23 [ACK] Seq=1 Ack=1 Win=0 Len=0 S5438 TSecr=4294952466 S56.774711072 192.168.200.150 TCP 66 541304 - 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466 S56.7751441273 192.168.200.150 TCP 66 541304 - 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466 TSecr=810535438 WS=64 188	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
18 36.774614776 192.168.200.100 192.168.200.150 TCP 74 41182 - 21 [\$YN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535438 TSecr=0 WS=128 19 36.774685555 192.168.200.150 192.168.200.100 TCP 74 111 - 56120 [\$YN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSVal=4294952466 TSecr=810535437 WS=64 21 36.774685565 192.168.200.150 192.168.200.100 TCP 74 111 - 56120 [\$YN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSVal=4294952466 TSecr=810535437 WS=64 21 36.774685769 192.168.200.150 192.168.200.100 TCP 60 443 - 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 192.168.200.150 192.168.200.150 TCP 60 135 - 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 192.168.200.150 TCP 60 135 - 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 192.168.200.150 TCP 64 1304 - 23 [ACK] Seq=1 Ack=1 Win=0 Len=0 TSVal=810535438 TSecr=4294952466 192.168.200.150 TCP 65 56120 - 111 [ACK] Seq=1 Ack=1 Win=0 Len=0 TSVal=810535438 TSecr=4294952466 192.168.200.150 TCP 65 56120 - 111 [ACK] Seq=1 Ack=1 Win=0 Len=0 TSVal=810535438 TSecr=4294952466 192.168.200.150 TCP 69 93 - 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 TSVal=810535438 TSecr=4294952466 192.168.200.150 TCP 69 93 - 46138 [RST, ACK] Seq=1 Ack=1 Win=5 Len=0 TSVal=810535438 TSecr=4294952466 TSecr=810535438 WS=64 192.168.200.150 TCP 60 41182 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSVal=810535438 TSecr=4294952466 TSecr=810535438 WS=64 192.168.200.150 TCP 66 41804 - 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSVal=810535438 TSecr=4294952466 TSecr=810535438 WS=64 192.168.200.150 TCP 74 51566 - 22 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 SACK_PERM TSVal=810535439 TSecr=0 WS=128 13 63.775524204 192.168.200.100 192.168.200.150 TCP 74 55066 - 22 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 SACK_PERM TSVal=810535439 TSecr=0 WS=128 13 63.7755288090 192.168.200.100 192.168.200.150 TCP 74 55066 - 22 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 SACK_PERM TSVal=810535439 TSecr=0 WS=128 13 63.775528980 192.168.200.100 192.168.200.150 TCP 74 55066 - 22 [SYN] Seq=0 Win=64240 Len=0 TSVal=810535439 TSecr=4294952466 TSecr=810535439 TSecr=4294	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
19 36.774685565 192.168.200.150 192.168.200.100 TCP 74 23 - 41304 [SVM, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSVal=4294952466 Tsecr=810535437 WS=64 21 36.774685565 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 22 36.774685569 192.168.200.150 192.168.200.100 TCP 00 443 - 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 23 36.774685770 192.168.200.150 192.168.200.100 TCP 05 54 - 58036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 23 36.774768576 192.168.200.150 TCP 06 135 - 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 25 36.774706464 192.168.200.100 192.168.200.150 TCP 06 135 - 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 TsVal=810535438 Tsecr=4294952466 TSecr=4294952466 192.168.200.100 TCP 06 56 56120 - 111 [ACK] Seq=1 Ack=1 Win=0 Len=0 TsVal=810535438 Tsecr=4294952466 192.168.200.150 TCP 06 993 - 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 TSVal=810535438 Tsecr=4294952466 192.168.200.150 TCP 06 993 - 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 TSVal=810535438 Tsecr=4294952466 192.168.200.150 TCP 06 993 - 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 TSVal=810535438 Tsecr=4294952466 TSecr=810535438 WS=64 192.168.200.150 TCP 06 41182 [SVN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSVal=4294952466 TSecr=810535438 WS=64 192.168.200.150 TCP 07 42 1 - 4182 [SVN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSVal=810535438 TSecr=4294952466 192.168.200.150 TCP 07 455565 - 22 [SVN] Seq=0 Win=64240 Len=0 WSS=1460 SACK_PERM TSVal=810535439 TSecr=0 WS=128 13.6.775524204 192.168.200.100 192.168.200.150 TCP 07 455656 - 22 [SVN] Seq=0 Win=64240 Len=0 WSS=1460 SACK_PERM TSVal=810535439 TSecr=0 WS=128 13.6.775528980 192.168.200.100 192.168.200.150 TCP 07 453062 - 80 [SVN] Seq=0 Win=64240 Len=0 WSS=1460 SACK_PERM TSVal=810535439 TSecr=0 WS=128 13.6.775528980 192.168.200.100 192.168.200.150 TCP 07 453062 - 80 [SVN] Seq=0 Win=64240 Len=0 WSS=1460 SACK_PERM TSVal=810535439 TSecr=0 WS=128 13.6.775528980 192.168.200.100 192.168.200.150 TCP 06	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
20 36.774685552 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 60 434 - 3878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 23 36.77468576 192.168.200.150 192.168.200.100 TCP 60 554 - 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 24 36.774700464 192.168.200.100 192.168.200.100 TCP 60 135 - 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 25 36.774711072 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 36.7751411073 192.168.200.150 TCP 66 56120 - 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSVal=810535438 TSecr=4294952466 27 36.7751411273 192.168.200.150 192.168.200.150 TCP 60 993 - 46138 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSVal=810535438 TSecr=4294952466 27 36.775141273 192.168.200.150 192.168.200.150 TCP 66 41182 [SYN, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSVal=810535438 TSecr=4294952466 TSecr=810535438 WS=64 28 36.7755387800 192.168.200.100 192.168.200.150 TCP 66 41182 [SYN, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSVal=810535438 TSecr=4294952466 TSecr=810535438 WS=64 28 36.775588694 192.168.200.100 192.168.200.150 TCP 74 55356 - 22 [SYN] Seq=0 Win=64240 Len=0 WS=1460 SACK_PERM TSVal=810535439 TSecr=0 WS=128 31 36.775589806 192.168.200.100 192.168.200.150 TCP 74 55366 - 22 [SYN] Seq=0 Win=64240 Len=0 WS=1460 SACK_PERM TSVal=810535439 TSecr=0 WS=128 32 36.775589806 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=6 Len=0 TSVal=810535439 TSecr=4294952466 TCP 74 55366 - 22 [SYN] Seq=0 Win=64240 Len=0 WS=1460 SACK_PERM TSVal=810535439 TSecr=0 WS=128 33 36.775598806 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=6 Len=0 TSVal=810535439 TSecr=4294952466 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=6 Len=0 TSVal=810535439 TSecr=4294952466 TSecr=810535439 TSecr=4294952466 TSecr=810535439 TSecr=4294952466 TSecr=810535439 TSecr=4294952466 TSecr=810535439 TSecr=4294952466 TSecr=810	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
21 36.774685737 192.168.209.159 192.168.209.109 TCP 69 443 - 33878 [RST, ACK] Seq=1 Ack=1 Win=9 Len=9 23 36.774685737 192.168.209.159 192.168.209.109 TCP 60 554 - 58036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 23 36.774708464 192.168.209.150 192.168.209.100 TCP 66 4304 - 23 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 25 36.7747101072 192.168.209.100 192.168.209.150 TCP 66 4304 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466 26 36.775141104 192.168.209.150 192.168.209.100 TCP 69 993 - 46138 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466 27 36.775141104 192.168.209.150 192.168.209.100 TCP 69 993 - 46138 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466 28 36.775174048 192.168.209.150 192.168.200.150 TCP 66 4182 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466 TSecr=810535438 WS=64 28 36.775174048 192.168.209.100 192.168.200.150 TCP 66 4182 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466 29 36.775378800 192.168.200.100 192.168.200.150 TCP 74 55056 - 22 [SVN] Seq=0 Win=64240 Len=0 WSS=1460 SACK_PERM TSVal=810535438 TSecr=0 WS=128 31 36.775524204 192.168.200.100 192.168.200.150 TCP 74 55056 - 22 [SVN] Seq=0 Win=64240 Len=0 WSS=1460 SACK_PERM TSVal=810535439 TSecr=0 WS=128 32 36.775588096 192.168.200.100 192.168.200.150 TCP 74 53062 - 80 [SVN] Seq=0 Win=64240 Len=0 WSS=1460 SACK_PERM TSVal=810535439 TSecr=0 WS=128 32 36.775588096 192.168.200.100 192.168.200.150 TCP 74 53062 - 80 [SVN] Seq=0 Win=64240 Len=0 WSS=1460 SACK_PERM TSVal=810535439 TSecr=0 WS=128 32 36.775580986 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 33 36.775508980 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 33 36.775508980 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 33 36.775508980 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 33 36.775508980 192.168.200.100 192.168.200.150 TCP 66 41304	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
22 36.774685776 192.168.200.150 192.168.200.100 TCP 60 554 - 58036 [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 36.775141072 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 36.775141273 192.168.200.150 192.168.200.150 TCP 69 93 - 46138 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535438 TSecr=4294952466 TSecr=810535438 WS=64 28 36.77514273 192.168.200.150 192.168.200.150 TCP 66 41182 [STM, ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64 28 36.77537800 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 TSecr=810535438 WS=64 28 36.775386694 192.168.200.100 192.168.200.150 TCP 74 55056 - 22 [STM] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128 31 36.775589806 192.168.200.150 192.168.200.150 TCP 74 55056 - 22 [STM] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128 32 36.775589806 192.168.200.150 192.168.200.150 TCP 74 55056 - 22 [STM] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128 33 36.775598806 192.168.200.150 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 32 36.775598806 192.168.200.150 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 32 36.7755189806 192.168.200.150 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 TSval=810535439 TSecr=4294952466	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
23 36.774685776 192.168.200.150 192.168.200.150 TCP 66 135 - \$2358 \text{RST}, ACK\forall Seq=1 Ack=1 Win=6 Len=0 \text{Len=0 TSval=810535438 TSecr=4294952466} \text{23 6c.77471072 192.168.200.150 192.168.200.150 TCP 66 41304 - 23 \text{Len=0 TSval=810535438 TSecr=4294952466} \text{25 6c.774711072 192.168.200.150 192.168.200.150 TCP 66 56120 - 111 \text{LCK} Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466} \text{26 Cen=0 TSval=810535438 TSecr=4294952466} \text{27 3 6c.775174104 192.168.200.150 192.168.200.150 TCP 69 93 - 46138 \text{RST}, ACK\forall Seq=1 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64 182 - 21 \text{LCK} Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466} 18 2 erg a decention of the secretary of the	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
24 36.774704644 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 36.775144104 192.168.200.150 192.168.200.100 TCP 60 993 - 46138 [RST, ACK] Seq=1 Ack=1 Win=54256 Len=0 TSval=810535438 TSecr=4294952466 TSecr=810535438 WS=64 28 36.775174048 192.168.200.100 192.168.200.150 TCP 66 4182 - 21 [ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64 29 36.77537800 192.168.200.100 192.168.200.150 TCP 66 4182 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=294952466 29 36.775386694 192.168.200.100 192.168.200.150 TCP 74 59174 - 113 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128 31 36.775584204 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 31 36.7755989806 192.168.200.150 192.168.200.150 TCP 74 53062 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128 33 36.7755989806 192.168.200.150 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466	22 36.774685737	192.168.200.150	192.168.200.100	TCP	68 554 - 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25 36.774711072 192.168.209.169 192.168.209.150 TCP 65 56120 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466 27 36.775141104 192.168.209.150 192.168.209.160 TCP 69 993 46138 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466 TSecr=810535438 WS=64 28 36.775174048 192.168.209.160 192.168.209.150 TCP 66 41182 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466 TSecr=810535438 WS=64 28 36.77537800 192.168.209.100 192.168.209.150 TCP 66 41182 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466 TSecr=810535438 WS=64 39 36.7753800 192.168.209.100 192.168.209.150 TCP 74 59174 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128 31 36.775589806 192.168.209.100 192.168.209.150 TCP 74 59174 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128 31 36.775589806 192.168.209.150 192.168.209.150 TCP 74 59174 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466 32 36.775589806 192.168.200.150 192.168.200.150 TCP 66 41304 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466	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
20 36.775141104 192.168.209.159 192.168.209.109 TCP 69 993 - 46138 [RST, ACK] Seq=1 Ack=1 Win=5 Len=0 MSS=1460 SACK_PERM TSVal=4294952466 TSecr=810535438 WS=64 275174048 192.168.209.150 192.168.209.150 TCP 64 1182 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSVal=810535438 TSecr=4294952466 TSecr=810535438 WS=64 28 36.775337809 192.168.209.150 TCP 64 1182 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSVal=810535438 TSecr=4294952466 TSecr=810535438 WS=64 28 36.775337809 192.168.209.150 TCP 74 59174 - 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535439 TSecr=0 WS=128 31 36.775524294 192.168.209.100 192.168.209.150 TCP 74 53062 - 89 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535439 TSecr=0 WS=128 32 36.7755089800 192.168.209.150 TCP 74 53062 - 89 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535439 TSecr=0 WS=128 13 36.7755089800 192.168.209.100 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=6 Len=0 TSVal=810535439 TSecr=4294952466	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
27 36.775141273 192.168.200.150 192.168.200.150 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 192.168.200.160 192.168.200.150 TCP 66 41182 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 Tsecr=24994952466 Tsecr=810535438 WS=64 192.168.200.160 192.168.200.150 TCP 66 41182 - 21 [ACK] Seq=0 Min=64256 Len=0 TSval=810535438 Tsecr=0 WS=128 192.168.200.150 TCP 74 55056 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 Tsecr=0 WS=128 192.168.200.150 TCP 74 53062 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 Tsecr=0 WS=128 192.168.200.150 TCP 74 53062 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 Tsecr=0 WS=128 192.168.200.150 TCP 74 53062 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 Tsecr=0 WS=128 192.168.200.150 TCP 74 53062 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 Tsecr=0 WS=128 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 Tsval=810535439 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
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 36.77537806 192.168.200.100 192.168.200.150 TCP 74 55056 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1406 SACK_PERM TSVal=810535438 TSecr=0 WS=128 31 36.7755284204 192.168.200.100 192.168.200.150 TCP 74 55056 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1406 SACK_PERM TSVal=810535439 TSecr=0 WS=128 31 36.775598806 192.168.200.100 192.168.200.150 TCP 74 53062 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1406 SACK_PERM TSVal=810535439 TSecr=0 WS=128 32 36.775598806 192.168.200.150 192.168.200.100 TCP 60 113 - 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 33 36.775519454 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	26 36.775141194	192.168.200.150	192.168.200.100	TCP	60 993 - 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29 36.775337880 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 36.775524204 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 36.775598806 192.168.200.150 192.168.200.150 TCP 66 113 - 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	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
30 36.7755886694 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 36.775589806 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 TCP 60 113 - 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 TSval=810535439 TSecr=4294952466	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
31 36.775524204 192.168.209.109 192.168.209.159 TCP 74.53062 -80 [SVN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535439 TSecr=0 WS=128 32.67.75589806 192.168.200.150 192.168.200.100 TCP 60 113 - 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 33.67.75619454 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	29 36.775337800	192.168.200.100	192.168.200.150	TCP	
31 36.775524204 192.168.209.109 192.168.209.159 TCP 74.53062 -80 [SVN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535439 TSecr=0 WS=128 32.67.75589806 192.168.200.150 192.168.200.100 TCP 60 113 - 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 33.67.75619454 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	39 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
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	31 36.775524204	192.168.200.100	192.168.200.150		74 53062 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
	32 36.775589886	192.168.200.150	192.168.200.100	TCP	
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	33 36.775619454	192.168.200.100	192.168.200.150	TCP	
	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

Possiamo inoltre dedurre che si tratti di qualcosa di **malevolo**, perché l'IP sospetto fa richieste su **porte non note** (al di sopra delle **1024**), porte 33878, 58636, 52358, con una certa decadenza quasi **programmata**;

Questo potrebbe comportare:

- Comunicazione con un server Command and Control (C2): è un sistema centrale utilizzato per controllare dispositivi compromessi in una rete. È un elemento chiave nelle operazioni di cyberattacco, come botnet, ransomware e trojan, consentendo agli aggressori di gestire i dispositivi infettati, eseguire comandi, rubare dati o distribuire ulteriori carichi malevoli.
- Esfiltrazione di dati o trasferimenti sospetti.

Time	Source	Destination	Protocol	Length Info
19 36.774685505	192.168.200.150	192.168.200.100	TCP	74 23 41394 [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 41394 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 41384 23 [RST, ACK] Seg=1 Ack=1 Win=64256 Len=8 TSval=810535439 TSecr=4294952466
24 26 775652407	102 169 200 100	192 169 200 150	TCD	88 58120 111 [PST ACV] San=1 AcV=1 Win=84258 Lan=0 TSval=810525420 TSpcr=4204052488

Proseguendo con la cattura notiamo che le **richieste successive** sono tutte così, confermando la **tesi** dell'IP malevolo.

Time	Source	Destination	Protocol	l Length Info
2038 36.876758682	192.168.200.150	192.168.200.100	TCP	60 929 → 55246 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2039 36.876758793	192.168.280.158	192.168.200.100	TCP	60 226 - 43104 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2040 36.876777523	192.168.200.100	192.168.200.150	TCP	74 41288 - 634 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535540 TSecr=0 WS=128
2041 36.876904687	192.168.280.100	192.168.209.150	TCP	74 59614 868 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERM TSval=810535540 TSecr=0 WS=128
2042 36.876962348	192.168.289.108	192.168.200.150	TCP	74 47788 - 643 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 SACK PERM TSval=810535540 TSecr=0 WS=128
2043 36.877009785	192.168.280.158	192.168.200.100	TCP	60 634 - 41288 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
2044 36.877034466	192.168.200.100	192.168.200.150	TCP	74 59668 - 452 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535540 TSecr=0 WS=128
2045 36.877057765	192.168.200.100	192.168.200.150	TCP	74 48334 - 844 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERM TSval=810535540 TSecr=0 WS=128
2046 36.877127876	192.168.280.158	192.168.209.100	TCP	60 868 - 59614 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2047 36.877127994	192.168.289.158	192.168.200.100	TCP	60 643 - 47788 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2048 36.877247484	192.168.280.158	192.168.200.100	TCP	60 452 - 59668 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2049 36.877247584	192.168.280.158	192.168.200.100	TCP	60 844 - 48334 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2050 36.877401110	192.168.200.100	192.168.200.150	TCP	74 44866 - 573 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535541 TSecr=0 WS=128
2051 36.877421694	192.168.200.100	192.168.200.150	TCP	74 60426 446 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535541 TSecr=0 WS=128
2052 36.877486226	192.168.200.100	192.168.200.150	TCP	74 44832 - 356 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535541 TSecr=0 WS=128
2053 36.877504764	192.168.200.100	192.168.200.150	TCP	74 44642 - 588 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535541 TSecr=0 WS=128
2054 36.877584877	192.168.200.100	192.168.200.150	TCP	74 53864 - 353 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535541 TSecr=0 WS=128
2055 36.877725143	192.168.200.150	192.168.200.100	TCP	60 573 - 44866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2056 36.877725247	192.168.280.158	192.168.209.100	TCP	60 446 60426 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2057 36.877725292		192.168.200.100	TCP	60 356 → 44832 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2058 36.877725340	192.168.200.150	192.168.200.100	TCP	60 588 - 44642 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2059 36.877725385	192.168.280.158	192.168.200.100	TCP	60 353 - 53864 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2060 36.877966945		192.168.200.150	TCP	74 48264 191 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535541 TSecr=0 WS=128
2061 36.877987825		192.168.200.150	TCP	74 44212 - 716 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535541 TSecr=0 WS=128
2062 36.878059560		192.168.200.150	TCP	74 34888 945 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535541 TSecr=0 WS=128
2063 36.878091593		192.168.200.150	TCP	74 36474 - 1017 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535541 TSecr=0 WS=128
2064 36.878126703		192.168.200.150	TCP	74 59962 971 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535541 TSecr=0 WS=128
2065 36.878210967	192.168.200.150	192.168.200.100	TCP	60 191 → 48264 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2066 36.878211066		192.168.200.100	TCP	60 716 → 44212 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2067 36.878231645		192.168.200.150	TCP	74 57278 873 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535541 TSecr=0 WS=128
2068 36.878288723		192.168.200.150	TCP	74 44182 893 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535542 TSecr=0 WS=128
2069 36.878336568		192.168.200.100	TCP	60 945 → 34888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2070 36.878336632		192.168.200.100	TCP	60 1017 → 36474 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2071 36.878336675		192.168.200.100	TCP	60 971 - 59962 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2072 36.878364352		192.168.200.150	TCP	74 54290 358 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535542 TSecr=0 WS=128
2073 36.878400106		192.168.200.150	TCP	74 42528 326 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535542 TSecr=0 WS=128
2074 36.878435498		192.168.200.150	TCP	74 34876 726 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535542 TSecr=0 WS=128
2075 36.878503055		192.168.200.100	TCP	60 873 → 57278 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2076 36.878503128		192.168.200.100	TCP	60 893 - 44182 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2077 36.878560311		192.168.200.150	TCP	74 60640 40 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535542 TSecr=0 WS=128
2078 36.878712720	192.168.280.158	192.168.200.100	TCP	60 358 - 54290 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Perciò ora il bisogno di **mitigare** o **risolvere** questo attacco sarà di **importanza** cruciale.

Soluzione:

Assodato che si tratta di una connessione maligna e pericolosa, è necessario procedere con la sua risoluzione seguendo determinati accorgimenti. In un contesto lavorativo reale, sarà essenziale rispettare le policy aziendali e affrontare ogni Indicatore di Compromissione (IoC) identificato. Gli IoC possono includere:

- Indirizzi IP malevoli: IP noti per attività dannose o sospette.
- **Hash di file:** Impronte digitali uniche di file associati a malware o altre attività malevole.
- **URL e domini malevoli:** Siti web utilizzati per phishing o distribuzione di codice malevolo.
- Processi anomali: Applicazioni o attività in esecuzione non autorizzate o sospette.
- Modifiche ai file: Alterazioni non autorizzate a file di sistema o applicazioni critiche.

In un ambiente aziendale reale, la gestione di tali minacce richiede un approccio sistematico che includa attività fondamentali come:

- Business Continuity Plan (BCP): Procedure per garantire il mantenimento delle attività aziendali critiche durante e dopo un incidente.
- Business Impact Assessment (BIA): Analisi per identificare le funzioni aziendali essenziali e valutare l'impatto di un'interruzione.

• **Disaster Recovery:** Strategie e strumenti per ripristinare rapidamente i sistemi e i dati dopo un incidente di sicurezza.

Nel nostro contesto invece, un **contesto simulato** possiamo risolvere tramite alcuni **accorgimenti specifici**:

- Bloccare l'IP sospetto: isolare l'IP 192.168.200.150 e vedere le sue attività per stabilirne il comportamento e intenzioni;
- Bloccare l'accesso alle porte non note;
- Impostare un **Firewall Dinamico** (consentendo solo connessioni che partono dal mio dispositivo verso l'esterno);

Soluzioni future:

- Abilitare un IDS/IPS;
- Segmentare la rete (Subnetting);
- Avere gli ultimi aggiornamenti su tutti i sistemi (evitare exploit conosciuti);
- Analizzare i log di sistema.