S9L5 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:

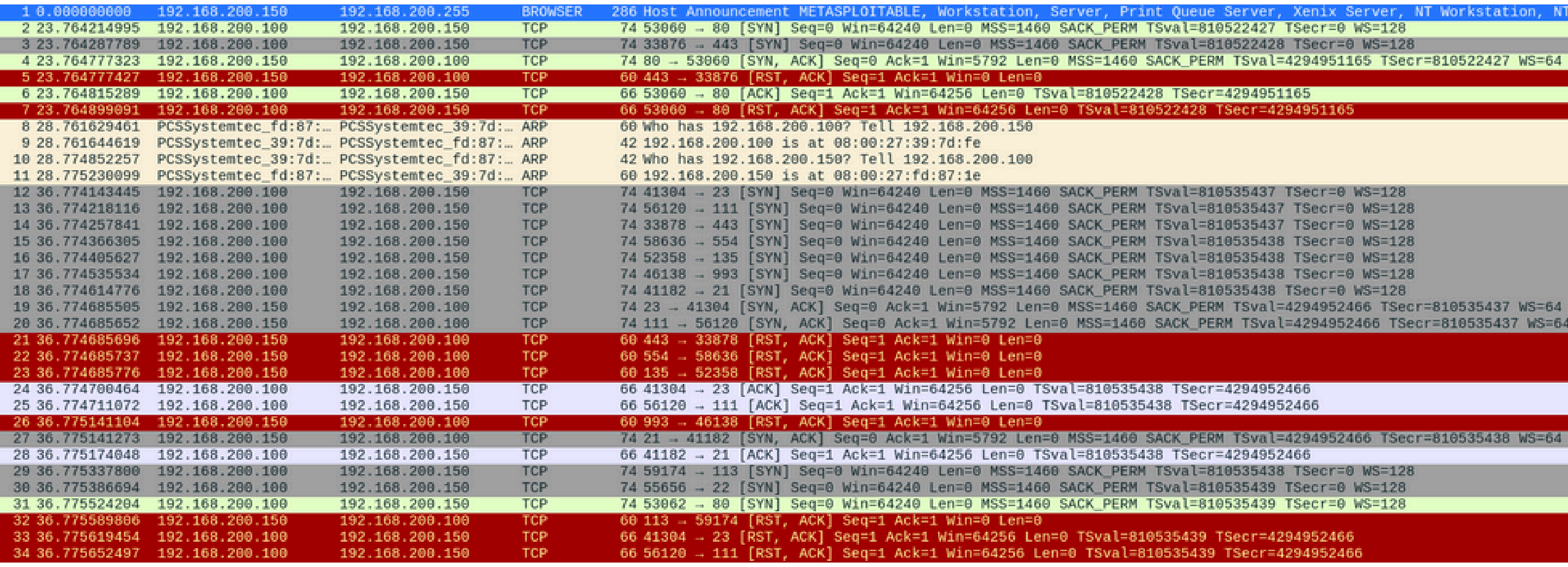
Le **policy** sono **linee guida** in materia di sicurezza seguite all'interno di un'azienda, è compito del **responsabile** della sicurezza **stabilire queste regole**, in accordo con i valori e gli obiettivi aziendali, e convincere il management a implementarle, affrontando i relativi costi. Seguendo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

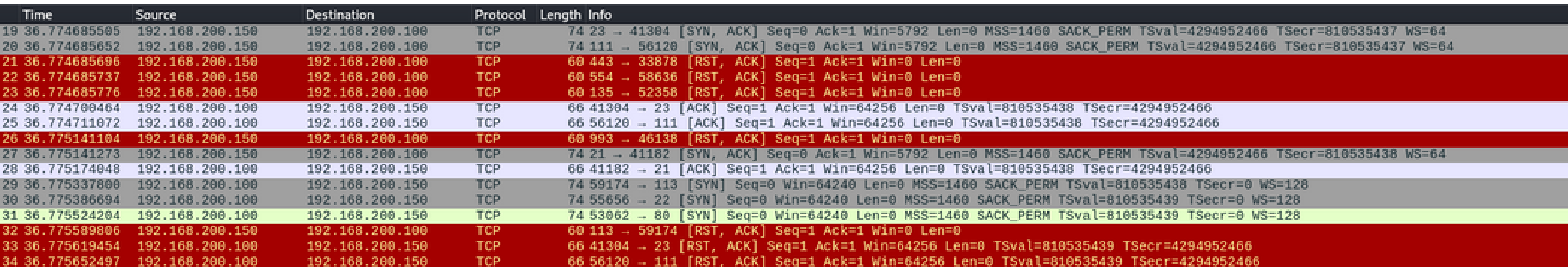


```
 1 0.000000000   192.168.200.150       192.168.200.255       BROWSER   286 Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT
 2 23.764214995  192.168.200.100       192.168.200.150       TCP        74 53060 → 80 [SYN] Seq=0 Win=64240 Len=0 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        66 53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
 7 23.764899091  192.168.200.100       192.168.200.150       TCP        66 53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
 8 28.761629461  PCSSystemtec_fd:87:…  PCSSystemtec_39:7d:…  ARP        60 Who has 192.168.200.100? Tell 192.168.200.150
 9 28.761644619  PCSSystemtec_39:7d:…  PCSSystemtec_fd:87:…  ARP        42 192.168.200.100 is at 08:00:27:39:7d:fe
10 28.774852257  PCSSystemtec_39:7d:…  PCSSystemtec_fd:87:…  ARP        42 Who has 192.168.200.150? Tell 192.168.200.100
11 28.775230099  PCSSystemtec_fd:87:…  PCSSystemtec_39:7d:…  ARP        60 192.168.200.150 is at 08:00:27:fd:87:1e
12 36.774143445  192.168.200.100       192.168.200.150       TCP        74 41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13 36.774218116  192.168.200.100       192.168.200.150       TCP        74 56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
14 36.774257841  192.168.200.100       192.168.200.150       TCP        74 33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15 36.774366305  192.168.200.100       192.168.200.150       TCP        74 58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16 36.774405627  192.168.200.100       192.168.200.150       TCP        74 52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
17 36.774535534  192.168.200.100       192.168.200.150       TCP        74 46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
18 36.774614776  192.168.200.100       192.168.200.150       TCP        74 41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
19 36.774685505  192.168.200.150       192.168.200.100       TCP        74 23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20 36.774685652  192.168.200.150       192.168.200.100       TCP        74 111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=6
21 36.774685696  192.168.200.150       192.168.200.100       TCP        60 443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22 36.774685737  192.168.200.150       192.168.200.100       TCP        60 554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23 36.774685776  192.168.200.150       192.168.200.100       TCP        60 135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24 36.774700464  192.168.200.100       192.168.200.150       TCP        66 41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
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 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
```

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**;

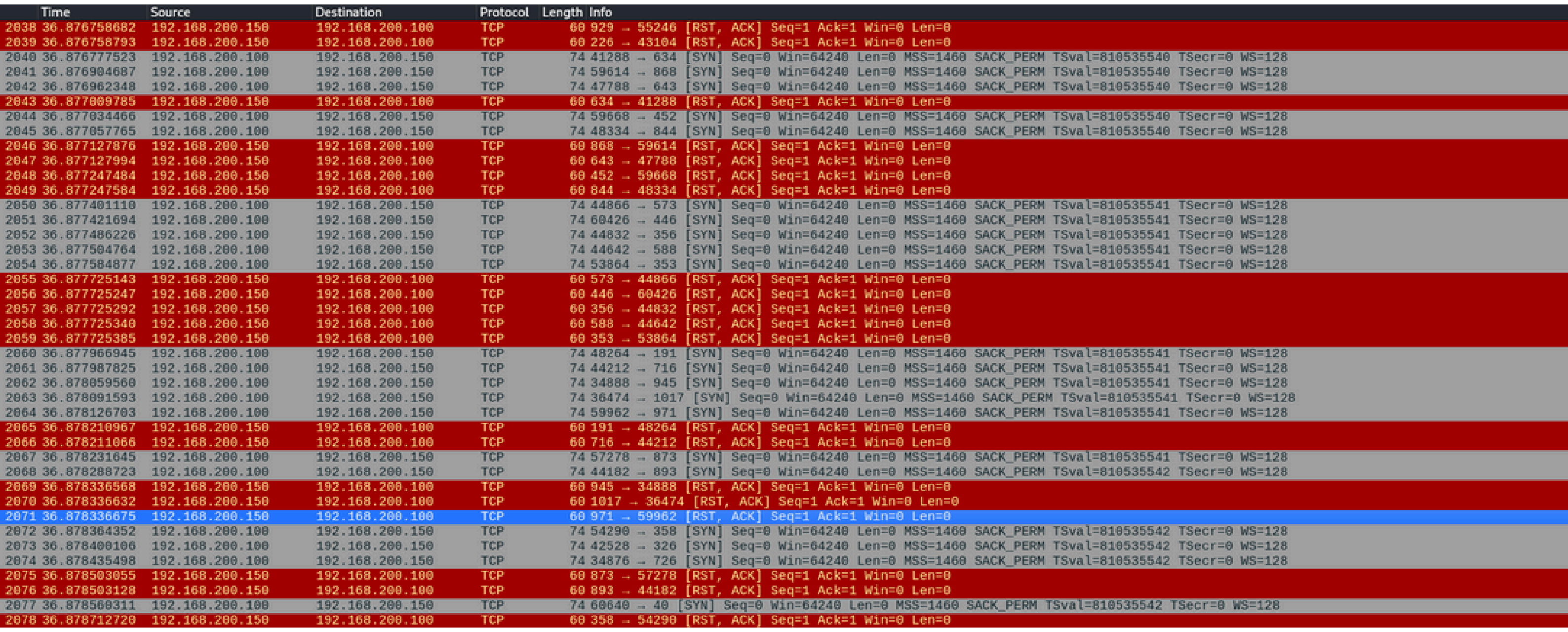
Questo potrebbe comportare:

- **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 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20 36.774685652  192.168.200.150     192.168.200.100     TCP         74 111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
21 36.774685696  192.168.200.150     192.168.200.100     TCP         60 443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22 36.774685737  192.168.200.150     192.168.200.100     TCP         60 554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23 36.774685776  192.168.200.150     192.168.200.100     TCP         60 135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24 36.774700464  192.168.200.100     192.168.200.150     TCP         66 41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
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 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
```

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



```
     Time           Source            Destination       Protocol  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  192.168.200.150  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  192.168.200.100  192.168.200.150  TCP       74 59614 → 868 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535540 TSecr=0 WS=128
2042 36.876962348  192.168.200.100  192.168.200.150  TCP       74 47788 → 643 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535540 TSecr=0 WS=128
2043 36.877009785  192.168.200.150  192.168.200.100  TCP       60 634 → 41288 [RST, ACK] Seq=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  192.168.200.150  192.168.200.100  TCP       60 868 → 59614 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2047 36.877127994  192.168.200.150  192.168.200.100  TCP       60 643 → 47788 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2048 36.877247484  192.168.200.150  192.168.200.100  TCP       60 452 → 59668 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2049 36.877247584  192.168.200.150  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  192.168.200.150  192.168.200.100  TCP       60 446 → 60426 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2057 36.877725292  192.168.200.150  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  192.168.200.150  192.168.200.100  TCP       60 353 → 53864 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2060 36.877966945  192.168.200.100  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  192.168.200.100  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  192.168.200.100  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  192.168.200.100  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  192.168.200.100  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  192.168.200.150  192.168.200.100  TCP       60 716 → 44212 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2067 36.878231645  192.168.200.100  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  192.168.200.100  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  192.168.200.150  192.168.200.100  TCP       60 945 → 34888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2070 36.878336632  192.168.200.150  192.168.200.100  TCP       60 1017 → 36474 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2071 36.878336675  192.168.200.150  192.168.200.100  TCP       60 971 → 59962 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2072 36.878364352  192.168.200.100  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  192.168.200.100  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  192.168.200.100  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  192.168.200.150  192.168.200.100  TCP       60 873 → 57278 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2076 36.878503128  192.168.200.150  192.168.200.100  TCP       60 893 → 44182 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2077 36.878560311  192.168.200.100  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  192.168.200.150  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**.