



S9-L5

T H R E A T   I N T E L L I G E N C E   &   I O C

# CONTENTS

01 Traccia

02 Cos'è Wireshark e perchè lo utilizziamo

03 Condivisione cartelle & Esportazione su Kali

04 Rilevazioni attraverso wireshark

05 Considerazioni sulle rilevazioni





# 01. TRACCIA

---

Analizzare la cattura fornita attraverso l'utilizzo del tool Wireshark 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

## 02. COS'È WIRESHARK E PERCHÈ LO UTILIZZIAMO

---



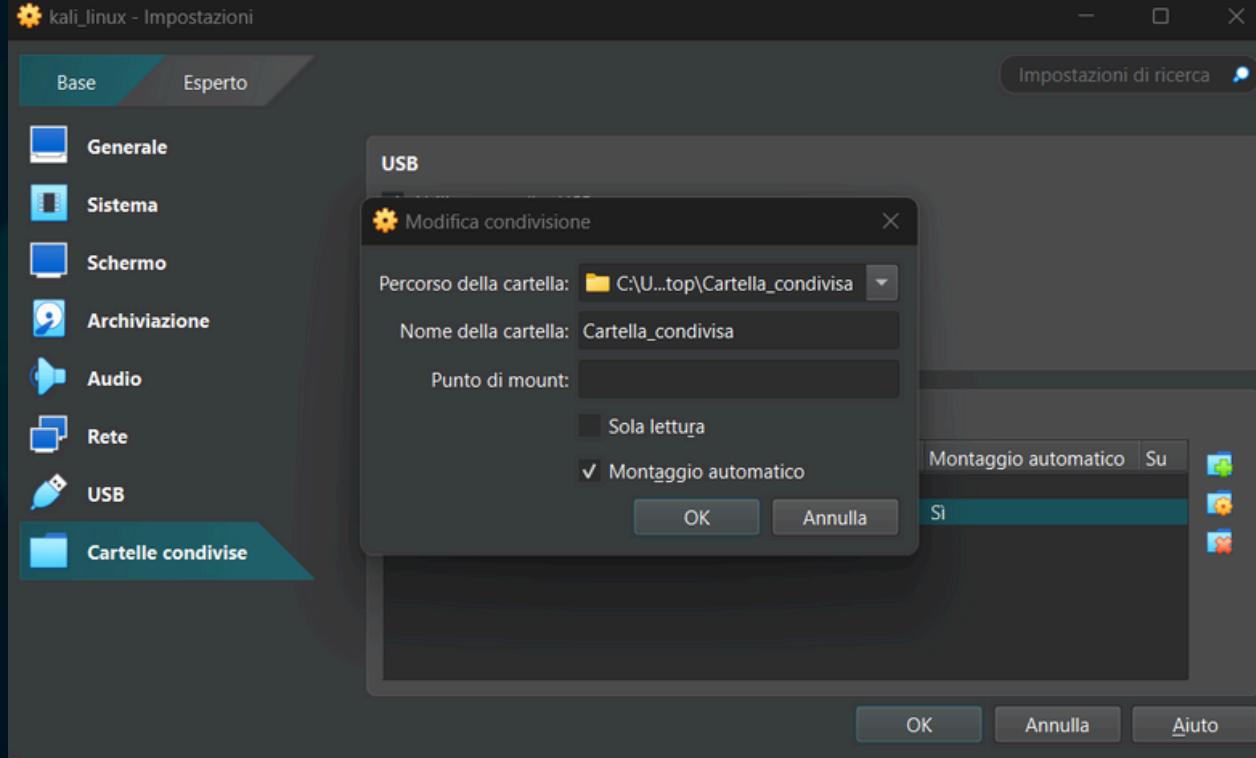
Wireshark è uno strumento straordinario per esplorare e comprendere il traffico di rete. Possiamo immaginarlo come una lente di ingrandimento che ci permette di osservare da vicino cosa accade mentre i dati viaggiano attraverso una rete. Grazie ad esso possiamo "vedere" i pacchetti di dati in transito, comprenderne il contenuto e scoprire come i dispositivi comunicano tra loro.

Lo utilizziamo poichè ci permette di capire cosa sta succedendo all'interno di una rete. Per esempio, se c'è un problema di connessione, possiamo analizzare i pacchetti per scoprire dove si trova l'intoppo. Oppure, se sospettiamo un'attività insolita, Wireshark ci aiuta a investigare e a rilevare eventuali minacce, come attacchi o vulnerabilità.

Il bello è che non si limita a mostrare i dati grezzi, ma li organizza e li rende comprensibili. Possiamo filtrare i pacchetti per concentrarci su quelli che ci interessano, come il traffico proveniente da un indirizzo specifico o relativo a un particolare protocollo, come HTTP o DNS. Questo lo rende uno strumento prezioso per chiunque lavori con le reti, dagli amministratori ai professionisti della sicurezza.

Per questa specifica situazione, utilizzeremo Wireshark per analizzare una cattura già effettuata per poter fornire un riscontro e delle considerazioni in merito.

# 03. CONDIVISIONE CARTELLE & ESPORTAZIONE SU KALI LINUX



Procediamo poi con l'esportazione muovendolo il file sul desktop di kali. Usiamo poi il comando "**chmod ugo+rw**" per concedere i permessi di lettura e scrittura al file e con il comando "**chown kali**" per modificare il proprietario del file che in questo caso diventerà kali.

Una volta ricevuto il file da analizzare, procediamo con la condivisione delle cartelle sulla nostra macchina virtuale Kali linux creando una cartella chiamata "Cartella\_condivisa" dove sarà presente il nostro file.

```
(kali㉿kali)-[/media]
└$ ls
cdrom  cdrom0  sf_Cartella_condivisa

(kali㉿kali)-[/media]
└$ cd sf_Cartella_condivisa
└$ ls
Cattura_U3_W1_L3.pcapng

(kali㉿kali)-[/media/sf_Cartella_condivisa]
└$ mv Cattura_U3_W1_L3.pcapng /home/kali/Desktop

(kali㉿kali)-[/media/sf_Cartella_condivisa]
└$ cd /home/kali/Desktop

(kali㉿kali)-[~/Desktop]
└$ chmod ugo+rw Cattura_U3_W1_L3.pcapng

(kali㉿kali)-[~/Desktop]
└$ chown kali Cattura_U3_W1_L3.pcapng
```

# 04. RILEVAZIONI ATTRAVERSO WIRESHARK

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential ..
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM 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=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
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 → 53062 [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	53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.775861964	192.168.200.100	192.168.200.150	TCP	66	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
41	36.776005853	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

# 04. RILEVAZIONI ATTRAVERSO WIRESHARK

35 36. 775797004 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 Tsva=4294952466 TSecr=810535439 WS=64
36 36. 775813232 192.168.200.150	192.168.200.150	TCP	74 80 - 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsva=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 Tsva=810535439 TSecr=4294952466
38 36. 775813232 192.168.200.100	192.168.200.150	TCP	66 53062 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535439 TSecr=4294952466
39 36. 775861964 192.168.200.100	192.168.200.150	TCP	66 41182 - 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=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 Tsva=810535439 TSecr=4294952466
41 36. 776005853 192.168.200.100	192.168.200.150	TCP	66 53062 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535439 TSecr=4294952466
42 36. 776179338 192.168.200.100	192.168.200.150	TCP	74 56684 - 199 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535439 TSecr=0 WS=128
43 36. 776233888 192.168.200.100	192.168.200.150	TCP	74 54220 - 995 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535439 TSecr=0 WS=128
44 36. 776330916 192.168.200.100	192.168.200.150	TCP	74 34648 - 587 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535440 TSecr=0 WS=128
45 36. 776385694 192.168.200.100	192.168.200.150	TCP	74 33042 - 445 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535440 TSecr=0 WS=128
46 36. 776402599 192.168.200.100	192.168.200.150	TCP	74 49814 - 256 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=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. 776476261 192.168.200.100	192.168.200.150	TCP	74 46990 - 139 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535440 TSecr=0 WS=128
50 36. 776496366 192.168.200.100	192.168.200.150	TCP	74 33266 - 143 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535440 TSecr=0 WS=128
51 36. 776512221 192.168.200.100	192.168.200.150	TCP	74 66632 - 25 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535440 TSecr=0 WS=128
52 36. 776568696 192.168.200.100	192.168.200.150	TCP	74 49654 - 110 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535440 TSecr=0 WS=128
53 36. 776671271 192.168.200.100	192.168.200.150	TCP	74 37282 - 53 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535440 TSecr=0 WS=128
54 36. 776720715 192.168.200.100	192.168.200.150	TCP	74 54898 - 500 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=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, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535440 TSecr=0 WS=128
57 36. 776904828 192.168.200.150	192.168.200.100	TCP	74 445 - 33042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsva=810535440 TSecr=0 WS=128
58 36. 776904922 192.168.200.150	192.168.200.100	TCP	60 256 - 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59 36. 776904961 192.168.200.150	192.168.200.100	TCP	74 139 - 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsva=810535440 TSecr=0 WS=128
60 36. 776905094 192.168.200.150	192.168.200.100	TCP	60 143 - 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61 36. 776905643 192.168.200.150	192.168.200.100	TCP	74 25 - 66632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsva=810535440 TSecr=0 WS=128
62 36. 776905882 192.168.200.150	192.168.200.100	TCP	60 110 - 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63 36. 776905123 192.168.200.150	192.168.200.100	TCP	74 53 - 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsva=810535440 TSecr=0 WS=128
64 36. 776905162 192.168.200.150	192.168.200.100	TCP	60 588 - 54898 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65 36. 776914772 192.168.200.100	192.168.200.150	TCP	66 33042 - 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535440 TSecr=4294952466
66 36. 776941029 192.168.200.100	192.168.200.150	TCP	66 46990 - 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535440 TSecr=4294952466
67 36. 776962328 192.168.200.100	192.168.200.150	TCP	66 66632 - 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=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 Tsva=810535440 TSecr=4294952466
69 36. 777118481 192.168.200.150	192.168.200.100	TCP	60 487 - 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
70 36. 777143014 192.168.200.100	192.168.200.150	TCP	74 56990 - 767 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535440 TSecr=0 WS=128
71 36. 777186821 192.168.200.100	192.168.200.150	TCP	74 35638 - 436 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535440 TSecr=0 WS=128
72 36. 777302991 192.168.200.100	192.168.200.150	TCP	74 34120 - 98 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535441 TSecr=0 WS=128
73 36. 777337934 192.168.200.100	192.168.200.150	TCP	74 49760 - 78 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535441 TSecr=0 WS=128
74 36. 777439632 192.168.200.150	192.168.200.100	TCP	60 787 - 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

\*\*Ulteriori rilevazioni wireshark\*\*

75 36. 777430741 192.168.200.150	192.168.200.100	TCP	60 436 - 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76 36. 777473018 192.168.200.100	192.168.200.150	TCP	74 36138 - 588 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535441 TSecr=0 WS=128
77 36. 777522494 192.168.200.100	192.168.200.150	TCP	74 52428 - 962 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535441 TSecr=0 WS=128
78 36. 777623082 192.168.200.150	192.168.200.100	TCP	60 98 - 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79 36. 777623149 192.168.200.150	192.168.200.100	TCP	60 78 - 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80 36. 777645027 192.168.200.100	192.168.200.150	TCP	74 41874 - 764 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535441 TSecr=0 WS=128
81 36. 7776680898 192.168.200.100	192.168.200.150	TCP	74 51506 - 435 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535441 TSecr=0 WS=128
82 36. 777758636 192.168.200.150	192.168.200.100	TCP	60 589 - 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83 36. 777758696 192.168.200.150	192.168.200.100	TCP	60 962 - 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84 36. 7777871245 192.168.200.150	192.168.200.100	TCP	60 764 - 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85 36. 7777871293 192.168.200.150	192.168.200.100	TCP	60 435 - 51506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86 36. 777893298 192.168.200.100	192.168.200.150	TCP	60 33042 - 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535441 TSecr=4294952466
87 36. 777912717 192.168.200.100	192.168.200.150	TCP	60 46990 - 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535441 TSecr=4294952466
88 36. 777986759 192.168.200.100	192.168.200.150	TCP	60 66632 - 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535441 TSecr=4294952466
89 36. 778031265 192.168.200.100	192.168.200.150	TCP	60 37282 - 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535441 TSecr=4294952466
90 36. 778179978 192.168.200.100	192.168.20		

## 05. CONSIDERAZIONI SULLE RILEVAZIONI

---

### Identificazione di IoC (indicatori di compromissione)

Di primo impatto l'intero traffico sembra avvenire tra indirizzi IP della stessa rete (gli indirizzi in questione sono "192.168.200.100" e "192.168.200.150"). Questo potrebbe indicare che un dispositivo compromesso sta tentando di muoversi all'interno della rete.

Si osservano tentativi di handshake TCP incompleti o irregolari (pacchetti SYN) seguiti da reset (RST), che possono essere sintomo di un attacco di scansione delle porte, comunicazioni interrotte da firewall o dispositivi o servizi configurati male. Questo è, tuttavia, comune in scenari di ricognizione attiva, quando un attaccante tenta di sondare porte o servizi aperti e il sistema bersaglio risponde con pacchetti di reset. Potrebbe anche indicare il tentativo di interrompere connessioni sospette o fallite.

Infine l'utilizzo ripetuto del flag ACK potrebbe indicare traffico alterato, problemi nella rete, oppure tentativi di flooding TCP (ovvero un tipo di attacco Dos o Ddos che mira a sovraccaricare un sistema di rete inviando un numero elevato di pacchetti TCP verso un bersaglio, con l'obiettivo di saturare la capacità della rete).

# 05. CONSIDERAZIONI SULLE RILEVAZIONI

---

## Ipotesi sui potenziali vettori di attacco

- Un attaccante potrebbe cercare di muoversi da un dispositivo a un altro all'interno della rete. Questo può succedere quando un malware o un ransomware si propaga da una macchina compromessa a un'altra. È un comportamento comune in molti tipi di attacchi informatici.
- Se si notano molte connessioni TCP che non si completano e tanti tentativi di connessione (SYN), potrebbe significare che un dispositivo nella rete sta cercando di "scansionare" altri dispositivi per individuare vulnerabilità, come accade durante la fase di ricognizione di un attacco.
- L'indirizzo IP 192.168.200.150 potrebbe essere il punto da cui partono attacchi diretti a servizi interni, come quelli che cercano di indovinare password tramite attacchi di brute force (tentativi ripetuti di accesso) o exploit per vulnerabilità note.
- Tuttavia il traffico sospetto potrebbe non risultare dannoso in quanto potrebbe essere risultante di un configurazione errata o malfunzionamenti dei dispositivi legittimi.

# 05. CONSIDERAZIONI SULLE RILEVAZIONI

---

## Consigli per ridurre gli impatti dell'attacco attuale

Per ridurre l'impatto dell'attacco consiglierei di:

- Identificare gli IP che mandano pacchetti sospetti e bloccarli temporaneamente con il firewall (sembrebbe che il dispositivo 192.168.200.150 è quello sospetto).
- Impostare limiti di connessioni simultanee per ridurre il carico sul server, utilizzando tool come iptables (che permette di configurare le regole del firewall).
- Abilitare i SYN Cookies che per la maggior parte dei server moderni, rappresentano una buona misura di protezione contro SYN flood. Tuttavia potrebbero ridurre leggermente le prestazioni e non supportano alcune funzionalità avanzate di TCP.
- Modificare il Timeout per connessioni incomplete in modo che il sistema rilasci risorse più rapidamente.
- Continuare a monitorare il traffico di rete per rilevare variazioni nel pattern degli attacchi.

# 05. CONSIDERAZIONI SULLE RILEVAZIONI

---

## Consigli per prevenire eventuali attacchi futuri

Per prevenire eventuali attacchi futuri consiglierei di:

- Implementare un WAF per filtrare traffico sospetto e proteggere le web application.
- Implementare un rate limiting per limitare la velocità delle richieste per prevenire abusi.
- Aggiornare Sistema operativo, servizi di rete e software in modo da prevenire l'uso di vulnerabilità note (I 0 days sono l'unica eccezione a cui si potrebbe allacciare un malintenzionato per attaccare la nostra rete se teniamo in considerazione questo).
- Segmentare la rete con delle VLAN per limitare l'impatto degli attacchi.
- Abilitare dei sistemi di rilevamento o prevenzione (IDS/IPS) per identificare e bloccare attacchi in tempo reale.
- Assicurarsi che il team IT sia formato per rispondere rapidamente agli incidenti di sicurezza.

THANK YOU FOR YOUR  
ATTENTION

MATTIA DI DONATO