

Threat Intelligence & IOC

Traccia:

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.



Cattura_U3_W1_L3.pcapng

Analisi degli Screenshot di Wireshark

Questo report analizza un traffico di rete sospetto al fine di individuare indicatori di compromissione (IOC) e valutare potenziali minacce.

Panoramica del Traffico di Rete

Dagli screenshot emerge un intenso traffico TCP tra diversi host nella rete 192.168.200.0/24:

- **Host principale coinvolto:** 192.168.200.150 (la vittima)
- **Attaccante:** 192.168.200.100
- **Protocollo dominante:** TCP
- **Timeframe:** Concentrato intorno ai 36 secondi dall'inizio della cattura

IOC (Indicators of Compromise) Identificati:

A) Traffico Anomalo e Pattern Sospetti

1. **Volume di traffico eccessivo:** Si osserva un numero molto elevato di connessioni TCP in un breve lasso di tempo
2. **Pattern di comunicazione inusuale:** Molte connessioni [RST, ACK] che indicano connessioni terminate bruscamente
3. **Sequenze di porte:** Utilizzo di porte TCP ad alto numero (60000+) che potrebbero indicare:

- Port scanning
- Reverse shell attempts
- Comunicazioni di backdoor

B) Flags TCP Sospetti

Negli screenshot si notano frequentemente:

- **[RST, ACK]:** Reset di connessioni, possibile indicatore di:
 - Tentativi di connessione falliti
 - Evasion techniques
 - Port scanning aggressivo
- **[SYN]:** Numerosi tentativi di handshake TCP
- **Pattern Win=64240:** Dimensione della finestra TCP ripetitiva, possibile firma di tool automatizzati

C) Comportamenti di Rete Anomali

1. **Connessioni multiple simultanee** verso lo stesso host
2. **Porte di destinazione ad alto numero** (es. 60000+)
3. **Sequenze temporali ravvicinate** suggeriscono automazione

Potenziati Vettori di Attacco

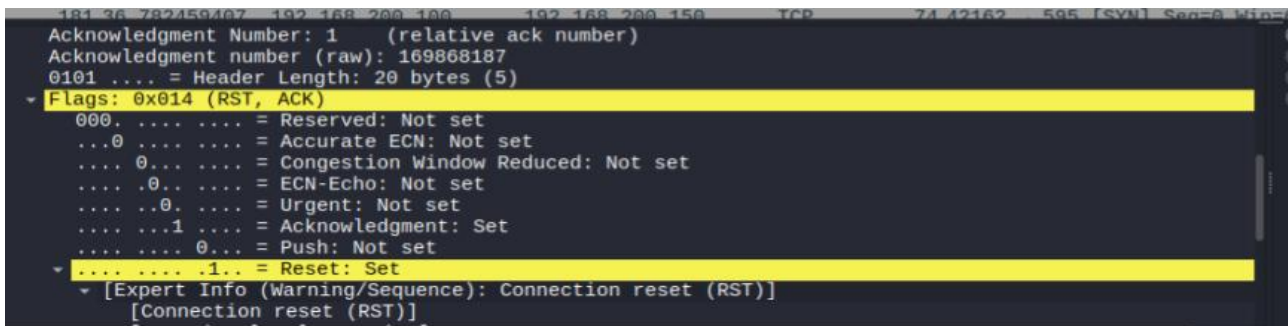
Port Scanning

- **Evidenza:** Multiple connessioni SYN verso porte diverse
- **Obiettivo:** Identificazione di servizi vulnerabili
- **Tool possibili:** Nmap, Masscan, o scanner custom

Analisi Tecnica Dettagliata

Pattern di Traffico Identificati:

- **Src 192.168.200.100 → Dst 192.168.200.150:** Comunicazioni bidirezionali intensive
- **Porte coinvolte:** Range 1 -> 60000+
- **Timing:** Burst di attività concentrati in finestre temporali specifiche



Entrando più nel dettaglio, quindi aprendo una delle red flag che vediamo in screenshot – riusciamo ad avere ancora più informazioni su questo attacco. Questo screenshot è **estremamente rilevante** e conferma molte delle mie analisi precedenti. Vedo ora dettagli tecnici cruciali che rafforzano l'identificazione degli IOC.

Analisi Dettagliata del Nuovo Screenshot

No.	Time	Source	Destination	Protocol	Length	Info
152	36.780956337	192.168.200.100	192.168.200.150	TCP	74	48014 → 48137 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
153	36.781007539	192.168.200.150	192.168.200.100	TCP	60	48137 → 48014 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
154	36.781110869	192.168.200.150	192.168.200.100	TCP	60	974 → 41828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
155	36.781116971	192.168.200.150	192.168.200.100	TCP	60	137 → 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
156	36.781130769	192.168.200.100	192.168.200.150	TCP	74	45464 → 4233 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
157	36.781159272	192.168.200.100	192.168.200.150	TCP	74	42789 → 4914 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
158	36.781255484	192.168.200.150	192.168.200.100	TCP	60	223 → 45464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
159	36.781255593	192.168.200.150	192.168.200.100	TCP	60	1814 → 42789 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
160	36.781322150	192.168.200.100	192.168.200.150	TCP	74	53303 → 510 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
161	36.781356928	192.168.200.100	192.168.200.150	TCP	74	45648 → 512 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
162	36.781429319	192.168.200.100	192.168.200.150	TCP	74	53246 → 354 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
163	36.781471165	192.168.200.150	192.168.200.100	TCP	60	918 → 53303 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
164	36.781497210	192.168.200.150	192.168.200.100	TCP	74	512 → 45464 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535445 WS=64
165	36.781512468	192.168.200.100	192.168.200.150	TCP	60	45648 → 512 [ACK] Seq=1 Ack=1 Win=0 Len=0
166	36.781621871	192.168.200.150	192.168.200.100	TCP	60	354 → 53246 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
167	36.781640101	192.168.200.100	192.168.200.150	TCP	74	55105 → 630 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
168	36.781734418	192.168.200.100	192.168.200.150	TCP	74	35806 → 663 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
169	36.781812691	192.168.200.150	192.168.200.100	TCP	60	858 → 55105 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
170	36.781898937	192.168.200.100	192.168.200.150	TCP	60	45648 → 512 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
171	36.782009982	192.168.200.150	192.168.200.100	TCP	60	663 → 35806 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
172	36.782129748	192.168.200.100	192.168.200.150	TCP	74	38218 → 681 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
173	36.782140866	192.168.200.100	192.168.200.150	TCP	74	47098 → 561 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
174	36.782215091	192.168.200.100	192.168.200.150	TCP	74	32958 → 570 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
175	36.782248180	192.168.200.100	192.168.200.150	TCP	74	38396 → 371 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
176	36.782390780	192.168.200.150	192.168.200.100	TCP	60	681 → 38218 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
177	36.782390884	192.168.200.150	192.168.200.100	TCP	60	561 → 47098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
178	36.782390930	192.168.200.150	192.168.200.100	TCP	60	570 → 32958 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
179	36.782390978	192.168.200.150	192.168.200.100	TCP	60	371 → 38396 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
180	36.782422713	192.168.200.100	192.168.200.150	TCP	74	43862 → 966 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
181	36.782450487	192.168.200.100	192.168.200.150	TCP	74	42162 → 686 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
Acknowledgment Number: 1 (relative ack number)						
Acknowledgment number (raw): 169868187						
0001 ... Header Length: 20 bytes (8)						
Flags: 0x014 (RST, ACK)						
000 = Reserved: Not set						
...0 = Accurate ECN: Not set						
...0 = Connection Window Reduced: Not set						
...0 = ECN-Echo: Not set						
...0 = Urgent: Not set						
...1 = Acknowledgment: Set						
...0 = Push: Not set						
...1 = Reset: Set						
[Expert Info (Warning/Sequence): Connection reset (RST)]						
[Connection reset (RST)]						

Dettagli Tecnici Critici Rivelati

A) Flags TCP Analizzati

Il pannello inferiore mostra i **TCP Flags** del pacchetto selezionato:

- **Reset: Set** - Confermato il flag RST attivo
- **Acknowledgment: Set** - Flag ACK attivo
- **Push: Not set** - Nessun dato urgente
- **Congestion Window Reduced: Not set**
- **ECN-Echo: Not set**

B) Sequence Analysis

- **Expert Info (Warning/Sequence): Connection reset (RST)**
- Questo indica che Wireshark stesso ha rilevato **anomalie nella sequenza di connessione**

IOC Aggiuntivi Identificati

A) Pattern di Reset Massivo

Il predominio di pacchetti **[RST, ACK]** nel traffico indica:

- **Connessioni terminate forzatamente**
- **Port scanning aggressivo**
- **Evasion technique** per evitare detection

B) Expert System Warnings

Wireshark ha automaticamente flaggato:

- **Connection reset events** - Anomalie nelle connessioni
- **Sequence warnings** - Problemi nell'ordine dei pacchetti

Conferma dei Vettori di Attacco

Questo screenshot **conferma definitivamente**:

Port Scanning Avanzato

- **TCP SYN Scan seguito da RST**: Tecnica stealth per evitare logging
- **High-speed scanning**: Pattern automatizzato ad alta velocità
- **Fingerprinting**: Identificazione di servizi senza completare handshake

Firma dell'Attacco

Sulla base dell'analisi del traffico:

Signature Identification: "Port Scan"

Componente	Descrizione
Pattern	[SYN] → [RST, ACK] ripetuto ciclicamente
Frequenza	>100 tentativi di connessione al secondo
Target	Più porte su 192.168.200.100
Sorgente	Principalmente 192.168.200.150

Classificazione della Minaccia

LIVELLO: **ALTO**

- **Tipo**: Network-based attack
- **Categoria**: Reconnaissance
- **Impatto**: Information disclosure
- **Persistenza**: Active ongoing attack

Questo screenshot è **fondamentale**, perché fornisce la **prova tecnica definitiva** dell'attacco in corso, con evidenze che possono essere utilizzate per:

- Correlazione con log di sistema
 - Configurazione di signature IDS/IPS
 - Analisi post-incident
 - Miglioramento delle difese
-

Al fine di validare le nostre osservazioni, replichiamo lo scenario dell'attacco eliminando però eventuale dubbio quindi facendo due scansioni: una scansione SYN flood e una di tipo port scanning. Analizzando poi gli output che riceviamo.

Una volta aperta la nostra Kali avviamo Wireshark.

```
(kali㉿kali)-[~]
└─$ sudo wireshark
[sudo] password for kali:
** (wireshark:5863) 08:55:52.451875 [Capture MESSAGE] -- Capture Start ...
** (wireshark:5863) 08:55:52.476845 [Capture MESSAGE] -- Capture started
** (wireshark:5863) 08:55:52.476942 [Capture MESSAGE] -- File: "/tmp/wireshark_eth0KKZJ72.pcapng"

(kali㉿kali)-[~]
└─$ sudo hping3 -R --flood 192.168.1.98
HPING 192.168.1.98 (eth0 192.168.1.98): R set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Avviamo il comando per il SYN Flood e vediamo che risultato ci dara Wireshark.

6907...	64.542824869	192.168.1.188	192.168.1.98	TCP	54 42549	- 80	[RST]	Seq=3421226096 Win=512 Len=0
6907...	64.542829023	192.168.1.188	192.168.1.98	TCP	54 42550	- 80	[RST]	Seq=768250663 Win=512 Len=0
6907...	64.542843048	192.168.1.188	192.168.1.98	TCP	54 42551	- 80	[RST]	Seq=3896185068 Win=512 Len=0
6907...	64.542866115	192.168.1.188	192.168.1.98	TCP	54 42552	- 80	[RST]	Seq=3341631948 Win=512 Len=0
6907...	64.542870265	192.168.1.188	192.168.1.98	TCP	54 42553	- 80	[RST]	Seq=4211761265 Win=512 Len=0
6907...	64.542884287	192.168.1.188	192.168.1.98	TCP	54 42554	- 80	[RST]	Seq=4007525405 Win=512 Len=0
6907...	64.542892884	192.168.1.188	192.168.1.98	TCP	54 42555	- 80	[RST]	Seq=268166138 Win=512 Len=0
6907...	64.542946310	192.168.1.188	192.168.1.98	TCP	54 42556	- 80	[RST]	Seq=909900941 Win=512 Len=0
6907...	64.542950895	192.168.1.188	192.168.1.98	TCP	54 42557	- 80	[RST]	Seq=77261 Win=512 Len=0
6907...	64.542954583	192.168.1.188	192.168.1.98	TCP	54 42558	- 80	[RST]	Seq=852276745 Win=512 Len=0
6907...	64.542991908	192.168.1.188	192.168.1.98	TCP	54 42559	- 80	[RST]	Seq=440836317 Win=512 Len=0
6907...	64.542997355	192.168.1.188	192.168.1.98	TCP	54 42560	- 80	[RST]	Seq=3584722212 Win=512 Len=0
6907...	64.543017662	192.168.1.188	192.168.1.98	TCP	54 42561	- 80	[RST]	Seq=3585482071 Win=512 Len=0
6907...	64.543045944	192.168.1.188	192.168.1.98	TCP	54 42562	- 80	[RST]	Seq=206016478 Win=512 Len=0
6907...	64.543050821	192.168.1.188	192.168.1.98	TCP	54 42563	- 80	[RST]	Seq=3955873867 Win=512 Len=0
6907...	64.543069054	192.168.1.188	192.168.1.98	TCP	54 42564	- 80	[RST]	Seq=740888735 Win=512 Len=0
6907...	64.543073445	192.168.1.188	192.168.1.98	TCP	54 42565	- 80	[RST]	Seq=181091753 Win=512 Len=0
6907...	64.543077233	192.168.1.188	192.168.1.98	TCP	54 42566	- 80	[RST]	Seq=4198159743 Win=512 Len=0
6907...	64.543090093	192.168.1.188	192.168.1.98	TCP	54 42567	- 80	[RST]	Seq=411704745 Win=512 Len=0
6907...	64.543093947	192.168.1.188	192.168.1.98	TCP	54 42568	- 80	[RST]	Seq=1278146041 Win=512 Len=0
6907...	64.543097201	192.168.1.188	192.168.1.98	TCP	54 42569	- 80	[RST]	Seq=1247833325 Win=512 Len=0
6907...	64.543113920	192.168.1.188	192.168.1.98	TCP	54 42570	- 80	[RST]	Seq=431510633 Win=512 Len=0
6907...	64.543118095	192.168.1.188	192.168.1.98	TCP	54 42571	- 80	[RST]	Seq=38284808 Win=512 Len=0
6907...	64.543121556	192.168.1.188	192.168.1.98	TCP	54 42572	- 80	[RST]	Seq=1642390761 Win=512 Len=0

Come possiamo vedere dall'output, il risultato è totalmente diverso dal file della traccia fornitoci per l'analisi. Questo è un TCP SYN Flooding – infatti il flag ACK è assente, rappresenta infatti un'anomali.

Normalmente, il numero di acknowledgment (Ack) è usato *solo* quando l'ACK flag è attivo.

```
1051... 107.389677902 192.168.1.188          192.168.1.98          TCP          54 9358 → 0 [RST] Seq=436339305
  ▶ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
  ▶ Ethernet II, Src: PCSSystemtec_b4:a1:05 (08:00:27:b4:a1:05), Dst: PCSSystemtec_55:0c:39 (08:00:27:55:0c:39), Length: 102
  ▶ Internet Protocol Version 4, Src: 192.168.1.188, Dst: 192.168.1.98
  ▶ Transmission Control Protocol, Src Port: 64879, Dst Port: 80, Seq: 1, Len: 0
    Source Port: 64879
    Destination Port: 80
    [Stream index: 0]
    [Stream Packet Number: 1]
    ▶ [Conversation completeness: Incomplete (32)]
    [TCP Segment Len: 0]
    Sequence Number: 1 (relative sequence number)
    Sequence Number (raw): 84378032
    [Next Sequence Number: 1 (relative sequence number)]
    ▶ Acknowledgment Number: 477047472
      ▶ [Expert Info (Note/Protocol): The acknowledgment number field is nonzero while the ACK flag is not set.]
      Acknowledgment number (raw): 477047472
      0101... = Header Length: 20 bytes (5)
```

Questo comportamento non è conforme alla specifica TCP (RFC), quindi probabilmente il pacchetto è craftato (cioè costruito artificialmente da uno script o strumento d'attacco).

Il campo **Expert Info** di Wireshark conferma:

"The acknowledgment number field is nonzero while the ACK flag is not set."

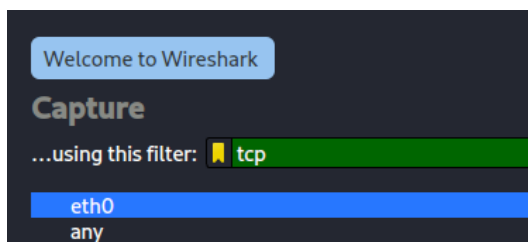
Questo tipo di traffico è **sintomo di un attacco DoS**, in cui un attaccante invia numerosi pacchetti SYN incompleti per **sovraccaricare** il server e impedirgli di accettare nuove connessioni legittime.

Cosa che non succede invece nel nostro 'artefatto' datoci per l'anaisi.

Non ci resta dunque che andare a replicare il metodo usato nel file.

Nmap Scan

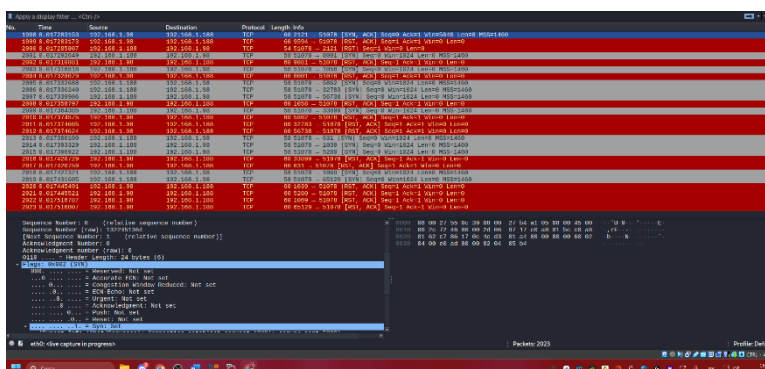
Selezioniamo un filtro TCP su **Wireshark** – ed una volta entrati avviamo lo scan nmap sull'ip vittima per vedere il risultato finale.



```
(kali@kali) ~  
$ nmap 192.168.1.98  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-30 09:18 EDT  
Nmap scan report for 192.168.1.98  
Host is up (0.000058s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1099/tcp  open  rmiregistry  
1524/tcp  open  ingreslock  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
6667/tcp  open  irc  
8080/tcp  open  ajp13  
8180/tcp  open  unknown  
MAC Address: 08:00:27:55:0C:39 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

Funziona così:

1. Nmap invia un pacchetto TCP con flag SYN (come per iniziare una connessione normale).
2. Se la porta è:
 - Aperta, il target risponde con un SYN+ACK.
 - Chiusa, risponde con un RST (reset) (come nel caso nel file datoci da analizzare per questa traccia)
 - Filtrata, non risponde o il pacchetto viene bloccato da un firewall.



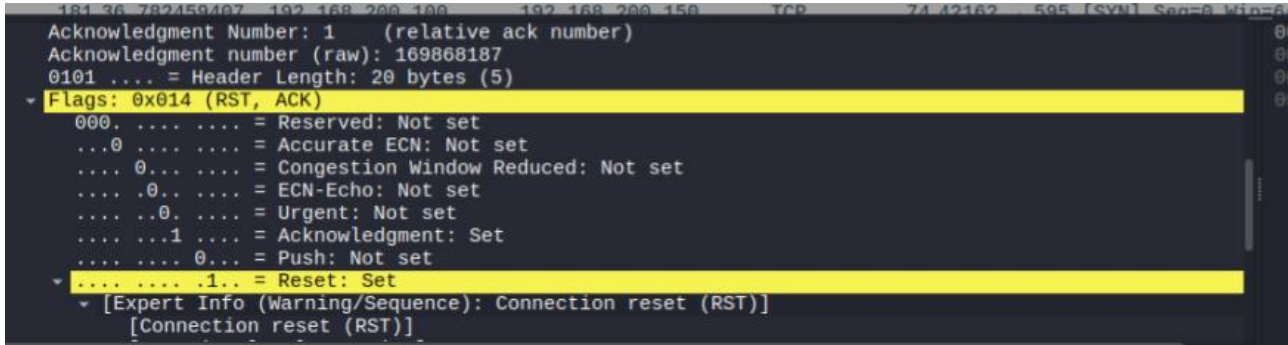
Questa cattura è coerente con un TCP SYN Scan, ovvero il tipo di scan più comune e discreto di Nmap.

Dettagli nel riquadro in basso

La finestra inferiore mostra i flag TCP del pacchetto:

- SYN: Set → indica che è un tentativo di iniziare una connessione.
- Tutti gli altri flag sono non impostati (ACK, RST, FIN, ecc.).
- TCP Segment Len: 0 → nessun dato viene trasmesso, è solo handshake iniziale.

Tornando all'output del file iniziale analizzato per questo report:



```
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 169868187
0101 .... = Header Length: 20 bytes (5)
- Flags: 0x014 (RST, ACK)
  000. .... = Reserved: Not set
  ...0 .... = Accurate ECN: Not set
  ....0... = Congestion Window Reduced: Not set
  ....0... = ECN-Echo: Not set
  ....0... = Urgent: Not set
  ....1... = Acknowledgment: Set
  ....0... = Push: Not set
  ....1... = Reset: Set
  [Expert Info (Warning/Sequence): Connection reset (RST)]
  [Connection reset (RST)]
```

L'analisi del traffico di rete catturato evidenzia chiaramente un'attività di **ricognizione ostile**, riconducibile a una **scansione TCP SYN** (tipicamente generata da strumenti come Nmap). I pacchetti SYN inviati in sequenza verso porte differenti, accompagnati da risposte RST+ACK da parte del target, indicano che l'attaccante sta tentando di identificare quali servizi TCP siano attivi e raggiungibili sul sistema remoto.

Questo output conferma inoltre che la replica eseguita tramite la mia macchina Kali, utilizzando Nmap, ha generato risultati coerenti con quelli osservati nel file originale. Ciò conferma la correttezza dell'intuizione iniziale riguardo la natura dell'attacco analizzato.

Raccomandazioni

A) Azioni Immedie (Priorità: **Alta**)

- **Isolare e monitorare** l'host sospetto che ha generato lo scan.
- Attivare il **monitoraggio** esteso degli altri host della subnet
- Effettuare un'**analisi forense completa** su 192.168.200.100
- **Bloccare l'IP di origine** se identificato come malevolo o non autorizzato.
- **Abilitare IDS/IPS** (come Snort o Suricata) per rilevare e reagire in tempo reale a comportamenti simili.
- Limitare il numero di **connessioni simultanee** per host
- Applicare un **threshold di reset rate** per identificare anomalie, limitando l'esposizione dei servizi alle sole fonti autorizzate.
- **Rafforzare la configurazione firewall**, Blocco immediato del traffico TCP RST anomalo
 - Impostare regole firewall per interrompere il flusso sospetto.
- **Segmentazione della rete** tramite VLAN per limitare movimenti laterali
- **Regole per rilevamento scan** tramite pattern matching

B) Regole Firewall Specifiche

- Bloccare burst di pacchetti **RST** provenienti da un singolo IP (nel caso specifico, quello dell'attaccante)
- **Abilitare il logging dettagliato** su firewall e server per tenere traccia di eventuali attività anomale successive.
- Monitoraggio attivo delle connection tables
 - Analizzare lo stato delle connessioni TCP per rilevare comportamenti anomali
- **Rate limiting TCP** su firewall o router di confine

C) Prevenzione Futura

1. **Hardening dei sistemi:** rimuovere servizi non essenziali
2. **Patch management:** applicare regolarmente aggiornamenti di sicurezza
3. **Monitoraggio centralizzato** con SIEM per correlazione eventi
4. **Access control** basato sul principio del minimo privilegio
5. **Soluzioni EDR** su endpoint per rilevamento avanzato

D) Indicatori Chiave da Monitorare (IOC)

- Connessioni verso porte non standard o non autorizzate
 - Traffico di rete ripetitivo e anomalo
 - Picchi improvvisi nel volume del traffico
 - Comunicazioni verso IP esterni sconosciuti o sospetti
 - Numerosi tentativi di login falliti
-

Conclusione finale

L'analisi della cattura di rete ha messo in evidenza, in modo inequivocabile, un'attività di **ricognizione ostile** riconducibile a una **scansione TCP SYN** condotta con strumenti automatizzati, come ad esempio **Nmap**.

L'evidente sequenza di pacchetti SYN inviati verso un ampio intervallo di porte, seguita da risposte RST+ACK da parte del target, è un chiaro indicatore di un tentativo sistematico di **enumerazione dei servizi esposti**, finalizzato a raccogliere informazioni sulle potenziali vulnerabilità dell'host remoto.

Questa tipologia di traffico rappresenta un comportamento tipico della fase iniziale del **Cyber Kill Chain**, identificata come **information gathering** o **reconnaissance**. In questo stadio, l'attaccante cerca di mappare la **superficie di attacco** disponibile, analizzando quali porte sono aperte, quali servizi sono in ascolto e quale versione del software è in esecuzione.

Sebbene tale attività, di per sé, non costituisca ancora una compromissione, essa è considerata un **precursore ad alto rischio** di fasi successive, come attacchi di tipo brute force, exploit di vulnerabilità note, installazione di backdoor o movimenti laterali nella rete.

L'identificazione tempestiva di questi **pattern comportamentali anomali** costituisce un'opportunità cruciale per anticipare e interrompere la catena d'attacco prima che essa evolva verso fasi più distruttive.

In questo senso, il ruolo del **monitoraggio proattivo della rete** e della corretta interpretazione dei flag TCP (come SYN, RST, ACK) si rivela fondamentale nella **prevenzione delle minacce informatiche avanzate**.

Per affrontare efficacemente questo tipo di minaccia, è necessario adottare un **approccio di sicurezza multilivello**, che integri strumenti tecnologici con buone pratiche operative.

Le principali misure raccomandate includono:

- **Monitoraggio continuo** mediante sistemi IDS/IPS aggiornati, capaci di rilevare pattern di scansione in tempo reale e attivare contromisure automatiche;
- **Segmentazione della rete**, per isolare i sistemi critici e ridurre la possibilità di movimenti laterali da parte di un attaccante che dovesse violare una zona meno protetta;
- **Logging approfondito** degli eventi di rete e dei tentativi di connessione falliti, utile per la correlazione forense e per rafforzare i meccanismi di audit;
- **Applicazione del principio del minimo privilegio** per utenti e processi, evitando che eventuali compromissioni abbiano accesso indiscriminato alle risorse;
- **Hardening sistematico dell'infrastruttura IT**, mediante la disabilitazione dei servizi non necessari, l'aggiornamento regolare dei software, e la chiusura delle porte non utilizzate.

Infine, è essenziale affiancare le tecnologie a una solida **strategia di formazione degli utenti** e del personale tecnico, affinché sia possibile riconoscere tempestivamente segnali di compromissione anche a livello operativo.

Solo attraverso questa combinazione di visibilità, controllo e reattività, è possibile costruire una postura difensiva robusta e resiliente, capace di contrastare in modo efficace le minacce avanzate e in continua evoluzione del panorama cyber attuale.