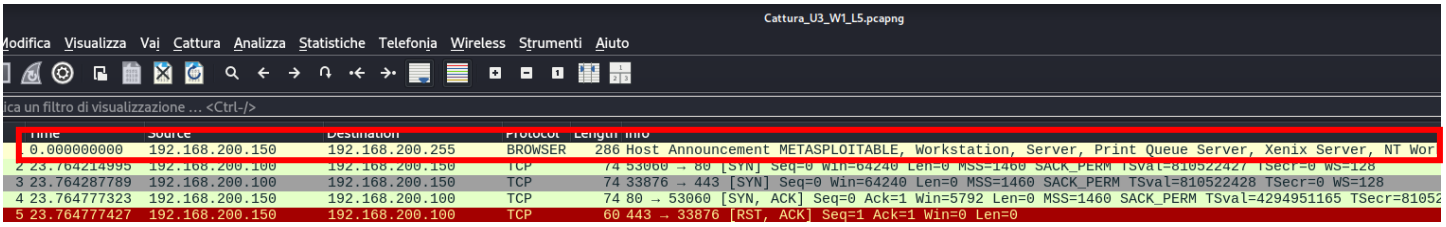
Relazione S9L5

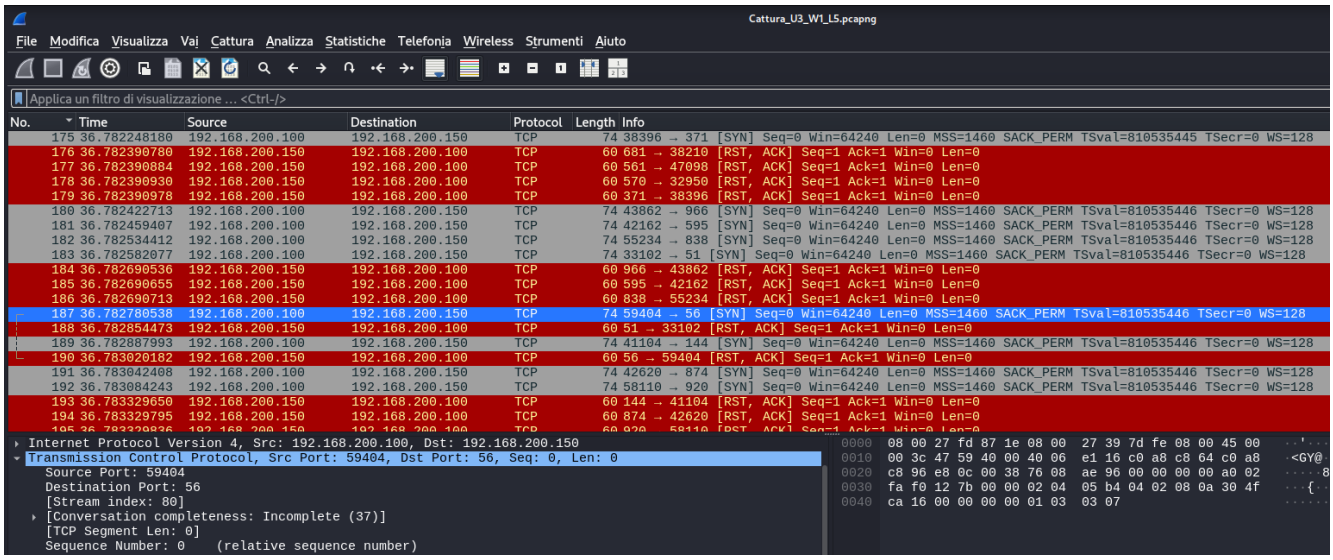
Dalla scansione Wireshark inviata dal nostro collega possiamo individuare degli IOC (Indicatori di Compromissione. Il probabile punto di ingresso nella rete è stato il server di una stampante lasciato scoperto.



	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Wor
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=81052
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

Tentativi di connessione TCP SYN Flooding

- L'IP **192.168.200.100** invia ripetutamente **TCP SYN** sulle porte dalla "**1**" alla "**1024**" verso l'IP **192.168.200.150**. Questi pacchetti indicano tentativi di stabilire delle connessioni, le quali potrebbero suggerire un primo approccio da parte dell'attaccante.



No.	Time	Source	Destination	Protocol	Length	Info
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 → 38210 [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 → 32950 [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	36.782459407	192.168.200.100	192.168.200.150	TCP	74	42162 → 595 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
182	36.782534412	192.168.200.100	192.168.200.150	TCP	74	55234 → 838 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
183	36.782582077	192.168.200.100	192.168.200.150	TCP	74	33102 → 51 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
184	36.782690536	192.168.200.150	192.168.200.100	TCP	60	966 → 43862 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
185	36.782690655	192.168.200.150	192.168.200.100	TCP	60	595 → 42162 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
186	36.782690713	192.168.200.150	192.168.200.100	TCP	60	838 → 55234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
187	36.782780538	192.168.200.100	192.168.200.150	TCP	74	59404 → 56 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
188	36.782854473	192.168.200.150	192.168.200.100	TCP	60	51 → 33102 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
189	36.782887993	192.168.200.100	192.168.200.150	TCP	74	41104 → 144 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
190	36.783020182	192.168.200.150	192.168.200.100	TCP	60	56 → 59404 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
191	36.783042408	192.168.200.100	192.168.200.150	TCP	74	42620 → 874 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
192	36.783084243	192.168.200.100	192.168.200.150	TCP	74	58110 → 920 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
193	36.783329650	192.168.200.150	192.168.200.100	TCP	60	144 → 41104 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
194	36.783329795	192.168.200.150	192.168.200.100	TCP	60	874 → 42620 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Risposte di Reset (RST):

- Ogni tentativo di connessione da parte di **192.168.200.100** viene seguito da una risposta **RST** (Reset) inviata da **192.168.200.150**. Il flag **RST** indica che la connessione viene immediatamente rifiutata, un comportamento che può essere causato da un firewall o da un sistema di difesa attivo che blocca i tentativi di connessione non autorizzati.

Pattern di pacchetti ripetitivi

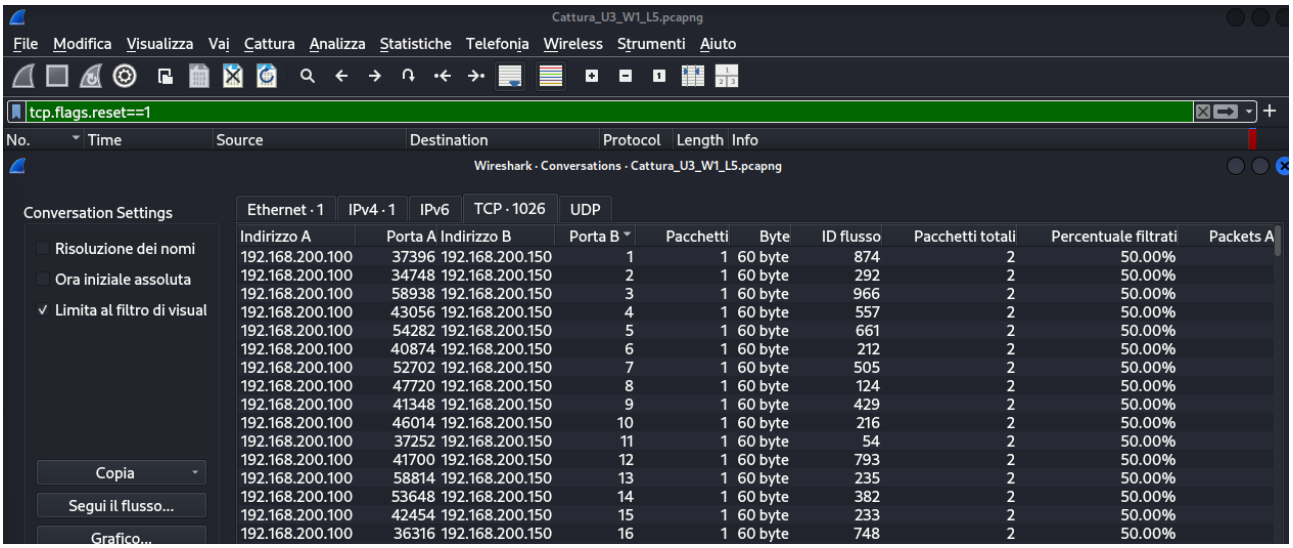
- I tentativi di connessione e le risposte **RST** sono ripetuti in modo quasi identico per diverse porte di comunicazione, indicando una scansione delle porte o un attacco a più porte del server. Questo tipo di comportamento è tipico di attività di scansione da parte di un attaccante che cerca di identificare vulnerabilità nel sistema.

Ipotesi sui Potenziali Vettori di Attacco

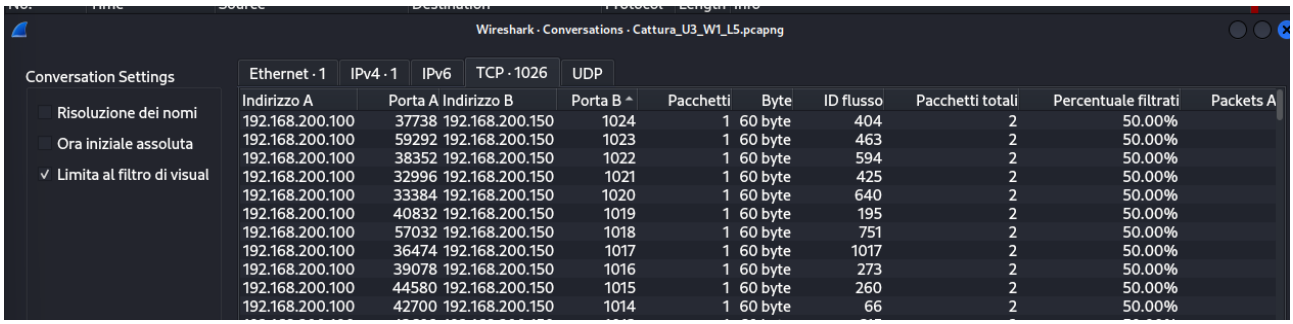
In base ai dati raccolti possiamo formulare delle ipotesi sui potenziali vettori d'attacco utilizzate in questo caso.

Scansione delle porte (Port scanning)

- L'invio di pacchetti SYN a diverse porte suggerisce che 192.168.200.100 stia eseguendo una scansione delle porte per identificare eventuali porte aperte o vulnerabili su 192.168.200.150. Questo comportamento è caratteristico di attacchi di tipo "Port Scanning", dove l'attaccante cerca di mappare la rete e individuare i punti deboli da sfruttare. Questi dati ci suggeriscono un probabile utilizzo di "nmap" come comando di scanning dato che sono state scansionate le prime 1024 porte.



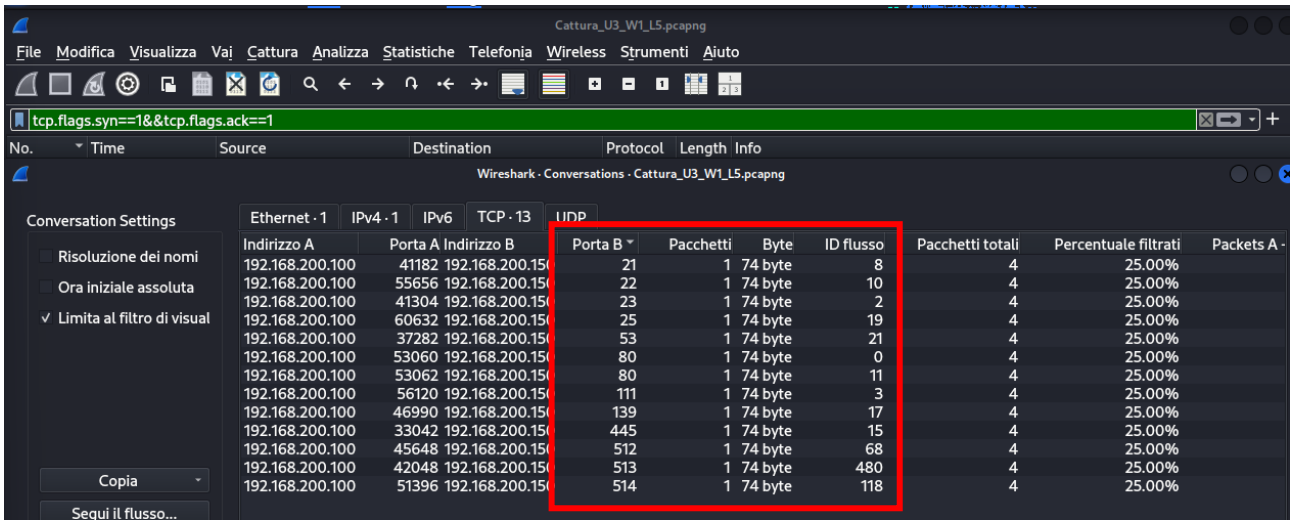
Indirizzo A	Porta A	Indirizzo B	Porta B	Pacchetti	Byte	ID flusso	Pacchetti totali	Percentuale filtrati	Packets A
192.168.200.100	37396	192.168.200.150	1	1	60 byte	874	2	50.00%	
192.168.200.100	34748	192.168.200.150	2	1	60 byte	292	2	50.00%	
192.168.200.100	58938	192.168.200.150	3	1	60 byte	966	2	50.00%	
192.168.200.100	43056	192.168.200.150	4	1	60 byte	557	2	50.00%	
192.168.200.100	54282	192.168.200.150	5	1	60 byte	661	2	50.00%	
192.168.200.100	40874	192.168.200.150	6	1	60 byte	212	2	50.00%	
192.168.200.100	52702	192.168.200.150	7	1	60 byte	505	2	50.00%	
192.168.200.100	47720	192.168.200.150	8	1	60 byte	124	2	50.00%	
192.168.200.100	41348	192.168.200.150	9	1	60 byte	429	2	50.00%	
192.168.200.100	46014	192.168.200.150	10	1	60 byte	216	2	50.00%	
192.168.200.100	37252	192.168.200.150	11	1	60 byte	54	2	50.00%	
192.168.200.100	41700	192.168.200.150	12	1	60 byte	793	2	50.00%	
192.168.200.100	58814	192.168.200.150	13	1	60 byte	235	2	50.00%	
192.168.200.100	53648	192.168.200.150	14	1	60 byte	382	2	50.00%	
192.168.200.100	42454	192.168.200.150	15	1	60 byte	233	2	50.00%	
192.168.200.100	36316	192.168.200.150	16	1	60 byte	748	2	50.00%	



Indirizzo A	Porta A	Indirizzo B	Porta B	Pacchetti	Byte	ID flusso	Pacchetti totali	Percentuale filtrati	Packets A
192.168.200.100	37738	192.168.200.150	1024	1	60 byte	404	2	50.00%	
192.168.200.100	59292	192.168.200.150	1023	1	60 byte	463	2	50.00%	
192.168.200.100	38352	192.168.200.150	1022	1	60 byte	594	2	50.00%	
192.168.200.100	32996	192.168.200.150	1021	1	60 byte	425	2	50.00%	
192.168.200.100	33384	192.168.200.150	1020	1	60 byte	640	2	50.00%	
192.168.200.100	40832	192.168.200.150	1019	1	60 byte	195	2	50.00%	
192.168.200.100	57032	192.168.200.150	1018	1	60 byte	751	2	50.00%	
192.168.200.100	36474	192.168.200.150	1017	1	60 byte	1017	2	50.00%	
192.168.200.100	39078	192.168.200.150	1016	1	60 byte	273	2	50.00%	
192.168.200.100	44580	192.168.200.150	1015	1	60 byte	260	2	50.00%	
192.168.200.100	42700	192.168.200.150	1014	1	60 byte	66	2	50.00%	

Tentativo di intrusione e ricognizione

- La scansione delle porte potrebbe anche indicare un tentativo di ricognizione finalizzato a identificare vulnerabilità sfruttabili (ad esempio, attraverso exploit di software o servizi non sicuri). Dalla scansione rileviamo le porte aperte che il malintenzionato potrebbe utilizzare per attaccare la nostra rete.



Raccomandazioni per Ridurre gli Impatti dell'Attacco Attuale e Futuri

Implementazione dell'anello debole in un firewall rigoroso o migliorare tutta la rete:

- Impostare regole firewall che limitano le connessioni in ingresso da indirizzi IP sospetti o non riconosciuti, oppure integrare la rete wireless della stampante all'interno delle competenze del firewall. Le risposte RST potrebbero già essere una difesa attiva, ma l'adozione di un firewall più restrittivo potrebbe aiutare a bloccare ulteriori tentativi di scansione o attacchi

Limiti di Connessione e Rate Limiting:

- Implementare un sistema di rate limiting che limiti il numero di connessioni simultanee per un singolo indirizzo IP o porta. Ciò ridurrebbe la capacità di un attaccante di eseguire attacchi SYN Flood.

Monitoraggio Attivo della Rete:

- Attivare il monitoraggio in tempo reale per rilevare anomalie nel traffico di rete, come un numero elevato di pacchetti SYN o tentativi di connessione da un singolo IP verso molteplici porte. L'analisi automatizzata dei flussi di rete può aiutare a identificare tempestivamente attacchi in corso

Implementazione di IDS/IPS:

- Utilizzare sistemi di rilevamento (IDS) e prevenzione delle intrusioni (IPS) per identificare e bloccare i tentativi di scansione delle porte e i possibili attacchi DoS prima che possano danneggiare i sistemi.

Aggiornamenti e Patch di Sicurezza:

- Assicurarsi che tutti i dispositivi e le applicazioni siano aggiornati con le ultime patch di sicurezza, per ridurre la possibilità che un attaccante possa sfruttare vulnerabilità note.

Formazione del Personale e Procedure di Incident Response:

- Formare il personale IT a riconoscere i segnali di attacco e rispondere tempestivamente, nonché a implementare e testare regolarmente procedure di risposta agli incidenti per ridurre i tempi di recupero durante un attacco.