Report Progetto S9/L5

Analisi della cattura di rete – Threat Intelligence & IOC

1. Executive Summary

Il presente report analizza una cattura di traffico di rete ottenuta tramite **Wireshark**, con l'obiettivo di individuare eventuali **comportamenti anomali** e possibili **indicatori di compromissione**.

L'analisi ha evidenziato un'attività sistematica di **scansione TCP** all'interno della rete locale, caratterizzata dall'invio ripetuto di pacchetti **SYN** verso un ampio insieme di porte, seguiti da risposte **RST/ACK**.

In alcuni casi, come sulle **porte 80 e 22**, è stato osservato il completamento del three-way handshake TCP; tuttavia, tali connessioni risultano estremamente brevi e prive di traffico applicativo significativo.

Nel complesso, **non sono state rilevate sessioni TCP complete né traffico applicativo significativo** e l'attività osservata non ha superato la fase di ricognizione, **senza portare a una compromissione riuscita del sistema target**.

Le evidenze tecniche a supporto dell'analisi, inclusi gli estratti più significativi della cattura di traffico, sono riportate nell'**Appendice A – Evidenze Tecniche**, a fini documentali.

2. Contesto e Obiettivo dell'Analisi

La presente analisi è stata condotta su una **cattura di traffico di rete** fornita nell'ambito del **Progetto S9/L5**, con l'obiettivo di esaminare in modo critico il traffico osservato al fine di individuare **eventuali indicatori di compromissione (IOC)** riconducibili ad attività di attacco in corso.
In particolare, l'analisi mira a **identificare e analizzare le evidenze di comportamenti anomali**, formulare **ipotesi sui potenziali vettori di attacco** sulla base degli IOC individuati e **proporre azioni di mitigazione** finalizzate a ridurre l'impatto dell'attacco osservato e a prevenire eventi analoghi in futuro.

3. Metodologia di Analisi

L'analisi è stata effettuata attraverso:

- osservazione **temporale e sequenziale** dei pacchetti catturati;
- analisi dei **flag TCP** (SYN, ACK, RST);
- correlazione delle diverse porzioni della cattura per individuare **pattern ripetitivi**;
- distinzione tra traffico legittimo e traffico anomalo.

L'approccio adottato consente di valutare l'attività di rete non come eventi isolati, ma come un'unica operazione coerente nel tempo.

4. Analisi Tecnica del Traffico

4.1 Identificazione degli Host Coinvolti

L'analisi del traffico ha evidenziato **due host** principali:

- **Host A**: 192.168.200.100
- **Host B**: 192.168.200.150

La presenza di **pacchetti ARP** nella cattura, utilizzati per la risoluzione degli indirizzi IP in indirizzi MAC tra i due sistemi, indica che **entrambi gli host appartengono allo stesso dominio di broadcast** e comunicano direttamente a livello **Layer 2**, senza l'intermediazione di dispositivi di routing.

Tale evidenza conferma che l'attività osservata avviene **all'interno della stessa rete locale**, configurando un contesto di **ricognizione interna**, piuttosto che di attacco proveniente dall'esterno del perimetro di rete.

4.2 Pattern di Comunicazione TCP

Il traffico analizzato è caratterizzato da un numero elevato di **tentativi di connessione TCP verso porte differenti**, realizzati tramite l'invio ripetuto di pacchetti **SYN** da parte dell'host che avvia la comunicazione e dalla successiva terminazione delle connessioni mediante pacchetti **RST/ACK**.

Nella maggior parte dei casi, tali sequenze **non portano all'instaurazione di connessioni durature** e vengono interrotte immediatamente.
In alcuni casi, come sulle **porte 80 e 22**, è stato osservato il completamento del **three-way handshake TCP**; tuttavia, le connessioni risultano **estremamente brevi e prive di qualsiasi traffico applicativo significativo**, senza richieste di servizio o scambi di dati.

È inoltre rilevante osservare che i **pacchetti RST/ACK** non provengono esclusivamente dal sistema che riceve il tentativo di connessione, ma in alcune circostanze risultano **inviati dall'host che ha avviato l'handshake**, indicando una **terminazione volontaria delle connessioni TCP** dopo la verifica della disponibilità dei servizi. Tale comportamento è tipico delle attività di **scansione automatizzata**, finalizzate a ridurre i tempi di attesa e a evitare il mantenimento di stati di connessione non necessari.

Nel traffico analizzato:

- non sono presenti pacchetti di tipo PSH né traffico applicativo;
- non si osservano tentativi di autenticazione o interazione applicativa;
- l'ACK associato ai pacchetti RST/ACK rappresenta un meccanismo di gestione dello stato del protocollo TCP e non indica una comunicazione riuscita.

Nel complesso, il pattern osservato risulta coerente con una **attività di scansione delle porte**, orientata alla verifica della raggiungibilità dei servizi e alla **mappatura della superficie di attacco**, piuttosto che con una comunicazione legittima o con un tentativo di sfruttamento.

4.3 Analisi Temporale e Ripetitività

L'analisi temporale della cattura evidenzia che il traffico osservato **non è episodico né casuale**, ma si sviluppa secondo una sequenza coerente e ripetitiva **distribuita lungo l'intera durata della registrazione**. I pacchetti analizzati mostrano un comportamento omogeneo in termini di **pattern TCP**, con tentativi di connessione ripetuti verso un ampio insieme di porte e con modalità operative costanti.

Nelle fasi iniziali della cattura si osservano **tentativi di connessione mirati verso porte comunemente associate a servizi noti**, compatibili con una fase di

ricognizione preliminare. Successivamente, l'attività si estende progressivamente a un numero maggiore di porte, includendo anche **porte medio–alte**, indicando un **ampliamento della mappatura della superficie di attacco**.

Nel corso della cattura, il pattern di comunicazione rimane invariato: i tentativi di connessione vengono **interrotti immediatamente**, sia tramite risposte **RST/ACK** da parte del sistema che riceve il tentativo, sia tramite **terminazioni volontarie delle connessioni** da parte dell'host che avvia l'handshake. Tale comportamento si ripete in modo sistematico, senza variazioni che possano suggerire un cambiamento di tecnica o un'evoluzione verso fasi di sfruttamento.

Nelle porzioni finali della cattura si osserva una **riduzione dei pacchetti SYN** e una prevalenza di pacchetti RST/ACK, comportamento compatibile con una **fase di chiusura o consolidamento dell'attività di scansione**, in cui vengono terminati gli stati TCP residui senza ulteriori tentativi di interazione.

Nel complesso, la distribuzione temporale e la ripetitività del traffico indicano che l'attività osservata è **riconducibile a un'unica operazione di scansione automatizzata**, articolata in più fasi ma **coerente nella tecnica e negli obiettivi**, senza evidenze di escalation verso comunicazioni applicative o tentativi di compromissione.

4.4 Porte Coinvolte e Superficie di Attacco

L'analisi del traffico evidenzia tentativi di connessione verso un insieme eterogeneo di porte, comprendenti **sia porte comunemente associate a servizi noti** (ad esempio **80**, **443**, **22**, **445**) sia un ampio numero di **porte distribuite su range numerici differenti, non immediatamente riconducibili a servizi standard** nel contesto osservato.

La presenza di tentativi di connessione verso porte appartenenti a **range elevati e variabili**, combinata con l'assenza di traffico applicativo e di richieste di servizio, suggerisce un'attività orientata alla **mappatura estesa della superficie di attacco**, piuttosto che a un'interazione mirata con specifici servizi.

Nel complesso, la distribuzione delle porte e la modalità con cui vengono interrogate indicano una **enumerazione sistematica dei servizi esposti**, finalizzata alla valutazione dell'esposizione complessiva del sistema, senza evidenze di tentativi di sfruttamento o utilizzo applicativo delle porte individuate.

5. Indicatori di Compromissione (IOC)

L'analisi della cattura di traffico di rete ha permesso di individuare diversi **Indicatori di Compromissione (IOC)** di tipo **comportamentale**, riconducibili a un'attività di ricognizione attiva all'interno della rete locale. Gli IOC identificati non sono di tipo file-based o domain-based, ma emergono dall'osservazione dei **pattern di comunicazione** e delle **modalità operative** adottate.

5.1 Indicatori di rete

Tra gli IOC di rete più rilevanti si evidenziano:

- **Elevato numero di tentativi di connessione TCP** verso un ampio insieme di porte, distribuite su range numerici eterogenei;
- **Pattern ricorrente SYN → RST/ACK**, indicativo di tentativi di enumerazione dei servizi senza instaurazione di sessioni persistenti;
- **Ripetitività temporale** dei tentativi, con sequenze regolari e prive di interazione applicativa;
- **Terminazione volontaria delle connessioni TCP** anche da parte dell'host che avvia l'handshake, comportamento tipico di strumenti di scansione automatizzata;
- **Assenza di traffico applicativo**, quali richieste HTTP, autenticazioni o scambi di dati.

Tali elementi, osservati nel loro insieme, rappresentano evidenze coerenti di **scansione delle porte** finalizzata alla mappatura della superficie di attacco.

5.2 Indicatori comportamentali

Dal punto di vista comportamentale, l'attività osservata presenta le seguenti caratteristiche:

- **Enumerazione sistematica dei servizi esposti**, piuttosto che interazione mirata con uno specifico servizio;
- **Connessioni estremamente brevi**, anche nei casi in cui il three-way handshake TCP risulta completato;

- **Assenza di escalation** verso fasi di sfruttamento, come invio di payload o tentativi di autenticazione;
- **Coerenza tecnica** lungo l'intera durata della cattura, indicativa di un'unica attività strutturata.

Questi indicatori sono compatibili con una **fase di ricognizione (reconnaissance)** e non con una comunicazione legittima o con un attacco già in fase avanzata.

5.3 Sintesi degli IOC individuati

In sintesi, gli IOC rilevati possono essere classificati come segue:

- **Tipologia**: comportamentale / di rete
- **Tecnica osservata**: scansione TCP delle porte
- **Ambito**: rete locale
- **Fase della kill chain**: ricognizione
- **Impatto osservato**: nessuna compromissione riuscita

L'insieme degli indicatori conferma che l'attività osservata rappresenta un **tentativo di preparazione a un potenziale attacco**, intercettato prima dell'avvio di fasi di sfruttamento o movimento laterale.

6. Analisi del Vettore di Attacco (Kill Chain)

Sulla base degli **Indicatori di Compromissione (IOC)** individuati e dell'analisi tecnica del traffico di rete, l'attività osservata può essere collocata all'interno della **fase di ricognizione (Reconnaissance)** della kill chain di un attacco informatico.

Durante l'intera cattura, i comportamenti rilevati risultano coerenti con una **attività di discovery ed enumerazione dei servizi**, finalizzata alla raccolta di informazioni preliminari sull'esposizione del sistema e sulla disponibilità dei servizi di rete. I tentativi di connessione TCP verso porte multiple, la ripetitività delle sequenze e la terminazione immediata delle comunicazioni indicano un'azione orientata alla **mappatura della superficie di attacco**, piuttosto che all'esecuzione di un attacco diretto.

È rilevante sottolineare che l'**attività non progredisce oltre la fase di ricognizione**. In particolare, non sono state osservate:

- fasi di **weaponization** o preparazione di payload;
- tentativi di **exploitation** di vulnerabilità note;
- **interazioni applicative**, quali autenticazioni o invio di richieste di servizio;
- evidenze di **movement laterale** o **command and control**.

Nei casi in cui il **three-way handshake TCP risulta completato**, le connessioni vengono comunque **interrotte immediatamente**, senza alcuno scambio di dati applicativi. Tale comportamento conferma che l'obiettivo dell'attività non è l'utilizzo dei servizi individuati, bensì la sola **verifica della loro raggiungibilità**.

Nel contesto della kill chain, l'assenza di qualsiasi evoluzione verso fasi successive indica che l'attività osservata **rappresenta un tentativo di preparazione** a un potenziale attacco, intercettato prima che potesse tradursi in una compromissione effettiva del sistema.

7. Valutazione del Rischio

L'attività osservata nella cattura di traffico di rete rappresenta un **evento di sicurezza rilevante**, pur non avendo prodotto evidenze di compromissione riuscita. La valutazione del rischio deve pertanto considerare sia l'**impatto effettivo osservato**, sia il **potenziale di evoluzione** dell'attività nel contesto di una rete operativa.

Dal punto di vista dell'**impatto immediato**, l'attività risulta **limitata alla fase di ricognizione**, senza instaurazione di sessioni applicative, senza sfruttamento di vulnerabilità e senza movimento laterale. In assenza di exploit o comunicazioni persistenti, **non si rilevano danni diretti** ai sistemi coinvolti né perdita di disponibilità, integrità o riservatezza delle informazioni.

Tuttavia, dal punto di vista del **rischio potenziale**, l'attività presenta elementi che non possono essere trascurati. La presenza di una **scansione sistematica delle porte**, effettuata all'interno della rete locale, indica una **possibile preparazione a fasi successive dell'attacco**, quali lo sfruttamento di servizi vulnerabili o l'espansione laterale qualora fossero individuati punti di ingresso utilizzabili.

In particolare, il rischio aumenta nel caso in cui:

- uno degli host coinvolti risulti **già compromesso**;
- siano presenti **servizi esposti non adeguatamente hardenizzati**;
- manchino sistemi di **monitoraggio o rilevamento delle attività anomale interne**.

Alla luce di tali considerazioni, il livello di rischio complessivo associato all'attività osservata può essere classificato come **medio**. Sebbene non siano state rilevate compromissioni riuscite, la natura e la modalità dell'attività indicano un **potenziale vettore di minaccia** che, in assenza di adeguate contromisure, potrebbe evolvere in un attacco più avanzato.

8. Azioni di Mitigazione Raccomandate

Le azioni di mitigazione proposte sono state definite sulla base degli Indicatori di Compromissione individuati, della fase della kill chain raggiunta e del livello di rischio stimato. Poiché l'attività osservata risulta confinata alla fase di ricognizione, le contromisure suggerite mirano sia a **ridurre l'impatto immediato**, sia a **prevenire l'evoluzione verso fasi di attacco più avanzate**.

8.1 Azioni immediate

Si raccomanda di intraprendere le seguenti azioni a breve termine:

- **Analisi approfondita degli host coinvolti**, con particolare attenzione ai sistemi che hanno avviato i tentativi di connessione, al fine di escludere una compromissione pregressa;
- **Verifica dei processi e dei servizi attivi** sugli host, per individuare eventuali strumenti di scansione o software non autorizzati;
- **Raccolta e conservazione dei log di rete**, utili per eventuali analisi forensi successive.

Tali azioni consentono di confermare se l'attività osservata sia riconducibile a un comportamento malevolo o a un'anomalia operativa interna.

8.2 Azioni di mitigazione a breve termine

Per ridurre la probabilità di ripetizione dell'evento e limitarne l'impatto, si raccomanda di:

- **Rafforzare le regole di filtraggio del traffico interno**, limitando le comunicazioni non necessarie tra host appartenenti alla stessa rete;
- **Implementare meccanismi di rilevamento del port scanning**, attraverso sistemi IDS/IPS o regole di monitoraggio dedicate;
- **Ridurre l'esposizione dei servizi di rete**, disabilitando quelli non necessari o applicando configurazioni di hardening adeguate.

Queste misure permettono di intercettare tempestivamente attività di ricognizione e di ridurre la superficie di attacco complessiva.

8.3 Azioni preventive a lungo termine

In ottica di prevenzione strutturale, si suggerisce di:

- **Segmentare la rete** per limitare la visibilità laterale e contenere eventuali compromissioni;
- Applicare il principio di **least privilege** anche a livello di rete, consentendo esclusivamente le comunicazioni strettamente necessarie;
- **Centralizzare il monitoraggio del traffico e dei log**, migliorando la capacità di individuare pattern anomali ricorrenti;
- Sensibilizzare il personale tecnico sull'importanza del **monitoraggio delle attività interne**, spesso sottovalutate rispetto al traffico perimetrale.

Queste azioni contribuiscono a rafforzare la postura di sicurezza complessiva e a ridurre l'efficacia di future attività di ricognizione.

9. Conclusione

L'analisi della cattura di traffico di rete ha evidenziato un'attività riconducibile a una **scansione TCP automatizzata** condotta all'interno della rete locale. I pattern osservati, caratterizzati da tentativi di connessione verso porte multiple, terminazioni immediate delle comunicazioni e assenza di traffico applicativo, risultano coerenti con una **fase di ricognizione** finalizzata alla mappatura della superficie di attacco.

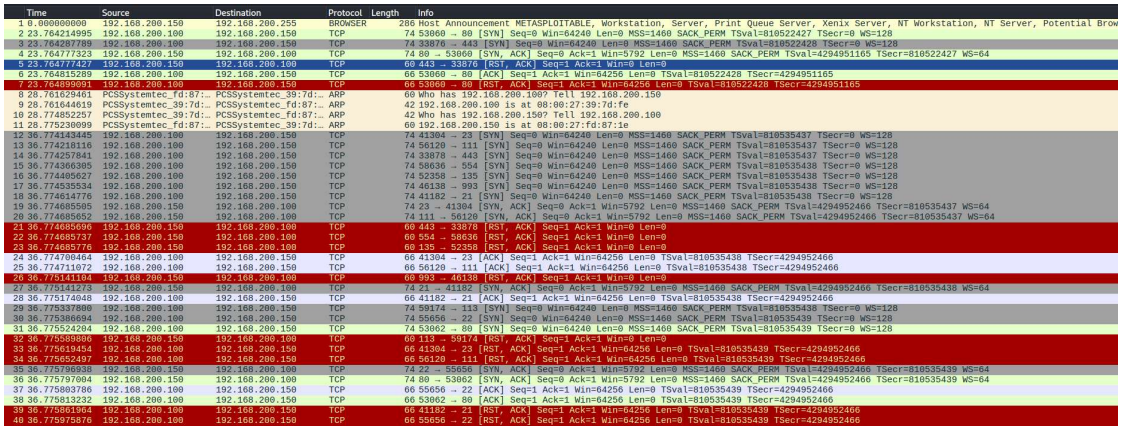
Sebbene in alcuni casi il **three-way handshake TCP** risulti completato, le connessioni osservate sono **estremamente brevi** e **prive di interazione applicativa**, escludendo evidenze di sfruttamento o compromissione riuscita. Nel complesso, l'attività non ha superato la fase preliminare dell'attacco, ma rappresenta un **potenziale rischio** qualora non adeguatamente monitorata e mitigata.

Le contromisure proposte mirano pertanto a **ridurre la superficie di attacco**, migliorare la **capacità di rilevamento delle attività anomale** e prevenire l'evoluzione di eventi simili verso fasi più avanzate della kill chain.

Appendice A – Evidenze Tecniche (Cattura Wireshark)

La presente appendice raccoglie gli **screenshot più significativi** estratti dalla cattura di traffico analizzata, a supporto delle evidenze descritte nelle sezioni precedenti del report.
Le immagini sono fornite a titolo **documentale**, al fine di dimostrare i pattern di traffico osservati e gli **Indicatori di Compromissione (IOC)** individuati.

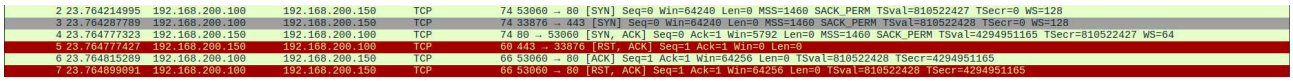
Figura A.1 – Vista generale dell'attività di scansione TCP



	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 Workstation, NT Server, Potential Brow
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

Vista complessiva del traffico di rete tra i due host coinvolti, caratterizzata da numerosi tentativi di connessione TCP verso porte multiple. È visibile il pattern ricorrente di pacchetti SYN seguiti da risposte RST/ACK, indicativo di un'attività di scansione delle porte.

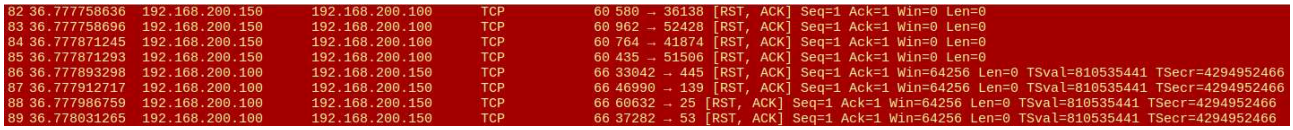
Figura A.2 – Completamento del three-way handshake TCP (porta 80)



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

Sequenza di pacchetti relativa alla porta 80, in cui si osserva il completamento del three-way handshake TCP (SYN, SYN/ACK, ACK), seguito da una chiusura immediata della connessione senza alcuno scambio di traffico applicativo.

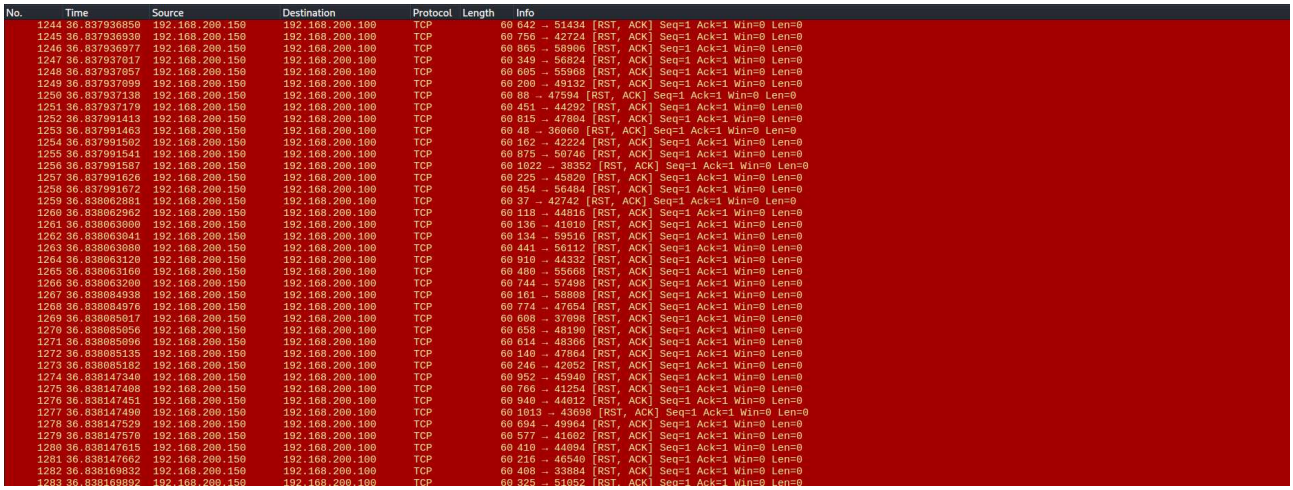
Figura A.3 – Terminazione volontaria delle connessioni TCP



82	36.777758636	192.168.200.150	192.168.200.100	TCP	60 580 → 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	36.777871245	192.168.200.150	192.168.200.100	TCP	60 764 → 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85	36.777871293	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	66 33042 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
87	36.777912717	192.168.200.100	192.168.200.150	TCP	66 46990 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
88	36.777986759	192.168.200.100	192.168.200.150	TCP	66 60632 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
89	36.778031265	192.168.200.100	192.168.200.150	TCP	66 37282 → 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466

Evidenza di pacchetti RST/ACK inviati anche dall'host che avvia il tentativo di connessione, indicativi di una terminazione volontaria delle sessioni TCP dopo la verifica della disponibilità dei servizi, comportamento tipico di strumenti di scansione automatizzata.

Figura A.4 – Fase finale dell'attività di scansione



No.	Time	Source	Destination	Protocol	Length	Info
1244	36.837936850	192.168.200.150	192.168.200.100	TCP	60	642 → 51434 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1245	36.837936930	192.168.200.150	192.168.200.100	TCP	60	756 → 42724 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1246	36.837936977	192.168.200.150	192.168.200.100	TCP	60	865 → 58906 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1247	36.837937017	192.168.200.150	192.168.200.100	TCP	60	349 → 56824 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1248	36.837937057	192.168.200.150	192.168.200.100	TCP	60	605 → 55968 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1249	36.837937099	192.168.200.150	192.168.200.100	TCP	60	200 → 49132 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1250	36.837937138	192.168.200.150	192.168.200.100	TCP	60	88 → 47594 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1251	36.837937179	192.168.200.150	192.168.200.100	TCP	60	451 → 44292 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1252	36.837991413	192.168.200.150	192.168.200.100	TCP	60	815 → 47804 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1253	36.837991463	192.168.200.150	192.168.200.100	TCP	60	48 → 36060 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1254	36.837991502	192.168.200.150	192.168.200.100	TCP	60	162 → 42224 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1255	36.837991541	192.168.200.150	192.168.200.100	TCP	60	875 → 50746 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1256	36.837991587	192.168.200.150	192.168.200.100	TCP	60	1022 → 38352 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1257	36.837991626	192.168.200.150	192.168.200.100	TCP	60	225 → 45820 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1258	36.837991672	192.168.200.150	192.168.200.100	TCP	60	454 → 56484 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1259	36.838062881	192.168.200.150	192.168.200.100	TCP	60	37 → 42742 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1260	36.838062962	192.168.200.150	192.168.200.100	TCP	60	118 → 44816 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1261	36.838063000	192.168.200.150	192.168.200.100	TCP	60	136 → 41010 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1262	36.838063041	192.168.200.150	192.168.200.100	TCP	60	134 → 59516 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1263	36.838063080	192.168.200.150	192.168.200.100	TCP	60	441 → 56112 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1264	36.838063120	192.168.200.150	192.168.200.100	TCP	60	910 → 44332 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1265	36.838063160	192.168.200.150	192.168.200.100	TCP	60	480 → 55668 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1266	36.838063200	192.168.200.150	192.168.200.100	TCP	60	744 → 57498 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1267	36.838084938	192.168.200.150	192.168.200.100	TCP	60	161 → 58808 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1268	36.838084976	192.168.200.150	192.168.200.100	TCP	60	774 → 47654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1269	36.838085017	192.168.200.150	192.168.200.100	TCP	60	608 → 37098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1270	36.838085056	192.168.200.150	192.168.200.100	TCP	60	658 → 48190 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1271	36.838085096	192.168.200.150	192.168.200.100	TCP	60	614 → 48366 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1272	36.838085135	192.168.200.150	192.168.200.100	TCP	60	140 → 47864 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1273	36.838085182	192.168.200.150	192.168.200.100	TCP	60	246 → 42052 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1274	36.838147340	192.168.200.150	192.168.200.100	TCP	60	952 → 45940 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1275	36.838147408	192.168.200.150	192.168.200.100	TCP	60	766 → 41254 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1276	36.838147451	192.168.200.150	192.168.200.100	TCP	60	940 → 44012 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1277	36.838147490	192.168.200.150	192.168.200.100	TCP	60	1013 → 43608 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1278	36.838147529	192.168.200.150	192.168.200.100	TCP	60	694 → 49964 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1279	36.838147570	192.168.200.150	192.168.200.100	TCP	60	577 → 41602 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1280	36.838147615	192.168.200.150	192.168.200.100	TCP	60	410 → 44094 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1281	36.838147662	192.168.200.150	192.168.200.100	TCP	60	216 → 46540 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1282	36.838169832	192.168.200.150	192.168.200.100	TCP	60	408 → 33884 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1283	36.838169882	192.168.200.150	192.168.200.100	TCP	60	325 → 51052 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Porzione della cattura caratterizzata da una sequenza densa e ripetitiva di pacchetti RST/ACK associati a porte di destinazione differenti. Il comportamento risulta stabile nel tempo e privo di traffico applicativo, confermando la natura automatizzata dell'attività e l'assenza di evoluzione verso fasi di sfruttamento.