

Threat Intelligence & IOC

In base all'analisi di Wireshark si possono notare due tipi di attacco principale:

- Reset con ACK che tenta di interrompere le connessioni esistenti con le porte chiuse(1026 pacchetti) senza connessioni SYN

No.	Time	Source	Destination	Protocol	Length	Info
5.23	7.64777427	192.168.200.150	192.168.200.100	TCP	60	443 - 3876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7.23	7.64809991	192.168.200.100	192.168.200.150	TCP	60	53060 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810522428 TSecr=4294951105
21.36	7.74685696	192.168.200.150	192.168.200.100	TCP	60	443 - 3876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22.36	7.74685737	192.168.200.150	192.168.200.100	TCP	60	554 - 58036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23.36	7.74685776	192.168.200.150	192.168.200.100	TCP	60	135 - 52368 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26.36	7.75141104	192.168.200.150	192.168.200.100	TCP	60	993 - 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
32.36	7.75589806	192.168.200.150	192.168.200.100	TCP	60	113 - 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33.36	7.75614554	192.168.200.100	192.168.200.150	TCP	60	41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535439 TSecr=4294952466
34.36	7.75652497	192.168.200.100	192.168.200.150	TCP	60	56120 - 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535439 TSecr=4294952466
39.36	7.75861964	192.168.200.100	192.168.200.150	TCP	60	41182 - 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535439 TSecr=4294952466
40.36	7.75975876	192.168.200.100	192.168.200.150	TCP	60	55566 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535439 TSecr=4294952466
41.36	7.76451357	192.168.200.150	192.168.200.100	TCP	60	53062 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535439 TSecr=4294952466
47.36	7.76451284	192.168.200.150	192.168.200.100	TCP	60	199 - 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48.36	7.76451357	192.168.200.150	192.168.200.100	TCP	60	995 - 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
55.36	7.76813123	192.168.200.150	192.168.200.100	TCP	60	587 - 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58.36	7.76904922	192.168.200.150	192.168.200.100	TCP	60	256 - 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
60.36	7.76905084	192.168.200.150	192.168.200.100	TCP	60	143 - 33286 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
62.36	7.76905082	192.168.200.150	192.168.200.100	TCP	60	110 - 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
64.36	7.76905102	192.168.200.150	192.168.200.100	TCP	60	580 - 54888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
69.36	7.77151488	192.168.200.100	192.168.200.150	TCP	60	407 - 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
74.36	7.77438632	192.168.200.150	192.168.200.100	TCP	60	797 - 56900 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75.36	7.77438741	192.168.200.150	192.168.200.100	TCP	60	436 - 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
78.36	7.77432302	192.168.200.150	192.168.200.100	TCP	60	96 - 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79.36	7.77623149	192.168.200.150	192.168.200.100	TCP	60	78 - 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
82.36	7.77758636	192.168.200.150	192.168.200.100	TCP	60	580 - 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83.36	7.77758696	192.168.200.150	192.168.200.100	TCP	60	962 - 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84.36	7.77871245	192.168.200.150	192.168.200.100	TCP	60	764 - 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85.36	7.77871293	192.168.200.150	192.168.200.100	TCP	60	435 - 51586 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86.36	7.77893298	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	7.77912717	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	7.77980759	192.168.200.100	192.168.200.150	TCP	60	69632 - 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535441 TSecr=4294952466
89.36	7.78031265	192.168.200.100	192.168.200.150	TCP	60	37202 - 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535441 TSecr=4294952466
93.36	7.78358546	192.168.200.150	192.168.200.100	TCP	60	148 - 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94.36	7.78358548	192.168.200.150	192.168.200.100	TCP	60	880 - 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95.36	7.78448494	192.168.200.150	192.168.200.100	TCP	60	221 - 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
99.36	7.78663964	192.168.200.150	192.168.200.100	TCP	60	1007 - 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
100.36	7.78721888	192.168.200.150	192.168.200.100	TCP	60	286 - 34640 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
103.36	7.78826294	192.168.200.150	192.168.200.100	TCP	60	131 - 54202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
105.36	7.78939327	192.168.200.150	192.168.200.100	TCP	60	392 - 40318 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
106.36	7.78939427	192.168.200.150	192.168.200.100	TCP	60	677 - 51270 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
108.36	7.79026210	192.168.200.150	192.168.200.100	TCP	60	656 - 39566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
110.36	7.79122299	192.168.200.150	192.168.200.100	TCP	60	84 - 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
112.36	7.79252884	192.168.200.150	192.168.200.100	TCP	60	807 - 56542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

- SYN Flood con spoofing delle porte si capisce perché ci sono molteplici pacchetti TCP con il flag SYN senza avere una risposta ACK(1039 pacchetti) ,

No.	Time	Source	Destination	Protocol	Length	Info
5.23	7.64777427	192.168.200.150	192.168.200.100	TCP	60	443 - 3876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6.23	7.64815289	192.168.200.100	192.168.200.150	TCP	60	53060 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810522428 TSecr=4294951105
7.23	7.64830293	192.168.200.100	192.168.200.150	TCP	60	53060 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810522428 TSecr=4294951105
21.36	7.74685696	192.168.200.150	192.168.200.100	TCP	60	443 - 3876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22.36	7.74685737	192.168.200.150	192.168.200.100	TCP	60	554 - 58036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23.36	7.74685776	192.168.200.150	192.168.200.100	TCP	60	135 - 52368 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24.36	7.74700464	192.168.200.100	192.168.200.150	TCP	60	41304 - 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535438 TSecr=4294952466
25.36	7.74711072	192.168.200.100	192.168.200.150	TCP	60	56120 - 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535438 TSecr=4294952466
28.36	7.75174048	192.168.200.100	192.168.200.150	TCP	60	41182 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535438 TSecr=4294952466
32.36	7.75589806	192.168.200.150	192.168.200.100	TCP	60	113 - 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33.36	7.75614554	192.168.200.100	192.168.200.150	TCP	60	41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535439 TSecr=4294952466
34.36	7.75652497	192.168.200.100	192.168.200.150	TCP	60	56120 - 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535439 TSecr=4294952466
37.36	7.75803786	192.168.200.100	192.168.200.150	TCP	60	55566 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535439 TSecr=4294952466
38.36	7.75913233	192.168.200.100	192.168.200.150	TCP	60	53062 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535439 TSecr=4294952466
39.36	7.75861964	192.168.200.100	192.168.200.150	TCP	60	41182 - 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535439 TSecr=4294952466
40.36	7.75975876	192.168.200.100	192.168.200.150	TCP	60	55566 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535439 TSecr=4294952466
41.36	7.76085853	192.168.200.150	192.168.200.100	TCP	60	53062 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535439 TSecr=4294952466
47.36	7.76451284	192.168.200.150	192.168.200.100	TCP	60	199 - 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48.36	7.76451357	192.168.200.150	192.168.200.100	TCP	60	995 - 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
55.36	7.76813123	192.168.200.150	192.168.200.100	TCP	60	587 - 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58.36	7.76904922	192.168.200.150	192.168.200.100	TCP	60	256 - 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
60.36	7.76905084	192.168.200.150	192.168.200.100	TCP	60	143 - 33286 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
62.36	7.76905082	192.168.200.150	192.168.200.100	TCP	60	110 - 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
64.36	7.76905102	192.168.200.150	192.168.200.100	TCP	60	580 - 54888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65.36	7.76914172	192.168.200.100	192.168.200.150	TCP	60	33042 - 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535440 TSecr=4294952466
66.36	7.76942020	192.168.200.100	192.168.200.150	TCP	60	46990 - 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535440 TSecr=4294952466
67.36	7.76962320	192.168.200.100	192.168.200.150	TCP	60	69632 - 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535440 TSecr=4294952466
68.36	7.76983878	192.168.200.100	192.168.200.150	TCP	60	37202 - 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535440 TSecr=4294952466
69.36	7.77141343	192.168.200.150	192.168.200.100	TCP	60	131 - 54202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
74.36	7.77438632	192.168.200.150	192.168.200.100	TCP	60	797 - 56900 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75.36	7.77438741	192.168.200.150	192.168.200.100	TCP	60	436 - 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
78.36	7.77432302	192.168.200.150	192.168.200.100	TCP	60	96 - 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79.36	7.77623149	192.168.200.150	192.168.200.100	TCP	60	78 - 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
82.36	7.77758636	192.168.200.150	192.168.200.100	TCP	60	580 - 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83.36	7.77758696	192.168.200.150	192.168.200.100	TCP	60	962 - 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84.36	7.77871245	192.168.200.150	192.168.200.100	TCP	60	764 - 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85.36	7.77871293	192.168.200.150	192.168.200.100	TCP	60	435 - 51586 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86.36	7.77893298	192.168.200.100	192.168.200.150	TCP	60	33042 - 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535441 TSecr=4294952466
87.36	7.77912717	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	7.77980759	192.168.200.100	192.168.200.150	TCP	60	69632 - 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535441 TSecr=4294952466
89.36	7.78031265	192.168.200.100	192.168.200.150	TCP	60	37202 - 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535441 TSecr=4294952466
93.36	7.78358546	192.168.200.150	192.168.200.100	TCP	60	148 - 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

- Indirizzi ip: 192.168.200.100(source) 192.168.200.150(destination)
- porte scansionate: tutte le porte

- pacchetti SYN ACK andati a buona fine

No.	Time	Source	Destination	Protocol	Length	Info
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=4294952466 TSecr=810535437 WS=64
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74	23 → 41384 [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
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
35	36.775780938	192.168.200.150	192.168.200.100	TCP	74	22 → 55056 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
36	36.775797084	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
57	36.776984628	192.168.200.150	192.168.200.100	TCP	74	445 → 33842 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
59	36.776984961	192.168.200.150	192.168.200.100	TCP	74	139 → 46900 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
61	36.776985043	192.168.200.150	192.168.200.100	TCP	74	25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
63	36.776985123	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 TSval=4294952466 TSecr=810535440 WS=64
164	36.781487210	192.168.200.150	192.168.200.100	TCP	74	512 → 45648 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535445 WS=64
267	36.788885940	192.168.200.150	192.168.200.100	TCP	74	514 → 51306 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952467 TSecr=810535452 WS=64
994	36.825722553	192.168.200.150	192.168.200.100	TCP	74	513 → 42048 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952471 TSecr=810535489 WS=64

Da qui si evince che molto sicuramente è un attacco di brute force, probabilmente l'attacco è partito con l'utilizzo da un nmap utilizzando una scansione molto aggressiva come -sV. Ipotesi questa soluzione perché utilizzano un RST accompagnato da ACK che rifiuta tutte le connessioni con le porte chiuse mentre quelle aperte le accetta.

Azioni per mitigare l'attacco attuale:

- Abilitare il Rate Limiting: configurando il Firewall o router per limitare il numero di richieste SYN e RST da una singola attività
- Filtraggio dei Pacchetti Anomali: inserendo delle regole nel Firewall per rifiutare pacchetti SYN e RST non richiesti o che provengono da indirizzi IP sconosciuti
- Attivare il SYN Cookie: per ridurre l'impatto degli attacchi SYN flood
- Utilizzare un Sistema di Prevenzione delle Intrusioni (IPS): per monitorare e bloccare traffico sospetto, compresi gli attacchi SYN e RST flood.
- Contattare il Fornitore di Servizi Internet (ISP): potrebbero essere in grado di bloccare il traffico malevolo prima che raggiunga la tua rete.

Azioni per prevenire attacchi futuri:

- Chiudi le porte non necessarie: Mantieni aperte solo le porte essenziali per il funzionamento dei servizi richiesti. Questo riduce le possibilità per gli attaccanti di scoprire servizi vulnerabili.
- Usa porte non standard: Sposta i servizi su porte non standard per ridurre la probabilità che vengano scansionate da strumenti automatici come Nmap.
- Blocco degli IP sospetti: Blocca l'accesso agli IP che mostrano comportamenti sospetti, come scansioni ripetitive.
- Rate limiting: Imposta dei limiti sul numero di connessioni che un singolo IP può stabilire in un determinato periodo.
- Geoblocking: Se appropriato, limita l'accesso da regioni geografiche non rilevanti per il tuo business.
- Configura un IDS o IPS come Snort, Suricata, o Zeek per rilevare e prevenire scansioni di rete e attività sospette.
- Imposta regole specifiche per rilevare le firme delle scansioni di Nmap e bloccare automaticamente il traffico proveniente da queste sorgenti.
- Imposta honeypots o honeynets che simulano servizi vulnerabili per attirare e monitorare attività di scansione. Questo ti permette di raccogliere dati sugli attaccanti senza esporre sistemi reali.