

No.	Time	Source	Destination	Protocol	Length	Info
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	36.774366395	192.168.200.100	192.168.200.150	TCP	74	56536 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16	36.774405027	192.168.200.100	192.168.200.150	TCP	74	52328 → 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	36.774685905	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
21	36.774685690	192.168.200.150	192.168.200.100	TCP	66	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	66	443 → 56536 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	66	135 → 52328 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774708464	192.168.200.100	192.168.200.150	TCP	66	41384 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711872	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	36.774811103	192.168.200.150	192.168.200.100	TCP	66	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	36.775174848	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	36.775337899	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	36.775396694	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	36.775524284	192.168.200.100	192.168.200.150	TCP	74	53662 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
32	36.775598880	192.168.200.150	192.168.200.100	TCP	66	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	41384 → 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	36.775797064	192.168.200.150	192.168.200.100	TCP	74	80 → 53662 [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	53662 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.775861904	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	36.775979076	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	36.776085853	192.168.200.100	192.168.200.150	TCP	66	53662 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
42	36.776179338	192.168.200.100	192.168.200.150	TCP	74	59684 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
43	36.776233889	192.168.200.100	192.168.200.150	TCP	74	54220 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
44	36.776339610	192.168.200.100	192.168.200.150	TCP	74	34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
45	36.776385694	192.168.200.100	192.168.200.150	TCP	74	33842 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
46	36.776402509	192.168.200.100	192.168.200.150	TCP	74	49814 → 250 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
47	36.776451324	192.168.200.150	192.168.200.100	TCP	66	193 → 59684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	36.776451357	192.168.200.150	192.168.200.100	TCP	66	995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	36.776478261	192.168.200.100	192.168.200.150	TCP	74	46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
50	36.776486366	192.168.200.100	192.168.200.150	TCP	74	33286 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
51	36.776512221	192.168.200.100	192.168.200.150	TCP	74	69632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
52	36.776568686	192.168.200.100	192.168.200.150	TCP	74	49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
53	36.776671271	192.168.200.100	192.168.200.150	TCP	74	37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
54	36.776728715	192.168.200.100	192.168.200.150	TCP	74	54098 → 680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
55	36.776813123	192.168.200.150	192.168.200.100	TCP	66	587 → 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56	36.776843423	192.168.200.150	192.168.200.100	TCP	74	51534 → 487 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128

Analizzando i dati forniti dalla cattura effettuata tramite Wireshark, possiamo notare come l'IP 192.168.200.100 stia tentando di effettuare delle connessioni TCP verso diverse porte dell'IP 192.168.200.150, il quale si trova nella stessa rete.

Analizzando gli IOC (Indicator of Compromise), possiamo notare come L'IP sorgente interrompa la connessione una volta che il server gli ha dato la disponibilità alla connessione, non permettendo di effettuare così una connessione TCP completa.

Questo suggerirebbe, ad esempio, un attacco di scansione delle porte utilizzando il SYN Scan (Half-Open Scan) di Nmap.

Questa tecnica invia un pacchetto SYN per iniziare una connessione, ma non completa il "three-way handshake". Questo può essere fatto con Nmap usando l'opzione -sS.

Non completando la connessione, l'attaccante riduce la probabilità di essere rilevato dai sistemi di sicurezza e dai log del server. Questo approccio permette di ottenere informazioni sulle porte aperte senza compromettere la propria anonimità. Non completare la connessione significa che l'attaccante può scansionare molte porte in un breve lasso di tempo. La scansione di porte SYN richiede meno risorse rispetto all'apertura di connessioni TCP complete. La mancata completa connessione lascia meno tracce nei log di rete, rendendo più difficile per gli amministratori di rete identificare la scansione come un'attività sospetta

No.	Time	Source	Destination	Protocol	Length	Info
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
21	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	36.775174848	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
39	36.775861904	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

Prendendo come esempio un tentativo di connessione alla porta 21 (nello screenshot qui sopra), possiamo notare come L'IP sorgente invii una richiesta di connessione (SYN), ricevendo una risposta dall'IP destinatario (SYN, ACK). A quel punto, l'IP sorgente sembra voler continuare il tentativo di connessione (ACK), ma subito dopo interrompe la connessione (RST, ACK), evitando così di effettuare una connessione completa. Per giungere alla conclusione che un servizio su una porta sia attivo, gli basta che il server gli risponda in modo positivo al tentativo di connessione.

Azioni Immediate per Ridurre l'Impatto dell'Attacco Attuale

1. Monitoraggio del Traffico di Rete:

Utilizzo di strumenti di monitoraggio della rete per identificare il traffico sospetto. Analisi dei log dei firewall e dei router per rilevare un aumento anomalo delle richieste SYN.

2. Bloccare l'Indirizzo IP Attaccante:

Per evitare ulteriori attacchi da un determinato IP, se questo è identificabile, lo si può bloccare tramite regole di firewall.

3. Aumentare le Regole di Timeout:

Aumentare il timeout dei pacchetti SYN, così da limitare la possibilità di stabilire una connessione in caso di scansione rapida.

4. Aggiornare e Configurare i Firewall:

Configurare i firewall correttamente per gestire le richieste SYN. Alcuni firewall possono bloccare automaticamente le scansioni delle porte o implementare il rate limiting per ridurre la velocità delle richieste.

Azioni a Lungo Termine per Prevenire Attacchi Futuri

1. Segmentazione della Rete:

Implementare una segmentazione della rete per limitare l'accesso a determinate risorse. Ciò può rendere più difficile per un attaccante effettuare una scansione efficace dell'intera rete.

2. Implementare IDS/IPS:

Utilizzare sistemi IDS/IPS per monitorare e rispondere a comportamenti sospetti in tempo reale. Questi sistemi possono rilevare modelli di scansione e rispondere automaticamente.

3. Educazione e Formazione del Personale:

Formare il personale IT e i team di sicurezza riguardo le tecniche di scansione delle porte e le best practice di sicurezza.

4. Regole di Rate Limiting:

Implementare politiche di rate limiting sui firewall per limitare il numero di richieste SYN che un singolo IP può inviare in un determinato intervallo di tempo.