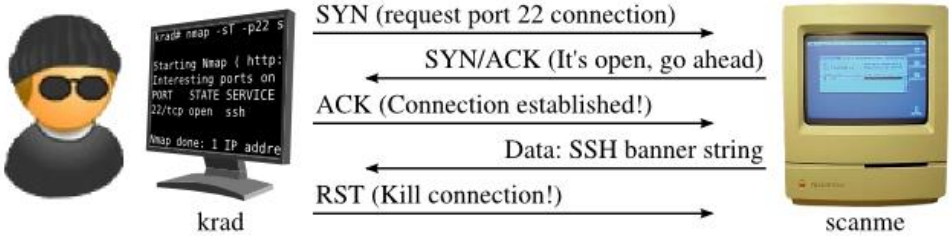
La tipologia di attacco in corso è uno scan di nmap/nessus per un port scanning massivo. La tipologia utilizzata è la -sS che, cito testualmente dal sito di nmap.org “è spesso indicata come "scanning semi-aperto" (tradotto letteralmente per esigenze di comprensione, da "half-open scanning", NdT), perché non viene aperta una connessione TCP completa. Viene mandato un pacchetto SYN come se si fosse sul punto di aprire una connessione reale e si attende una risposta. Un SYN/ACK indica che la porta è in ascolto (aperta), mentre un RST (reset) indica che la porta non è in ascolto. Se non viene ricevuta nessuna risposta dopo diverse ritrasmissioni la porta viene marcata come filtrata. La porta viene marcata come tale anche se viene ricevuto un pacchetto di errore "ICMP unreachable" (tipo 3, codici 1, 2, 3, 9, 10, 13). La porta viene considerata aperta anche nel caso in cui un pacchetto SYN (senza il flag ACK) viene ricevuto in risposta. Questo in base ad una feature TCP estremamente rara conosciuta come "apertura simultanea" ("simultaneous open") o connessione "split handshake".



Al solito, per prevenire eventuali scansioni, intrusioni o attacchi possiamo implementare le seguenti misure di sicurezza:

Monitoraggio costante: un sistema di monitoraggio continuo per rileva e risponde tempestivamente alle scansioni e agli attacchi.

Firewall: Configurare un firewall robusto per limitare l'accesso non autorizzato ai tuoi sistemi e filtrare il traffico di rete indesiderato. I firewall possono bloccare determinati tipi di scansioni o limitare il numero di connessioni per evitare scansioni di port scanning e vulnerabilità.

Configurazione sicura: Questo include l'implementazione di politiche di sicurezza solide, l'uso di password complesse e l'aggiornamento regolare dei software e delle patch di sicurezza.

Protezione dei servizi esposti: Se si hanno servizi o applicazioni esposte su Internet, vanno adottate misure per proteggerli, come, ad esempio, utilizzare protocolli crittografici come HTTPS, autenticazione forte, limitazione dei tentativi di accesso e controlli di accesso basati sull'indirizzo IP.

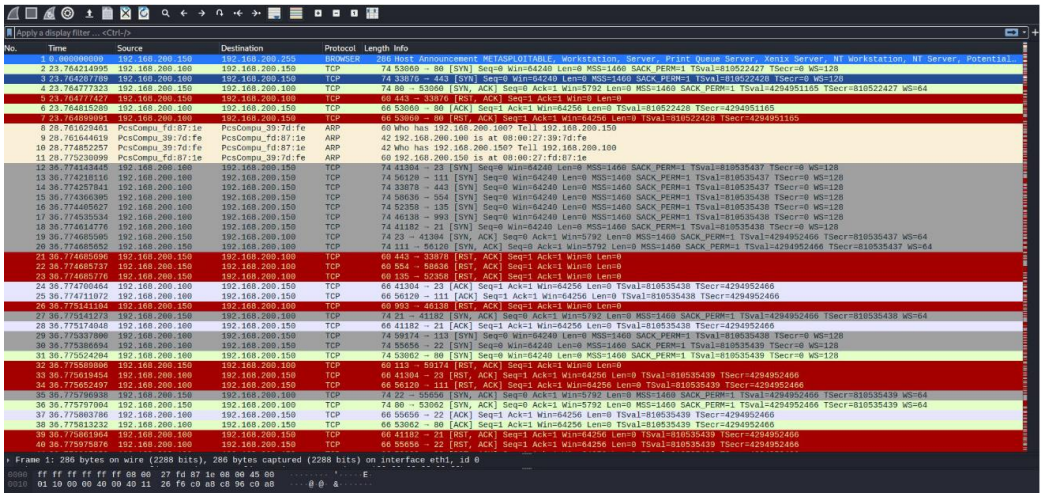
Isolamento dei sistemi: Assicurarsi che i tuoi sistemi siano adeguatamente isolati l'uno dall'altro. Utilizzare reti virtuali private (VPN), sottoreti o segmentazione di rete per separare i sistemi sensibili da quelli non critici. In questo modo, anche se una scansione rileva una vulnerabilità su un sistema, sarà più difficile che l'attacco si propaghi ad altri.

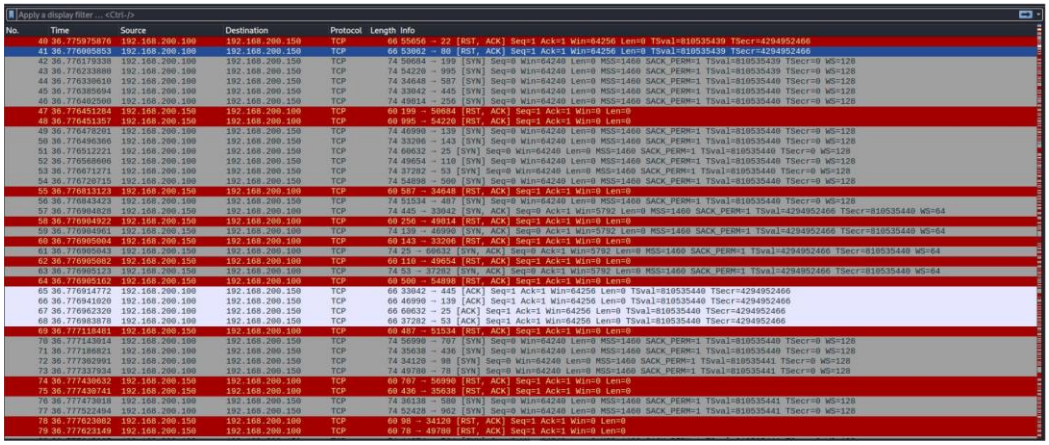
Test di sicurezza: Effettuare regolarmente test di vulnerabilità e penetrazione sui tuoi sistemi per identificare e risolvere le potenziali debolezze prima che possano essere sfruttate da attaccanti. I test possono includere scansione delle vulnerabilità, test di penetrazione e valutazioni della sicurezza dell'applicazione.

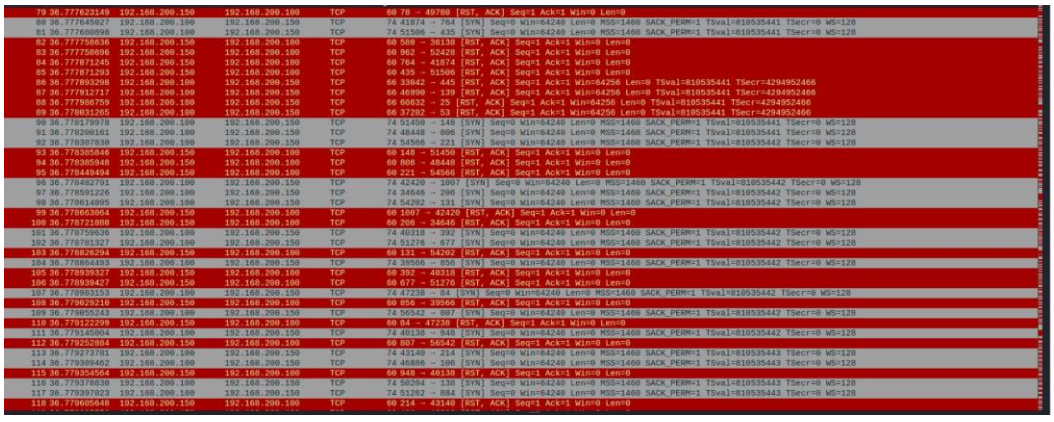
Informazione e consapevolezza degli utenti: Sensibilizzare gli utenti alle migliori pratiche di sicurezza informatica. I dipendenti devono essere consapevoli dei rischi legati alle scansioni e alle vulnerabilità e adottare comportamenti sicuri come l'utilizzo di password complesse, la verifica delle fonti di comunicazione e il riconoscimento di tentativi di phishing.

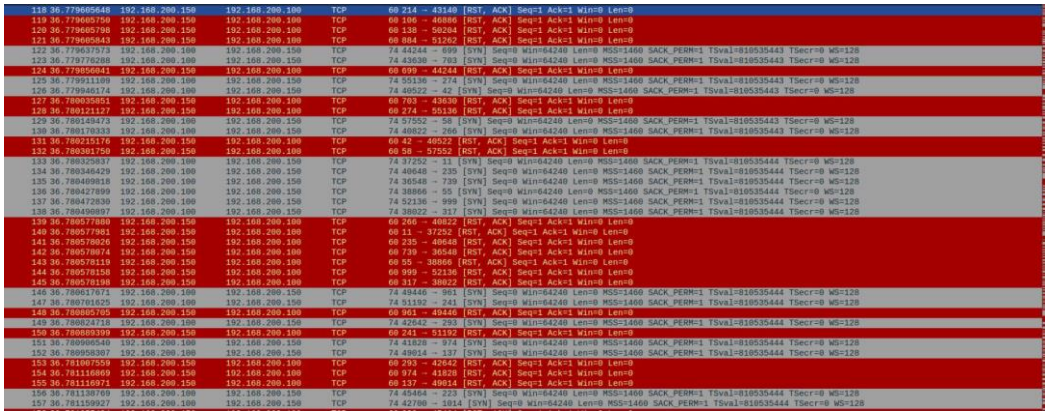
Aggiornamenti regolari: Assicurarsi di tenere aggiornati i tuoi sistemi operativi, software e applicazioni con le ultime patch di sicurezza. Le vulnerabilità note vengono spesso risolte tramite questi aggiornamenti, riducendo la probabilità che gli attaccanti possano sfruttarle.

Protezione avanzata: Considera l'utilizzo di soluzioni di sicurezza avanzate come sistemi di rilevamento delle intrusioni (IDS), sistemi di prevenzione delle intrusioni (IPS) e sistemi di rilevamento delle anomalie per rilevare scansioni e attacchi più sofisticati.









```
118 36.779605648  192.168.200.150  192.168.200.100  TCP  60 214 → 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119 36.779605750  192.168.200.150  192.168.200.100  TCP  60 106 → 46886 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
120 36.779605798  192.168.200.150  192.168.200.100  TCP  60 138 → 50204 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
121 36.779605843  192.168.200.150  192.168.200.100  TCP  60 884 → 51262 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
122 36.779637573  192.168.200.100  192.168.200.150  TCP  74 44244 → 699 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
123 36.779776288  192.168.200.100  192.168.200.150  TCP  74 43630 → 703 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
124 36.779856041  192.168.200.150  192.168.200.100  TCP  60 699 → 44244 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
125 36.779911100  192.168.200.100  192.168.200.150  TCP  74 55136 → 274 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
126 36.779946174  192.168.200.100  192.168.200.150  TCP  74 49522 → 42 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
127 36.780035851  192.168.200.150  192.168.200.100  TCP  60 703 → 43630 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
128 36.780121127  192.168.200.150  192.168.200.100  TCP  60 274 → 55136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
129 36.780145472  192.168.200.100  192.168.200.150  TCP  74 57552 → 58 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
130 36.780170333  192.168.200.100  192.168.200.150  TCP  74 40822 → 266 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
131 36.780215176  192.168.200.150  192.168.200.100  TCP  60 42 → 49522 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
132 36.780301750  192.168.200.150  192.168.200.100  TCP  60 58 → 57552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
133 36.780325837  192.168.200.100  192.168.200.150  TCP  74 37252 → 11 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
134 36.780346429  192.168.200.100  192.168.200.150  TCP  74 40648 → 235 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
135 36.780409818  192.168.200.100  192.168.200.150  TCP  74 36548 → 739 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
136 36.780427899  192.168.200.100  192.168.200.150  TCP  74 38866 → 55 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
137 36.780472830  192.168.200.100  192.168.200.150  TCP  74 52136 → 999 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
138 36.780490897  192.168.200.100  192.168.200.150  TCP  74 38022 → 317 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
139 36.780517880  192.168.200.150  192.168.200.100  TCP  60 266 → 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
140 36.780577801  192.168.200.150  192.168.200.100  TCP  60 11 → 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
141 36.780578026  192.168.200.150  192.168.200.100  TCP  60 235 → 40648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
142 36.780578074  192.168.200.150  192.168.200.100  TCP  60 739 → 36548 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
143 36.780578119  192.168.200.150  192.168.200.100  TCP  60 55 → 38866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
144 36.780578158  192.168.200.150  192.168.200.100  TCP  60 999 → 52136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
145 36.780578198  192.168.200.150  192.168.200.100  TCP  60 317 → 38022 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
146 36.780617671  192.168.200.100  192.168.200.150  TCP  74 49446 → 961 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
147 36.780701625  192.168.200.100  192.168.200.150  TCP  74 51192 → 241 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
148 36.780805705  192.168.200.150  192.168.200.100  TCP  60 961 → 49446 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
149 36.780824718  192.168.200.100  192.168.200.150  TCP  74 42642 → 293 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
150 36.780889390  192.168.200.150  192.168.200.100  TCP  60 241 → 51192 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
151 36.780960540  192.168.200.100  192.168.200.150  TCP  74 41828 → 974 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
152 36.780958307  192.168.200.100  192.168.200.150  TCP  74 49014 → 137 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
153 36.781007559  192.168.200.150  192.168.200.100  TCP  60 293 → 42642 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
154 36.781116869  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 → 49014 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
156 36.781138769  192.168.200.100  192.168.200.150  TCP  74 45464 → 223 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
157 36.781159927  192.168.200.100  192.168.200.150  TCP  74 42780 → 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
```