# Relazione sull'Analisi del Traffico di Rete

## Introduzione

Nel corso dell'analisi del traffico di rete acquisito, è stato identificato un comportamento sospetto che suggerisce un attacco di Port Scanning, con l'indirizzo IP 192.168.200.100 che invia pacchetti SYN a una serie di porte casuali sul server di destinazione 192.168.200.150. L'intento di questa scansione sembra essere quello di raccogliere informazioni sulle porte aperte del server, senza completare effettivamente le connessioni. La presenza di pacchetti ACK in misura ridotta fa pensare che l'attaccante stia cercando di mascherare la scansione per non essere rilevato facilmente.

## Analisi del Traffico

Il traffico osservato mostra che l'indirizzo IP 192.168.200.100 invia numerosi pacchetti SYN a porte casuali del server, suggerendo l'uso di una scansione non sequenziale. I pacchetti SYN-ACK inviati dal server indicano che alcune di queste porte sono aperte, mentre i pacchetti RST-ACK segnalano che altre porte sono chiuse. Tuttavia, la peculiarità di questa scansione risiede nel fatto che le porte scansionate sembrano essere scelte in modo casuale, piuttosto che seguire una sequenza predefinita. Questo comportamento riduce la possibilità di rilevamento da parte di sistemi di monitoraggio e firewall, rendendo l'attività più difficile da tracciare.

## Ipotesi sul Vettore di Attacco

L'attività osservata sembra essere una scansione delle porte casuale, condotta per identificare quali porte siano aperte e quindi vulnerabili. La scelta di porte in modo non sequenziale è un tentativo di evitare la rilevazione automatica da parte di strumenti di sicurezza, come firewall e sistemi di rilevamento delle intrusioni (IDS). L'attaccante probabilmente sta cercando di raccogliere informazioni per identificare eventuali vulnerabilità da sfruttare in un attacco futuro, senza lasciare tracce facilmente identificabili.

Poiché la scansione non porta al completamento delle connessioni, non è possibile confermare un tentativo di attacco immediato. Tuttavia, la scansione delle porte potrebbe essere la fase preliminare di un potenziale attacco, con l'obiettivo di mappare i punti di ingresso vulnerabili.

## Azioni Consigliate

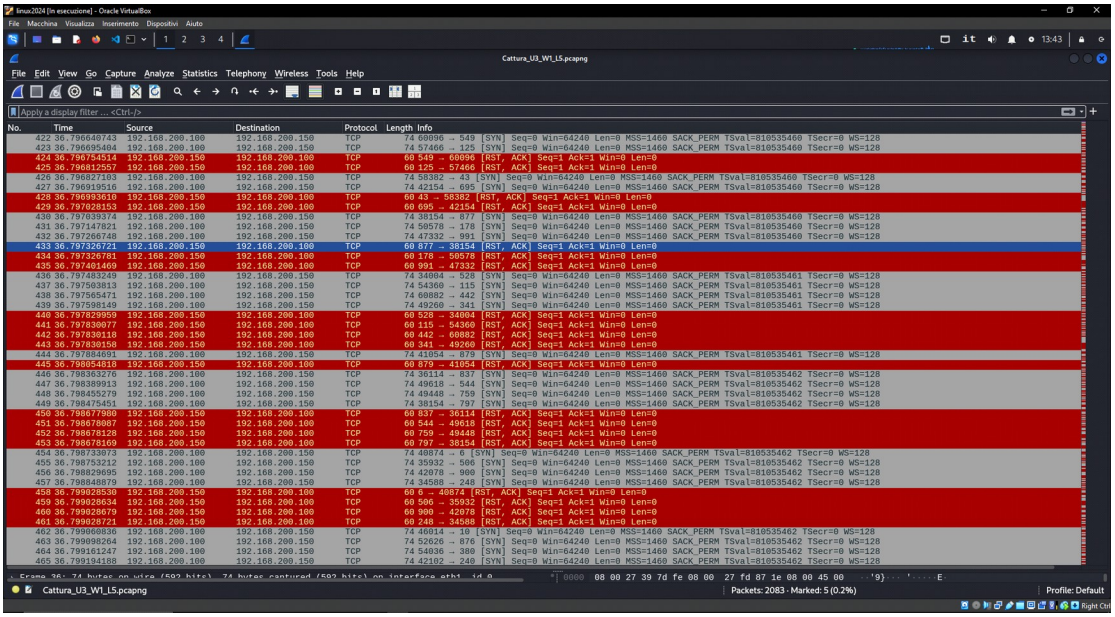
Per contrastare efficacemente un attacco di Port Scanning di tipo casuale, è fondamentale implementare una serie di misure di difesa. Il traffico di rete dovrebbe essere monitorato in modo continuo per rilevare

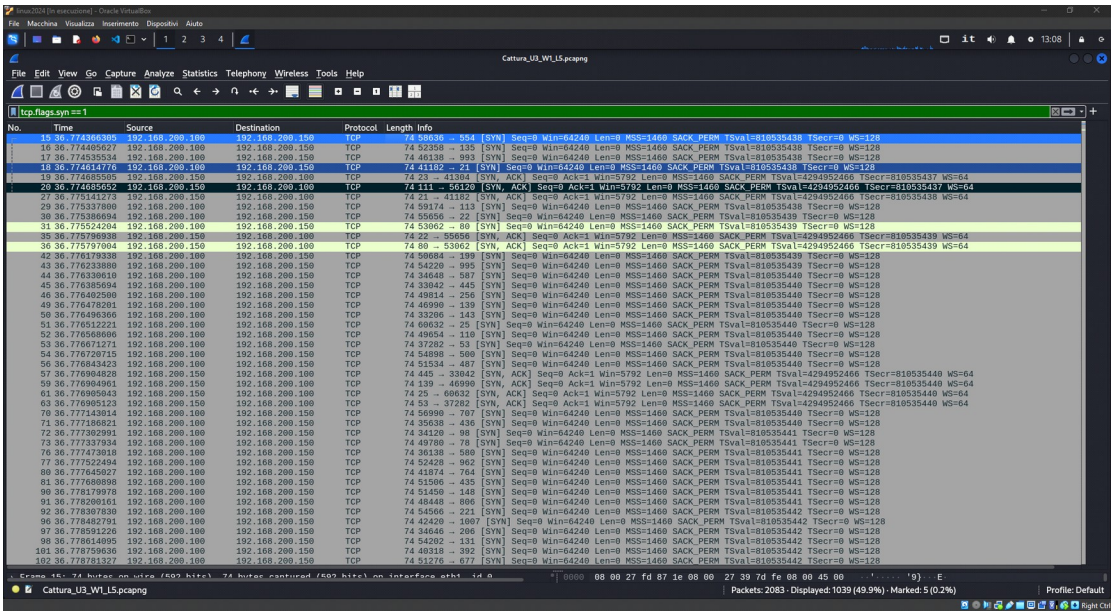
attività sospette, come l'invio di pacchetti SYN su porte in modo casuale. Configurare i firewall in modo da limitare il numero di pacchetti SYN provenienti dallo stesso indirizzo IP può contribuire a prevenire scansioni aggressive. L'utilizzo di sistemi IDS/IPS aiuterà a identificare e bloccare automaticamente gli IP che sembrano essere coinvolti in scansioni delle porte.

Inoltre, si consiglia di attivare l'uso di SYN Cookies sui sistemi per mitigare eventuali attacchi di tipo SYN Flood e di adottare politiche di sicurezza che limitino l'accesso alle porte sensibili del server, riducendo così il rischio di sfruttamento.

## Conclusioni

L'analisi ha confermato che l'attività sospetta rilevata è una Port Scanning, con un attacco condotto tramite l'invio di pacchetti SYN a porte casuali. Sebbene l'attività non costituisca un attacco diretto, essa rappresenta una fase preliminare di raccolta informazioni per eventuali exploit futuri. Per ridurre il rischio di attacchi successivi, è fondamentale implementare un monitoraggio efficace del traffico di rete, configurare correttamente firewall e sistemi di rilevamento delle intrusioni e utilizzare tecniche di mitigazione appropriate.




Kinux2024 [in esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Cattura_U3_W1_L5.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn == 1
No. Time Source Destination Protocol Length Info
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 36.774455627 192.168.200.100 192.168.200.150 TCP 74 52350 → 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 36.774685065 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=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
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
35 36.775796038 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
42 36.776179338 192.168.200.100 192.168.200.150 TCP 74 50684 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
43 36.776233880 192.168.200.100 192.168.200.150 TCP 74 54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
44 36.776330610 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 33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
46 36.776402500 192.168.200.100 192.168.200.150 TCP 74 49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
49 36.776478201 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 36.776496366 192.168.200.100 192.168.200.150 TCP 74 33206 → 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 60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
52 36.776568006 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 36.776720715 192.168.200.100 192.168.200.150 TCP 74 54898 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
56 36.776843423 192.168.200.100 192.168.200.150 TCP 74 51534 → 487 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
57 36.776904828 192.168.200.150 192.168.200.100 TCP 74 445 → 33042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
59 36.776904961 192.168.200.150 192.168.200.100 TCP 74 139 → 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
61 36.776905043 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 36.776905123 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
70 36.777143014 192.168.200.100 192.168.200.150 TCP 74 56990 → 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
71 36.777186821 192.168.200.100 192.168.200.150 TCP 74 35638 → 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
72 36.777302991 192.168.200.100 192.168.200.150 TCP 74 34120 → 98 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
73 36.777337934 192.168.200.100 192.168.200.150 TCP 74 49780 → 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
76 36.777473018 192.168.200.100 192.168.200.150 TCP 74 36138 → 580 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
77 36.777522494 192.168.200.100 192.168.200.150 TCP 74 52428 → 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
80 36.777645027 192.168.200.100 192.168.200.150 TCP 74 41874 → 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
81 36.777680890 192.168.200.100 192.168.200.150 TCP 74 51506 → 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
90 36.778179978 192.168.200.100 192.168.200.150 TCP 74 51450 → 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
91 36.778200161 192.168.200.100 192.168.200.150 TCP 74 48448 → 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
92 36.778307830 192.168.200.100 192.168.200.150 TCP 74 54566 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
96 36.778482791 192.168.200.100 192.168.200.150 TCP 74 42420 → 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
97 36.778591226 192.168.200.100 192.168.200.150 TCP 74 34646 → 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
98 36.778614095 192.168.200.100 192.168.200.150 TCP 74 54202 → 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
101 36.778759636 192.168.200.100 192.168.200.150 TCP 74 40318 → 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
102 36.778781327 192.168.200.100 192.168.200.150 TCP 74 51276 → 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
Frame 15: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth1, id 0
0000 08 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45 00
Cattura_U3_W1_L5.pcapng
Packets: 2083 · Displayed: 1039 (49.9%) · Marked: 5 (0.2%)
Profile: Default