

# 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.

No.	Time	Source	Destination	Protocol	Length	Info
422	36.798440743	192.168.200.100	192.168.200.150	TCP	74	60806 -- 549 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535460 TSecr=0 WS=128
423	36.798695484	192.168.200.100	192.168.200.150	TCP	74	57486 -- 125 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535460 TSecr=0 WS=128
424	36.798755514	192.168.200.150	192.168.200.100	TCP	60	549 -- 60806 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
425	36.798815557	192.168.200.150	192.168.200.100	TCP	60	125 -- 57486 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
426	36.798871583	192.168.200.100	192.168.200.150	TCP	74	58382 -- 43 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535460 TSecr=0 WS=128
427	36.798915510	192.168.200.100	192.168.200.150	TCP	74	42154 -- 695 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535460 TSecr=0 WS=128
428	36.798935010	192.168.200.150	192.168.200.100	TCP	60	43 -- 58382 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
429	36.797028153	192.168.200.150	192.168.200.100	TCP	60	695 -- 42154 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
430	36.797033374	192.168.200.100	192.168.200.150	TCP	74	58314 -- 417 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535460 TSecr=0 WS=128
431	36.797147821	192.168.200.100	192.168.200.150	TCP	74	58578 -- 178 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535460 TSecr=0 WS=128
432	36.797206748	192.168.200.100	192.168.200.150	TCP	74	47332 -- 951 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535460 TSecr=0 WS=128
433	36.797252921	192.168.200.150	192.168.200.100	TCP	60	178 -- 47332 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
434	36.797328781	192.168.200.150	192.168.200.100	TCP	60	178 -- 58578 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
435	36.797462460	192.168.200.100	192.168.200.150	TCP	60	991 -- 47332 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
436	36.797483249	192.168.200.100	192.168.200.150	TCP	74	34684 -- 528 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535461 TSecr=0 WS=128
437	36.797563813	192.168.200.100	192.168.200.150	TCP	74	54368 -- 115 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535461 TSecr=0 WS=128
438	36.797665471	192.168.200.100	192.168.200.150	TCP	74	68882 -- 442 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535461 TSecr=0 WS=128
439	36.797588149	192.168.200.100	192.168.200.150	TCP	74	49260 -- 341 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535461 TSecr=0 WS=128
440	36.797492550	192.168.200.150	192.168.200.100	TCP	60	528 -- 34084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
441	36.797838077	192.168.200.150	192.168.200.100	TCP	60	115 -- 54368 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
442	36.797838118	192.168.200.150	192.168.200.100	TCP	60	442 -- 68882 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
443	36.797838150	192.168.200.100	192.168.200.150	TCP	60	341 -- 49260 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
444	36.797884593	192.168.200.100	192.168.200.150	TCP	74	41054 -- 879 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535461 TSecr=0 WS=128
445	36.798054518	192.168.200.150	192.168.200.100	TCP	60	879 -- 41054 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
446	36.798105276	192.168.200.100	192.168.200.150	TCP	74	49314 -- 847 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535462 TSecr=0 WS=128
447	36.798389913	192.168.200.100	192.168.200.150	TCP	74	49318 -- 544 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535462 TSecr=0 WS=128
448	36.798458278	192.168.200.100	192.168.200.150	TCP	74	48448 -- 759 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535462 TSecr=0 WS=128
449	36.798475451	192.168.200.100	192.168.200.150	TCP	74	38154 -- 797 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535462 TSecr=0 WS=128
450	36.798677880	192.168.200.150	192.168.200.100	TCP	60	837 -- 36114 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
451	36.798678087	192.168.200.150	192.168.200.100	TCP	60	544 -- 49318 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
452	36.798678128	192.168.200.150	192.168.200.100	TCP	60	759 -- 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
453	36.798678169	192.168.200.150	192.168.200.100	TCP	60	797 -- 38154 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
454	36.798728372	192.168.200.100	192.168.200.150	TCP	74	48974 -- 4 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535462 TSecr=0 WS=128
455	36.798753212	192.168.200.100	192.168.200.150	TCP	74	35932 -- 586 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535462 TSecr=0 WS=128
456	36.798828695	192.168.200.100	192.168.200.150	TCP	74	42078 -- 988 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535462 TSecr=0 WS=128
457	36.798848979	192.168.200.100	192.168.200.150	TCP	74	34588 -- 248 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535462 TSecr=0 WS=128
458	36.799028530	192.168.200.150	192.168.200.100	TCP	60	4 -- 48974 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
459	36.799028634	192.168.200.150	192.168.200.100	TCP	60	988 -- 35932 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
460	36.799028679	192.168.200.150	192.168.200.100	TCP	60	988 -- 42078 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
461	36.799028721	192.168.200.100	192.168.200.150	TCP	60	248 -- 34588 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
462	36.799050530	192.168.200.100	192.168.200.150	TCP	74	46014 -- 10 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535462 TSecr=0 WS=128
463	36.799088264	192.168.200.100	192.168.200.150	TCP	74	52626 -- 876 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535462 TSecr=0 WS=128
464	36.799161247	192.168.200.100	192.168.200.150	TCP	74	54006 -- 380 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535462 TSecr=0 WS=128
465	36.799184189	192.168.200.150	192.168.200.100	TCP	74	42102 -- 249 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535462 TSecr=0 WS=128

linux2024 [in esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Impostazioni Dispositivi Auto

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Cattura\_U3\_WL5 pcapng

tcp.flags.syn == 1

No.	Time	Source	Destination	Protocol	Length	Info
15	36.774364360	192.168.200.100	192.168.200.150	TCP	74	58036 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16	36.774459520	192.168.200.100	192.168.200.150	TCP	74	52338 → 555 [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	36.774617170	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	36.774685550	192.168.200.150	192.168.200.100	TCP	74	23 → 4304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952460 TSecr=810535437 WS=64
20	36.774685552	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=4294952460 TSecr=810535437 WS=64
21	36.774718212	192.168.200.150	192.168.200.100	TCP	74	21 → 43102 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952460 TSecr=810535438 WS=64
29	36.775377880	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	36.775396594	192.168.200.100	192.168.200.150	TCP	74	55056 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31	36.775525264	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	36.775789938	192.168.200.150	192.168.200.100	TCP	74	22 → 55058 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952460 TSecr=810535439 WS=64
36	36.775791904	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=4294952460 TSecr=810535439 WS=64
42	36.776171330	192.168.200.100	192.168.200.150	TCP	74	59084 → 199 [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	36.776338010	192.168.200.100	192.168.200.150	TCP	74	54648 → 507 [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	36.776402580	192.168.200.100	192.168.200.150	TCP	74	48914 → 258 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
49	36.776470201	192.168.200.100	192.168.200.150	TCP	74	46980 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
50	36.776496360	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	68032 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
52	36.776568060	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	54808 → 580 [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	192.168.200.100	192.168.200.150	TCP	74	445 → 33042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952460 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=4294952460 TSecr=810535440 WS=64
61	36.776950543	192.168.200.150	192.168.200.100	TCP	74	25 → 68032 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952460 TSecr=810535440 WS=64
63	36.776981521	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=4294952460 TSecr=810535440 WS=64
70	36.777143014	192.168.200.100	192.168.200.150	TCP	74	60990 → 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 → 438 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
72	36.777202991	192.168.200.100	192.168.200.150	TCP	74	34120 → 80 [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	36.777473818	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	36.777522484	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	36.777688980	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	36.778206161	192.168.200.100	192.168.200.150	TCP	74	48448 → 896 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
92	36.778307839	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	36.778759836	192.168.200.100	192.168.200.150	TCP	74	49318 → 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

Croma 16: 74 bytes on wire (405 bits) 74 bytes captured (405 bits) on interface eth1 id 0

0000 08 00 27 fd 87 1e 08 00 27 39 fd fe 08 00 45 00 .....9) E

Packets: 2083 - Displayed: 1039 (49.9%) - Marked: 5 (0.2%)

Profile: Default

Right Click