



Obiettivo dell'esercizio è capire eventuali attacchi, quali sono i vettori di attacco e come ridurre gli impatti dell'attacco

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=...
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951...
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=42...
8	28.761629461	08:00:27:fd:87:1e	08:00:27:39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	08:00:27:39:7d:fe	08:00:27:fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	08:00:27:39:7d:fe	08:00:27:fd:87:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	08:00:27:fd:87:1e	08:00:27:39:7d:fe	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437...
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...
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...
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...
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438...
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...
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 ...
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74	23 → 41304 [SYN, ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK PERM TSval=...
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...
81	36.777680898	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...
82	36.777758636	192.168.200.150	192.168.200.100	TCP	60	580 → 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83	36.777758696	192.168.200.150	192.168.200.100	TCP	60	962 → 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84	36.777871245	192.168.200.150	192.168.200.100	TCP	60	764 → 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85	36.777871293	192.168.200.150	192.168.200.100	TCP	60	435 → 51506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86	36.777893298	192.168.200.100	192.168.200.150	TCP	66	33042 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4...
87	36.777912717	192.168.200.100	192.168.200.150	TCP	66	46990 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4...
88	36.777986759	192.168.200.100	192.168.200.150	TCP	66	60632 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=42...
89	36.778031265	192.168.200.100	192.168.200.150	TCP	66	37282 → 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=42...
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...
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...
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=8105354

Si noti che intuire chi è attaccante e chi attaccato non è immediato.

Tuttavia osservando lo scan nel dettaglio è possibile vedere che 192.168.200.100 sta inoltrando un' enorme quantità di richieste ARK verso 192.168.200.150.

Molto probabilmente 192.168.200.100 è l'attaccante.

8	28.761629461	08:00:27:fd:87:1e	08:00:27:39:7d:fe	ARP	60 Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	08:00:27:39:7d:fe	08:00:27:fd:87:1e	ARP	42 192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	08:00:27:39:7d:fe	08:00:27:fd:87:1e	ARP	42 Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	08:00:27:fd:87:1e	08:00:27:39:7d:fe	ARP	60 192.168.200.150 is at 08:00:27:fd:87:1e
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74 41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 ...
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...
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...
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...
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74 52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438...
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...
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 ...
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74 23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=...
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=...

Inoltre, "RST" sta per "Reset". Quando un host riceve un segmento TCP con il flag RST impostato, significa che la connessione TCP è stata ripristinata o "azzerata" bruscamente. Questo può avvenire per vari motivi, ad esempio quando si verifica un errore di comunicazione o quando un host desidera interrompere una connessione in modo improvviso.

Questo potrebbe avvenire perchè l'attaccato registra tentativi di connessione anomali.

39	36.780577880	192.168.200.150	192.168.200.100	TCP	60 266 → 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
40	36.780577981	192.168.200.150	192.168.200.100	TCP	60 11 → 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
41	36.780578026	192.168.200.150	192.168.200.100	TCP	60 235 → 40648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42	36.780578074	192.168.200.150	192.168.200.100	TCP	60 739 → 36548 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
43	36.780578119	192.168.200.150	192.168.200.100	TCP	60 55 → 38866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
44	36.780578158	192.168.200.150	192.168.200.100	TCP	60 999 → 52136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
45	36.780578198	192.168.200.150	192.168.200.100	TCP	60 317 → 38022 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

IL VETTORE UTILIZZATO È IL PROTOCOLLO TCP

TCP è uno dei principali protocolli utilizzati nella comunicazione su Internet e viene utilizzato per trasferire dati in modo affidabile tra computer connessi in una rete.

La soluzione migliore sarebbe impostare regole sul firewall affinché la comunicazione con 192.168.200.100 non avvenga e qualsiasi pacchetto bloccato.