

In questo esercizio bisogna riscontrare delle evidenze di un attacco in corso, ipotizzare i vettori di attacco ed infine capire che metodo utilizzare per contrastare e ridurre l'impatto di eventuali attacchi.

Possiamo subito notare svariate richieste TCP da parte dell'host che finisce in .100. Questo dovrebbe essere già un campanello d'allarme. Potrebbe essere un potenziale attacco DoS, ma investigando un po' più a fondo, la richiesta TCP sta avvenendo su più e più porte, facendoci pensare ad una probabile **scansione**.

Cattura_U3_W1_L3.pcapng

File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto

Applica un filtro di visualizzazione ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential Browser
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
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=4294951165 TSecr=810522427 WS=64
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=4294951165
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=4294951165
8	28.761629461	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PcsCompu_fd:87:1e	PcsCompu_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 TSecr=0 WS=128
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	36.774366305	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	36.774405627	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 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	36.774685505	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=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	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711072	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	36.775141104	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

> Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0

> Ethernet II, Src: PcsCompu_fd:87:1e (08:00:27:fd:87:1e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.255

> User Datagram Protocol, Src Port: 138, Dst Port: 138

> NetBIOS Datagram Service

> SMB (Server Message Block Protocol)

> SMB Mailslot Protocol

> Microsoft Windows Browser Protocol

```

0000 ff ff ff ff ff 08 00 27 fd 87 1e 08 00 45 00 .....E
0010 01 10 00 00 40 00 40 11 26 f6 c0 a8 c8 96 c0 a8 ..@.@:&.....
0020 c8 ff 00 8a 00 8a 00 fc 4b 01 11 0a 75 b4 c0 a8 .....K...u...
0030 c8 96 00 8a 00 e6 00 00 20 45 4e 45 46 
```

Notando che la richiesta viene effettuata e droppata più e più volte, su porte diverse, possiamo decisamente confermare l'ipotesi di una scansione in corso.

Potremmo ovviare mettendo una policy/regola all'interno del firewall, che blocchi l'accesso a tutte le porte da parte di quell'indirizzo IP. E' comunque "good practice" chiudere l'accesso alle known ports dei servizi che non vengono utilizzati.

FileModificaVisualizzaVaiCatturaAnalizzaStatisticheTelefoniaWirelessStrumentiAiuto

Applica un filtro di visualizzazione ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
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
74	36.777430632	192.168.200.150	192.168.200.100	TCP	60	707 → 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75	36.777430741	192.168.200.150	192.168.200.100	TCP	60	436 → 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
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
78	36.777623082	192.168.200.150	192.168.200.100	TCP	60	98 → 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79	36.777623149	192.168.200.150	192.168.200.100	TCP	60	78 → 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
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	36.777680898	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 TSecr=0 WS=128
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=4294952466
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=4294952466
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=4294952466
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=4294952466
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
93	36.778385846	192.168.200.150	192.168.200.100	TCP	60	148 → 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94	36.778385948	192.168.200.150	192.168.200.100	TCP	60	806 → 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95	36.778449494	192.168.200.150	192.168.200.100	TCP	60	221 → 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
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

> Frame 76: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth1, id 0

> Ethernet II, Src: PcsCompu_39:7d:fe (08:00:27:39:7d:fe), Dst: PcsCompu_fd:87:1e (08:00:27:fd:87:1e)

> Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200.150

> Transmission Control Protocol, Src Port: 36138, Dst Port: 580, Seq: 0, Len: 0

0000 08 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45 00 ..'.....'9}...E-

0010 00 3c 35 ff 40 00 40 06 f2 70 c0 a8 c8 64 c0 a8 <5.@. .p...d..

0020 c8 96 8d 2a 02 44 20 55 6e 51 00 00 00 00 a0 02 ...*:D U nQ.....

0030 fa f0 12 7b 00 00 02 04 05 b4 04 02 08 0a 30 4f ...{.....00

0040 ca 11 00 00 00 00 01 03 03 07