

Analisi pacchetti con wireshark

Possiamo subito notare che l'host 150 (in questo caso METASPLOITABLE) fa un avviso in broadcast

Time	Source	Destination	Protocol	Length	Info
1 0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE,
.\MAILSL OT\BROWS E..... METASPLO ITABLE..... U metasp loitable server (Samba 3 .0.20-De bian)					

Possiamo vedere il server di samba

Poi notiamo che avviene una connessione alla porta 80 del server dal host 100

2 23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=
3 23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=
4 23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=
5 23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=
6 23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=
7 23.764820091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=

Vediamo che viene completata la triple hand shake

Andando avanti nella cattura notiamo un'altra cosa interessante

11 28.775230099	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60	192.168.200.150 is at 08:00
12 36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=
13 36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=
14 36.774257841	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=
15 36.774366305	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=
16 36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=
17 36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=
18 36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=
19 36.774685505	192.168.200.150	192.168.200.100	TCP	74	23 → 41304 [SYN, ACK] Seq=
20 36.774685652	192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=
21 36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, ACK] Seq=
22 36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=
23 36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=
24 36.774700464	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [ACK] Seq=1 Ack=1
25 36.774711072	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [ACK] Seq=1 Ack=1

Una serie di richieste di syn dal host 100 al 150 su varie porte, potrebbe essere uno scan con nmap, vediamo che sotto è stata completata la connessione anche su queste porte

24 36.774700464	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [ACK] Seq=1 Ack=1
25 36.774711072	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [ACK] Seq=1 Ack=1
26 36.775144181	192.168.200.150	192.168.200.100	TCP	66	888 → 41304 [RST, ACK] Seq=1 Ack=1

Possiamo ipotizzare che lo scan sia -sT

Notiamo che viene rifatta la connessione alla porta 80

31	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53062 → 80 [SYN] Seq=0 Wi
32	36.775589806	192.168.200.150	192.168.200.100	TCP	60	113 → 59174 [RST, ACK] Seq=1
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [RST, ACK] Seq=1
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [RST, ACK] Seq=1
35	36.775796938	192.168.200.150	192.168.200.100	TCP	74	22 → 55656 [SYN, ACK] Seq=0
36	36.775797004	192.168.200.150	192.168.200.100	TCP	74	80 → 53062 [SYN, ACK] Seq=1
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [ACK] Seq=1
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [ACK] Seq=1
39	36.775861964	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [RST, ACK] Seq=1
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [RST, ACK] Seq=1
41	36.776005853	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [RST, ACK] Seq=1
42	36.776179338	192.168.200.100	192.168.200.150	TCP	74	50684 → 199 [SYN] Seq=0
43	36.776233880	192.168.200.100	192.168.200.150	TCP	74	54220 → 995 [SYN] Seq=0
44	36.776330610	192.168.200.100	192.168.200.150	TCP	74	34648 → 587 [SYN] Seq=0
45	36.776385694	192.168.200.100	192.168.200.150	TCP	74	33042 → 445 [SYN] Seq=0
46	36.776402500	192.168.200.100	192.168.200.150	TCP	74	49814 → 256 [SYN] Seq=0
47	36.776451284	192.168.200.150	192.168.200.100	TCP	60	189 → 50684 [RST, ACK] Seq=1

Notiamo per esempio alcune porte che rispondono

163	36.781487105	192.168.200.150	192.168.200.100	TCP	60	918 → 55360 [RST, ACK]
164	36.781487210	192.168.200.150	192.168.200.100	TCP	74	512 → 45648 [SYN, ACK]
165	36.781512468	192.168.200.100	192.168.200.150	TCP	66	45648 → 512 [ACK] Seq=1
166	36.781621871	192.168.200.150	192.168.200.100	TCP	60	354 → 53246 [RST, ACK]
267	36.788805940	192.168.200.150	192.168.200.100	TCP	74	514 → 51396 [SYN, ACK]
268	36.788833247	192.168.200.100	192.168.200.150	TCP	66	51396 → 514 [ACK] Seq=1
269	36.788954711	192.168.200.150	192.168.200.100	TCP	60	224 → 56758 [RST, ACK]

Le richieste sono quasi 2000 in poco tempo, è in questo caso quasi certo che si tratti di uno scan delle porte, vista la randomicità è probabilmente nmap

1970	36.873906267	192.168.200.100	192.168.200.150	TCP	74	57518 → 525 [SYN]
1971	36.873927281	192.168.200.100	192.168.200.150	TCP	74	48420 → 925 [SYN]
1972	36.874010804	192.168.200.100	192.168.200.150	TCP	74	60958 → 618 [SYN]
1973	36.874028994	192.168.200.100	192.168.200.150	TCP	74	41876 → 73 [SYN] Seq=1
1974	36.874106428	192.168.200.150	192.168.200.100	TCP	60	525 → 57518 [RST]

Una possibilità per ridurre il rischio di questi attacchi è filtrare le porte con il firewall facendo in modo che i ping vengano bloccati su tutte le porte che non vogliamo vengano raggiunte per eventuali servizi pubblici

Bonus

```
(alesio㉿kali)-[~]
$ ping www.atac.roma.it
PING www.atac.roma.it (217.221.16.25) 56(84) bytes of data.
^C
--- www.atac.roma.it ping statistics ---
72 packets transmitted, 0 received, 100% packet loss, time 72725ms

(alesio㉿kali)-[~]
```

La pagina in questo momento non risponde, però possiamo comunque vedere il suo indirizzo ip grazie al dns