

Analisi Wiresharke

Prendendo in considerazione il file di Wireshark possiamo notare che:

- ❖ I primi quattro pacchetti sono protocolli ARP che servono per stabilire la comunicazione e i due host

8	09:59:28.655446...	PCSSystemtec_fd:87:1e	PCSSystemtec_3...	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	09:59:28.655462...	PCSSystemtec_39:7d:fe	PCSSystemtec_f...	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	09:59:28.668669...	PCSSystemtec_39:7d:fe	PCSSystemtec_f...	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	09:59:28.669047...	PCSSystemtec_fd:87:1e	PCSSystemtec_3...	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e

- ❖ C'è un pacchetto che ci fa capire che la macchina target 192.168.200.150 è una probabile macchina Metasploitable, potremmo andare ancora più nel dettaglio con

1	09:58:59.893817...	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server,
---	--------------------	-----------------	-----------------	---------	-----	--

- ❖ Ci sono due attori in gioco : 192.168.200.100 e 192.168.200.150
192.168.200.100 risulta effettuare richieste SYN su molteplici porte
192.168.200.150 risponde a tutte le richieste con RST,ACK
- ❖ Quasi tutte i pacchetti sono con protocollo TCP

Frame	100.0	2083	100.0	139872	30 k
Ethernet	100.0	2083	25.2	35276	7652
Internet Protocol Version 4	99.8	2079	29.7	41580	9019
User Datagram Protocol	0.0	1	0.0	8	1
NetBIOS Datagram Service	0.0	1	0.2	244	52
SMB (Server Message Block Protocol)	0.0	1	0.1	162	35
SMB MailSlot Protocol	0.0	1	0.0	25	5
Microsoft Windows Browser Protocol	0.0	1	0.1	76	16
Transmission Control Protocol	99.8	2078	44.8	62652	13 k
Address Resolution Protocol	0.2	4	0.1	148	32

Possiamo supporre che la macchina con IP 192.168.200.100 sta effettuando una scansione su molteplici porte sulla macchina con IP 192.168.200.150.

Nelle info dei pacchetti inviati da 192.168.200.100 sono presenti soltanto messaggi SYN, come se stesse effettuando una scansione in modalità stealth.

Le risposte della macchina target 192.168.200.150 sono tutte RST,ACK.

Possiamo inoltre individuare quali porte sono aperte in quanto avviene una comunicazione TCP 3 way-Handshake. Alcune delle porte aperte sono: 23,80,111,445 ecc..

192.168.200.100	33042	192.168.200.150	445	4	280 bytes	15	3	206 bytes
192.168.200.100	37282	192.168.200.150	53	4	280 bytes	21	3	206 bytes
192.168.200.100	41182	192.168.200.150	21	4	280 bytes	8	3	206 bytes
192.168.200.100	41304	192.168.200.150	23	4	280 bytes	2	3	206 bytes
192.168.200.100	42048	192.168.200.150	513	4	280 bytes	480	3	206 bytes
192.168.200.100	45648	192.168.200.150	512	4	280 bytes	68	3	206 bytes
192.168.200.100	46990	192.168.200.150	139	4	280 bytes	17	3	206 bytes
192.168.200.100	51396	192.168.200.150	514	4	280 bytes	118	3	206 bytes
192.168.200.100	53060	192.168.200.150	80	4	280 bytes	0	3	206 bytes
192.168.200.100	53062	192.168.200.150	80	4	280 bytes	11	3	206 bytes
192.168.200.100	55656	192.168.200.150	22	4	280 bytes	10	3	206 bytes
192.168.200.100	56120	192.168.200.150	111	4	280 bytes	3	3	206 bytes
192.168.200.100	60632	192.168.200.150	25	4	280 bytes	19	3	206 bytes

Una possibile soluzione e prevenzione sarebbe quella di settare un firewall in modo da filtrare la comunicazione sulle porte aperte che potrebbero essere un pericoloso vettore di attacco.