

IOC (Indicator of compromise)

Dopo aver aperto il file di cattura con Wireshark andiamo a svolgere un'analisi sulla trasmissione di dati intercettata.

Il primo pacchetto già si rivela interessante dato che è un messaggio di broadcast inviato all'IP 192.168.200.255

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

No.	Time	Source	Destination	Protocol
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER

Browser Protocol Major Version: 15
Browser Protocol Minor Version: 1
Signature: 0xaa55
Host Comment: metasploitable server (Samba 3.0.20-Debian)

Da qui capiamo subito che all'indirizzo 192.168.200.150 si trova la macchina target del successivo attacco ed è metasploitable che dichiara in automatico quali funzioni ha attive, la sua versione e vari protocolli attivi.

Successivamente vediamo l'attaccante rivolgersi alle porte 80 HTTP, 443 HTTPS e il protocollo arp per la risoluzione degli indirizzi.

2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
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
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
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
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

In seguito nella comunicazione possiamo ipotizzare che l'attaccante stia eseguendo un nmap con metodo sync sul target, possiamo capirlo dal fatto che viene scandagliato un ampio range di porte di metasploitable e nessuna connessione viene mai stabilita anzi vengono sempre resettate.

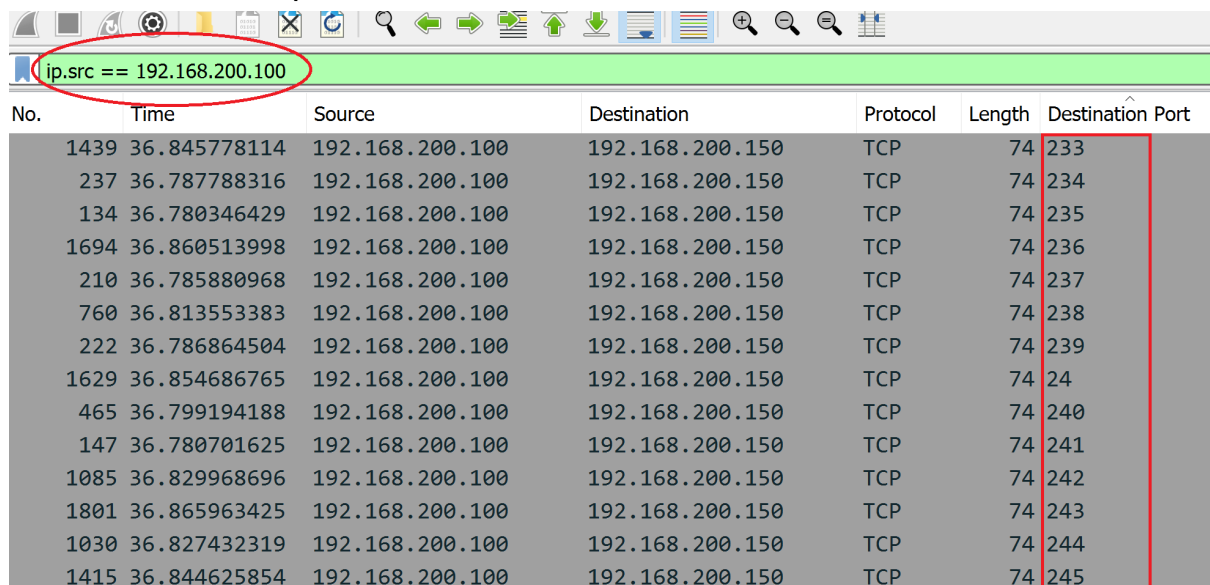
Infatti Wireshark ci segna in automatico quando una connessione viene resettata direttamente dalla sorgente.

... = Header Length: 20 bytes (5)

▼ Flags: 0x014 (RST, ACK)

- 000. = Reserved: Not set
- ...0 = Nonce: Not set
- 0... = Congestion Window R
-0.. = ECN-Echo: Not set
-0. = Urgent: Not set
-1 = Acknowledgment: Set
- 0... = Push: Not set
- >1.. = Reset: Set
-0. = Syn: Not set
-0 = Fin: Not set

Possiamo escludere si tratti di un dos (denial of service) semplicemente applicando come filtro l'ip della sorgente attacco e come nuova colonna la destinazione della porta:



The image shows a Wireshark interface. At the top, a filter bar contains the text 'ip.src == 192.168.200.100', which is circled in red. Below the filter bar is a table of captured packets. The table has seven columns: 'No.', 'Time', 'Source', 'Destination', 'Protocol', 'Length', and 'Destination Port'. The 'Destination Port' column is highlighted with a red border. The table contains 15 rows of data, all showing TCP traffic from source IP 192.168.200.100 to destination IP 192.168.200.150 on various ports.

No.	Time	Source	Destination	Protocol	Length	Destination Port
1439	36.845778114	192.168.200.100	192.168.200.150	TCP	74	233
237	36.787788316	192.168.200.100	192.168.200.150	TCP	74	234
134	36.780346429	192.168.200.100	192.168.200.150	TCP	74	235
1694	36.860513998	192.168.200.100	192.168.200.150	TCP	74	236
210	36.785880968	192.168.200.100	192.168.200.150	TCP	74	237
760	36.813553383	192.168.200.100	192.168.200.150	TCP	74	238
222	36.786864504	192.168.200.100	192.168.200.150	TCP	74	239
1629	36.854686765	192.168.200.100	192.168.200.150	TCP	74	24
465	36.799194188	192.168.200.100	192.168.200.150	TCP	74	240
147	36.780701625	192.168.200.100	192.168.200.150	TCP	74	241
1085	36.829968696	192.168.200.100	192.168.200.150	TCP	74	242
1801	36.865963425	192.168.200.100	192.168.200.150	TCP	74	243
1030	36.827432319	192.168.200.100	192.168.200.150	TCP	74	244
1415	36.844625854	192.168.200.100	192.168.200.150	TCP	74	245