

Relazione

Relazione sull'analisi del traffico di rete

1. Descrizione del traffico anomalo

Durante l'analisi del file di cattura di rete con **Wireshark**, è stato individuato un traffico sospetto associato alla macchina con indirizzo IP **192.168.200.150**, che sembra essere una macchina **Metasploitable**. Il traffico evidenziato in rosso, segnalato da **Wireshark** come pacchetti non andati a buon fine, potrebbe indicare tentativi di attacco o scansioni aggressive delle porte.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROADCAST	208	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	23.764287189	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	23.764771233	192.168.200.100	192.168.200.150	TCP	74	80 -> 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=810522427 WS=64
5	23.764837742	192.168.200.150	192.168.200.150	TCP	60	4182 -> 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764852390	192.168.200.100	192.168.200.150	TCP	60	53060 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810523420 TSecr=4294951165
7	23.764883091	192.168.200.100	192.168.200.150	TCP	60	53060 -> 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810523420 TSecr=4294951165
8	28.761626461	PCSSystemtec_fd:87...	PCSSystemtec_fd:7d...	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d...	PCSSystemtec_fd:87...	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PCSSystemtec_39:7d...	PCSSystemtec_fd:87...	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230999	PCSSystemtec_fd:87...	PCSSystemtec_39:7d...	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
12	36.774434448	192.168.200.100	192.168.200.150	TCP	74	43304 -> 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	56128 -> 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	36.774366395	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	36.774541776	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	36.774685955	192.168.200.150	192.168.200.150	TCP	74	23 -> 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=810535437 WS=64
20	36.774685952	192.168.200.150	192.168.200.150	TCP	74	111 -> 56128 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=810535437 WS=64
21	36.774685996	192.168.200.150	192.168.200.150	TCP	60	443 -> 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.150	TCP	60	554 -> 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.150	TCP	60	135 -> 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774709464	192.168.200.100	192.168.200.150	TCP	60	41304 -> 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
25	36.774715872	192.168.200.100	192.168.200.150	TCP	60	56128 -> 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775141104	192.168.200.150	192.168.200.150	TCP	60	993 -> 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	192.168.200.150	192.168.200.150	TCP	74	21 -> 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=4294952466
28	36.775174848	192.168.200.100	192.168.200.150	TCP	60	41182 -> 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775337986	192.168.200.100	192.168.200.150	TCP	74	59174 -> 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30	36.775386994	192.168.200.100	192.168.200.150	TCP	74	55656 -> 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53062 -> 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
32	36.775588806	192.168.200.150	192.168.200.150	TCP	60	113 -> 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.100	192.168.200.150	TCP	60	41304 -> 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775653097	192.168.200.100	192.168.200.150	TCP	60	59209 -> 113 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35	36.775757933	192.168.200.150	192.168.200.150	TCP	74	22 -> 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=4294952466
36	36.775797084	192.168.200.150	192.168.200.150	TCP	74	80 -> 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=4294952466
37	36.775803786	192.168.200.100	192.168.200.150	TCP	60	55656 -> 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38	36.775813232	192.168.200.100	192.168.200.150	TCP	60	53062 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.775813904	192.168.200.100	192.168.200.150	TCP	60	41182 -> 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

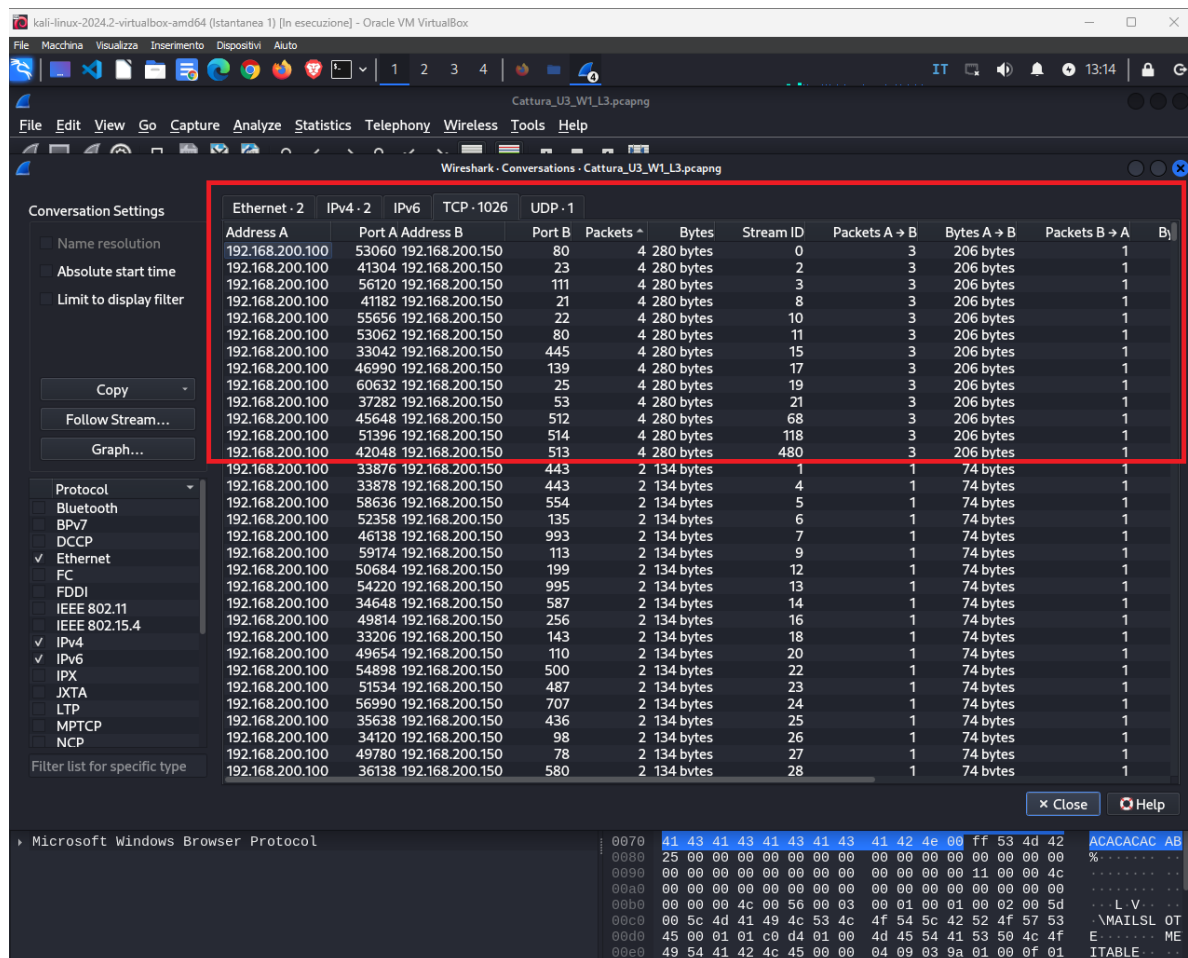
Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0
Ethernet II, Src: PCSSystemtec_fd:87:1e (08:00:27:fd:87:1e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.255
User Datagram Protocol, Src Port: 138, Dst Port: 138
NetBIOS Datagram Service
Message Type: Direct_group datagram (17)
Flags: 0x0a, This is first fragment, Node Type: M node
Datagram ID: 0x7504

0000 ff ff ff ff ff ff ff ff 08 00 27 fd 87 1e 08 00 45 00 E..
0010 01 09 00 00 00 00 4b 11 26 f6 c8 a8 c8 90 c8 a8 @ &.....
0020 c8 ff 00 00 00 00 f6 4b 01 11 8a 75 04 c8 00 K
0030 c8 96 00 00 00 e0 00 20 4e 4e 4e 4e 4e 4e 4e ENFFEE
0040 42 46 44 46 41 45 46 45 50 45 4a 46 45 42 45 BDF0AEME PEJFEERE
0050 43 45 4d 45 46 43 41 41 00 20 46 48 45 50 46 CENEFCAA A PHEPF
0060 43 45 4c 45 48 46 43 45 50 46 46 41 43 41 43 CELEHFCCE PFFFCAC
0070 41 43 41 43 41 43 41 43 41 42 4e 00 ff 53 42 42 ACACACAC ABN SBN

2. Porte coinvolte

Dall'analisi della cattura di rete, le seguenti porte sono risultate aperte sulla macchina **192.168.200.150**:

- **TCP**: 80 (HTTP), 23 (Telnet), 111 (RPC), 21 (FTP), 22 (SSH), 445 (SMB), 139 (NetBIOS), 25 (SMTP), 53 (DNS), 5125 (probabile servizio custom), 514 (Syslog)
- **UDP**: 138 (NetBIOS Datagram Service)



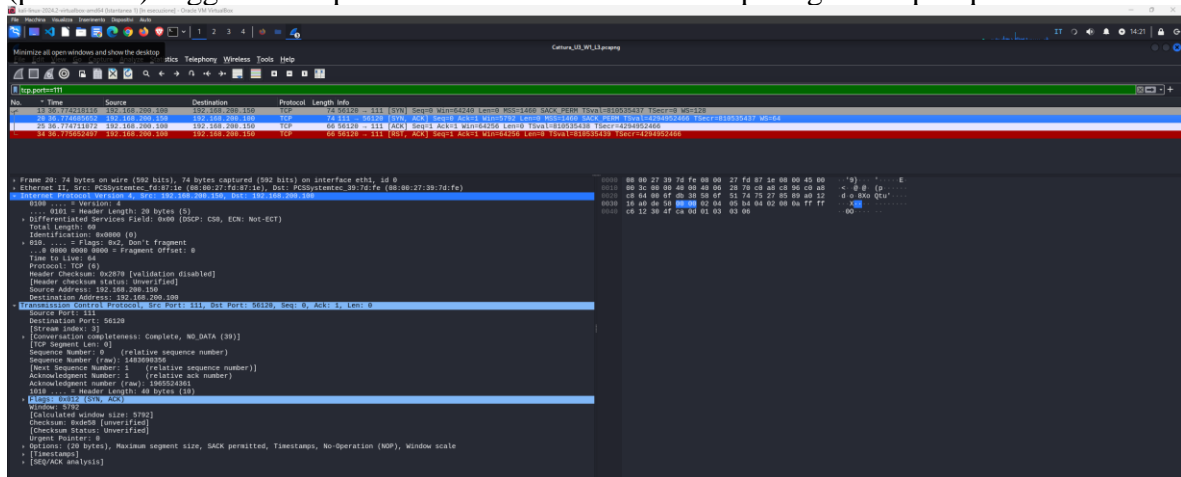
Questa configurazione lascia presumere che la macchina Metasploitable sia vulnerabile a diversi attacchi, in quanto espone un numero considerevole di servizi, molti dei quali notoriamente deboli dal punto di vista della sicurezza, come **Telnet** (porta 23) e **FTP** (porta 21), entrambi non criptati.

3. Indicatori di compromissione (IOC)

Durante l'analisi del traffico, i seguenti Indicatori di Compromissione (IOC) sono stati identificati:

- **Connessioni fallite**: Il traffico segnalato in rosso, evidenziando connessioni non completate, potrebbe rappresentare tentativi di ricognizione o attacco, come **scansioni di porte** o tentativi di brute force.

- **Porte vulnerabili aperte:** La presenza di porte vulnerabili come Telnet, FTP, SMB e RPC (porta 111) suggerisce la possibilità di attacchi tramite exploit già noti per questi servizi.



- **Traffico UDP sulla porta 138:** Il servizio NetBIOS Datagram sulla porta UDP 138 potrebbe essere usato per intercettare dati sensibili o facilitare un attacco **man-in-the-middle**.

4. Ipotesi sui vettori di attacco

Basandoci sugli IOC individuati, possiamo ipotizzare che i vettori di attacco più probabili siano:

- **Scansioni di porte:** L'alto numero di pacchetti inviati, in particolare su molteplici porte aperte, indica un possibile tentativo di scansione delle porte per identificare i servizi attivi e preparare un attacco mirato.
- **Tentativi di brute force** su servizi non sicuri come **Telnet** (porta 23) o **FTP** (porta 21), che non offrono cifratura e sono vulnerabili a questo tipo di attacchi.
- **Attacchi SMB:** Le porte 445 e 139, associate al protocollo SMB, sono note per essere vettori di attacchi quali **EternalBlue**, utilizzato da malware come **WannaCry**.
- **Possibile exploit su RPC (porta 111):** Questa porta è comunemente associata a vulnerabilità come **RPC DCOM** che potrebbe consentire esecuzione di codice da remoto.

5. Azioni consigliate per mitigare l'attacco

Per ridurre gli impatti dell'attacco in corso e prevenire eventuali attacchi futuri, si consiglia di adottare le seguenti azioni:

- **Chiusura delle porte non necessarie:** Disattivare o filtrare le porte che non sono strettamente necessarie, in particolare servizi vulnerabili come **Telnet** (23), **FTP** (21), **RPC** (111) e **SMB** (445/139). L'uso di firewall per limitare l'accesso a queste porte potrebbe ridurre drasticamente la superficie di attacco.
- **Implementazione di protocolli sicuri:** Sostituire servizi non sicuri con alternative più sicure, ad esempio:
 - Usare **SSH** (22) al posto di Telnet per connessioni remote.
 - Usare **SFTP** o **FTPS** al posto di FTP per il trasferimento di file.
- **Aggiornamenti di sicurezza:** Assicurarsi che il sistema operativo e i servizi esposti siano aggiornati con le ultime patch di sicurezza per prevenire attacchi basati su vulnerabilità note come **EternalBlue**.

- **Monitoraggio del traffico di rete:** Utilizzare strumenti di **Intrusion Detection System (IDS)** per identificare tempestivamente traffico sospetto e bloccare gli IP da cui provengono le scansioni o i tentativi di attacco.
- **Abilitazione del logging:** Configurare il sistema per registrare tutti i tentativi di accesso falliti, in modo da poter effettuare un'analisi forense in caso di compromissione e correlare gli eventi.

6. Prevenzione di attacchi futuri

Per prevenire simili attacchi in futuro, si suggerisce di:

- **Applicare una difesa in profondità:** Oltre a chiudere le porte non necessarie, implementare misure come la segmentazione della rete e il monitoraggio continuo per rilevare comportamenti anomali.
- **Formazione del personale:** Assicurare che gli amministratori di sistema comprendano le implicazioni della sicurezza dei servizi esposti e l'importanza di protocolli sicuri.
- **Pianificazione della risposta agli incidenti:** Preparare e testare piani di risposta agli incidenti per ridurre il tempo di reazione in caso di attacco.

Conclusioni

L'analisi della cattura di rete ha rivelato che la macchina **192.168.200.150** è potenzialmente sotto attacco. Il traffico anomalo, le porte aperte e i servizi vulnerabili indicano tentativi di scansione e possibile sfruttamento delle vulnerabilità. È essenziale intervenire tempestivamente con l'adozione di misure di sicurezza come la chiusura delle porte vulnerabili e il rafforzamento della rete per prevenire attacchi futuri.