

Obiettivo: Analizzare una cattura di rete effettuata con Wireshark:

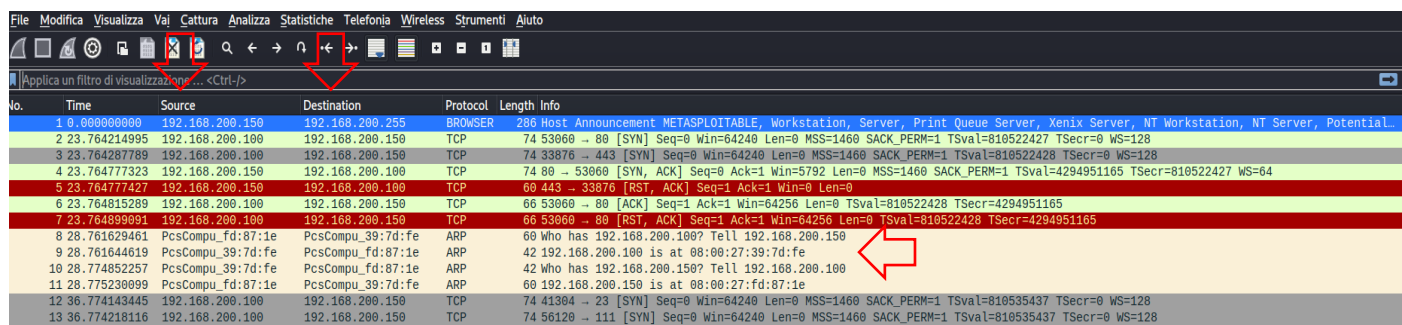
- Indentificare eventuali IOC, ovvero evidenziare attacchi in corso
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco

Prima Fase

Andiamo ad aprire con Wireshark la cattura fornita dalla traccia e possiamo notare già da subito dai pacchetti che visualizziamo che è stato eseguito un protocollo ARP sulla macchina attaccata. Quindi si è tentato di stabilire una connessione, lo notiamo anche dai protocolli TCP sulle varie porte, con lo scopo di ricevere informazioni o prendere il controllo da parte dell'attaccante sulla macchina target.

Inoltre, possiamo notare dalla prima riga dell'immagine seguente che nel protocollo browser ci viene specificato l'indirizzo ip source (attaccante) e l'indirizzo ip destination (target), di quest'ultimo possiamo vedere anche che si tratta dell'OS Metasploitable.

Questi segnali ci indicano la presenza di **IOC**, ovvero di **Indicatori di compromissione**.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	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...
2	23.764214955	192.168.200.100	192.168.200.150	TCP	74	53960 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 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=1 TSval=810522428 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53960 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 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	53960 → 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	53960 → 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	28.775239099	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=1 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=1 TSval=810535437 TSecr=0 WS=128

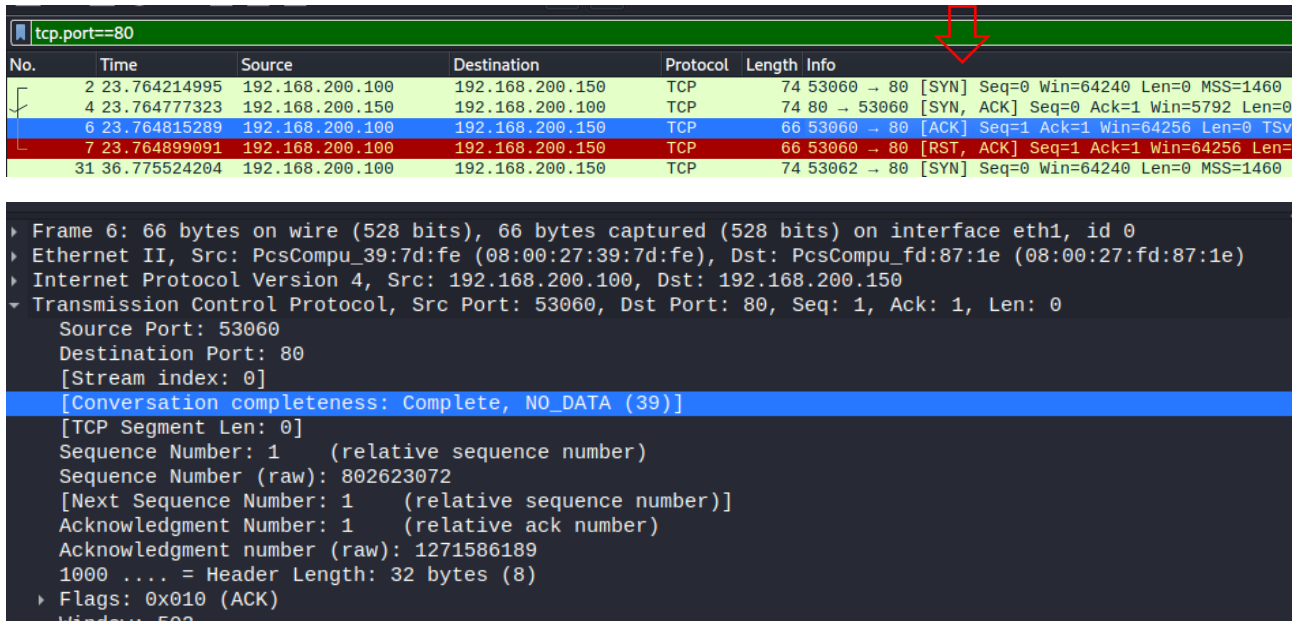
Possiamo ricavare ulteriori informazioni analizzando nel dettaglio il protocollo BROWSER, confermando le informazioni dell'host, come la versione e altri dettagli che abbiamo già detto.

```
► SMB MailSlot Protocol
▼ Microsoft Windows Browser Protocol
  Command: Host Announcement (0x01)
  Update Count: 1
  Update Periodicity: 2 minutes
  Host Name: METASPLOITABLE
  Windows version:
  OS Major Version: 4
  OS Minor Version: 9
  ► Server Type: 0x00019a03, Workstation, Server, Print, Xenix, NT Workstation, NT Server, Potential Browser
  Browser Protocol Major Version: 15
  Browser Protocol Minor Version: 1
  Signature: 0xaa55
  Host Comment: metasploitable server (Samba 3.0.20-Debian)
```

Seconda Fase

Analizzando nello specifico i protocolli TCP della cattura, nel caso specifico la porta 80 che sappiamo sia aperta su Metasploitable. Possiamo notare che viene appunto completata una connessione completa con il protocollo ARP, SYN/SYN-ACK/ACK detto anche three-way

handshake, da cui l'attaccante può ricavare il MAC della macchina oltre a poter sfruttarla per prendere il controllo del target.

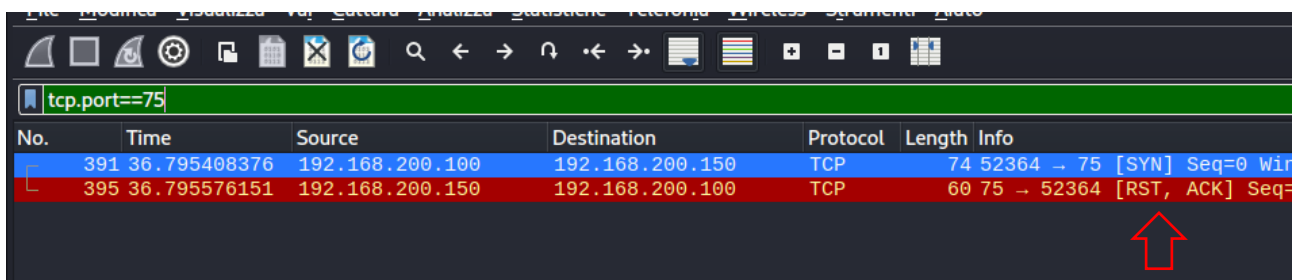


tcp.port==80

No.	Time	Source	Destination	Protocol	Length	Info
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [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
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
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460

Frame 6: 66 bytes on wire (528 bits), 66 bytes captured (528 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: 53060, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
Source Port: 53060
Destination Port: 80
[Stream index: 0]
[Conversation completeness: Complete, NO_DATA (39)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 802623072
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1271586189
1000 = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
Window: 502

Mentre prendendo in esame i pacchetti di una porta che sappiamo chiusa, vediamo che la connessione viene tentata ma poi resettata senza concludere il protocollo ARP.



tcp.port==75

No.	Time	Source	Destination	Protocol	Length	Info
391	36.795408376	192.168.200.100	192.168.200.150	TCP	74	52364 → 75 [SYN] Seq=0 Win=0 Len=0
395	36.795576151	192.168.200.150	192.168.200.100	TCP	60	75 → 52364 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0

Possiamo quindi dedurre che l'attaccante abbia effettuato una scansione sulla macchina target, con un tool scan come ad esempio nmap, per ricavare servizi e porte aperte. Questo lo possiamo dedurre proprio dai protocolli ARP sulle porte aperte, quindi, possiamo dire che l'attaccante abbia usato come vettore di attacco lo switch -sV e -sT per enumerare la versione dei servizi attivi, le porte aperte e per effettuare una scansione più invasiva che infatti si completa con il protocollo ARP e viene invece resettata dal flag di reset sulle porte chiuse.

Un'azione **per ridurre l'impatto dell'attacco** potrebbe essere quella di utilizzare il firewall di Metasploitable, iptables, per bloccare la scansione di un possibile attaccante così da non poter ottenere informazioni sulle porte che risulterebbero tutte filtrate.

Oppure un'altra soluzione è quella di inserire l'indirizzo ip dell'attaccante su una blacklist.

Abbiamo anche un altro metodo più veloce per analizzare le catture di wireshark, ovvero facendo decifrare il file PCAP online da siti che offrono questo servizio, ad esempio:

<https://apackets.com/>