PROGETTO S9/L5 YURI PEDRANA 07/02/2025

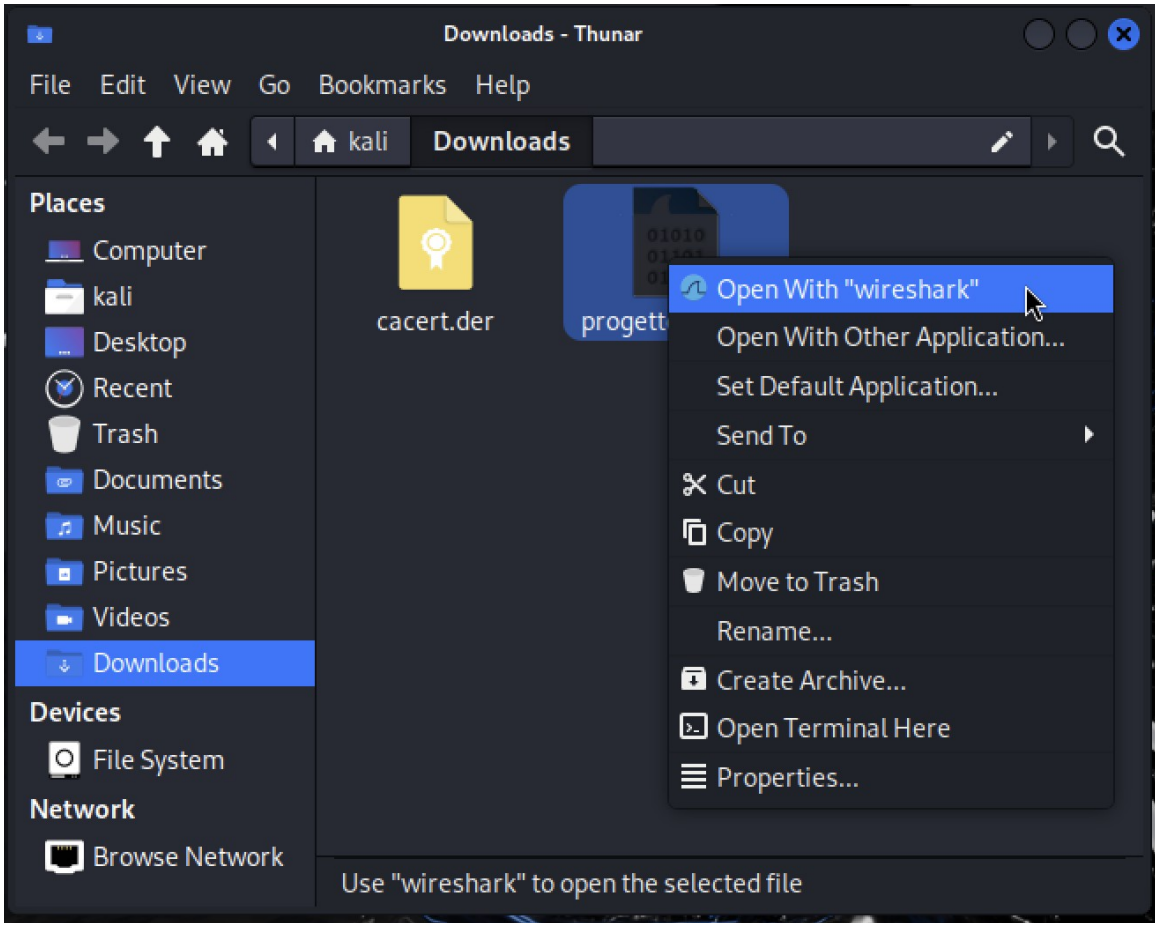
Per l’esercizio pratico di oggi, trovate in alle gato una cattura di rete effettuata con Wireshark. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

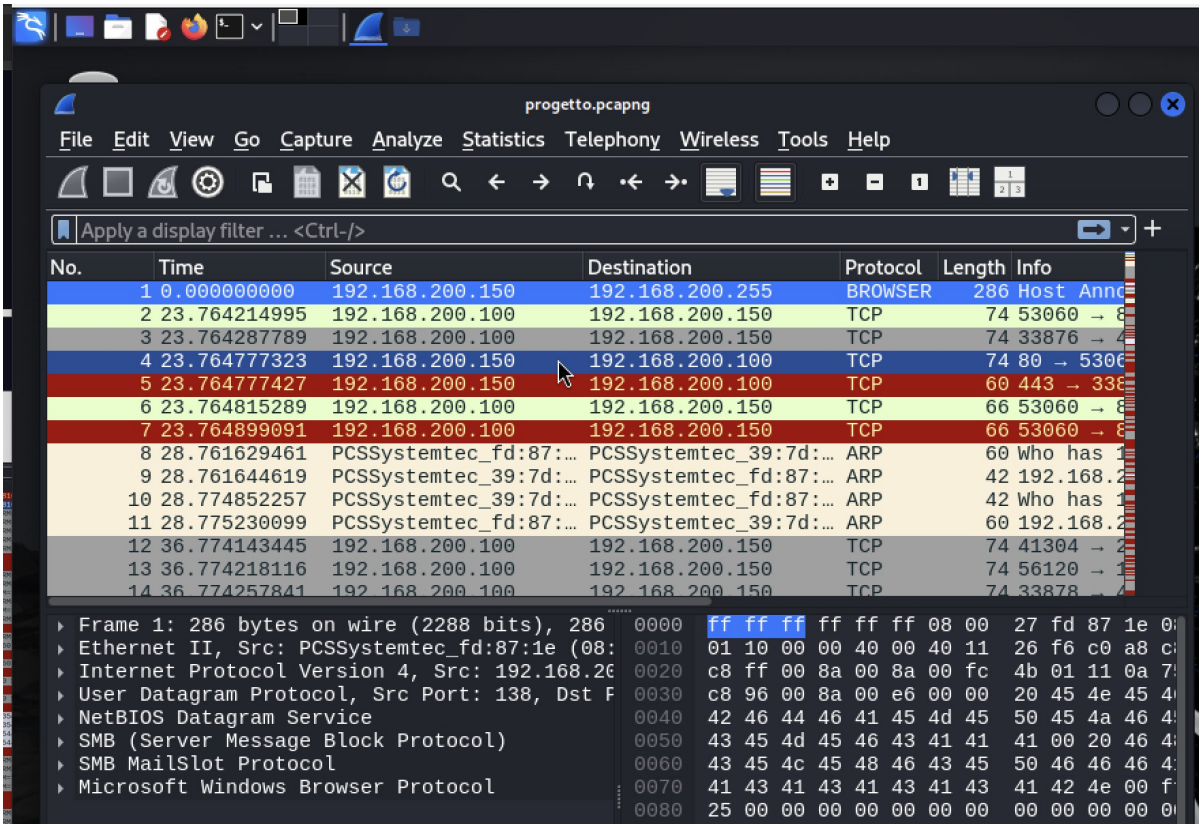
● Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso

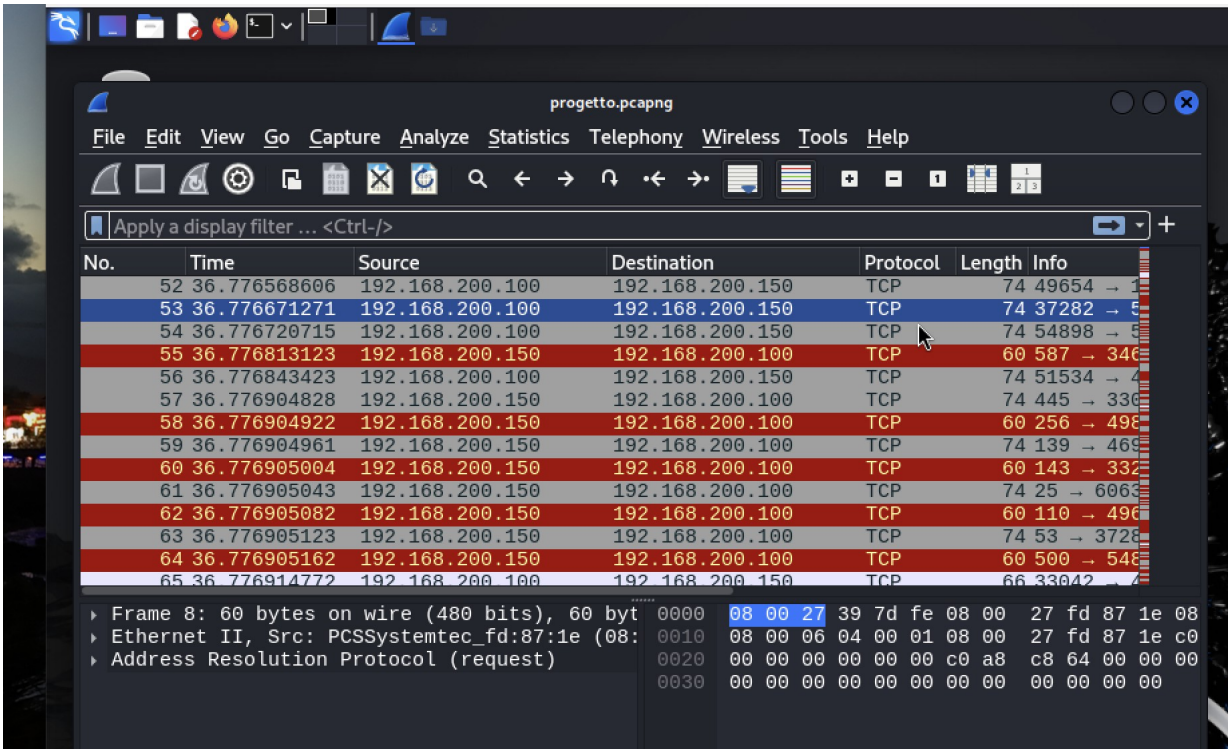
● In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati

● Consigliate un’azione per ridurre gli impatti dell’attacco attuale ed eventualmente un s imile attacco futuro

Procediamo con il download del file dannoso tramite il link fornito. Una volta completato il download, facciamo clic destro sul file e lo apriamo con Wireshark, come mostrato nell’immagine sottostante:




progetto.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.200.150 192.168.200.255 BROWSER 286 Host Anno
2 23.764214995 192.168.200.100 192.168.200.150 TCP 74 53060 →
3 23.764287789 192.168.200.100 192.168.200.150 TCP 74 33876 →
4 23.764777323 192.168.200.150 192.168.200.100 TCP 74 80 → 5306
5 23.764777427 192.168.200.150 192.168.200.100 TCP 60 443 → 338
6 23.764815289 192.168.200.100 192.168.200.150 TCP 66 53060 →
7 23.764899091 192.168.200.100 192.168.200.150 TCP 66 53060 →
8 28.761629461 PCSSystemtec_fd:87:... PCSSystemtec_39:7d:... ARP 60 Who has
9 28.761644619 PCSSystemtec_39:7d:... PCSSystemtec_fd:87:... ARP 42 192.168.2
10 28.774852257 PCSSystemtec_39:7d:... PCSSystemtec_fd:87:... ARP 42 Who has
11 28.775230099 PCSSystemtec_fd:87:... PCSSystemtec_39:7d:... ARP 60 192.168.2
12 36.774143445 192.168.200.100 192.168.200.150 TCP 74 41304 →
13 36.774218116 192.168.200.100 192.168.200.150 TCP 74 56120 →
Frame 1: 286 bytes on wire (2288 bits), 286
Ethernet II, Src: PCSSystemtec_fd:87:1e (08:
Internet Protocol Version 4, Src: 192.168.20
User Datagram Protocol, Src Port: 138, Dst P
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
Microsoft Windows Browser Protocol
0000 ff ff ff ff ff ff 08 00 27 fd 87 1e 0
0010 01 10 00 00 40 00 40 11 26 f6 c0 a8 c
0020 c8 ff 00 8a 00 8a 00 fc 4b 01 11 0a 7
0030 c8 96 00 8a 00 e6 00 00 20 45 4e 45 4
0040 42 46 44 46 41 45 4d 45 50 45 4a 46 4
0050 43 45 4d 45 46 43 41 41 41 00 20 46 4
0060 43 45 4c 45 48 46 43 45 50 46 46 46 4
0070 41 43 41 43 41 43 41 43 41 42 4e 00 f
0080 25 00 00 00 00 00 00 00 00 00 00 00 0


progetto.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
52 36.776568606 192.168.200.100 192.168.200.150 TCP 74 49654 →
53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 →
54 36.776720715 192.168.200.100 192.168.200.150 TCP 74 54898 →
55 36.776813123 192.168.200.150 192.168.200.100 TCP 60 587 → 346
56 36.776843423 192.168.200.100 192.168.200.150 TCP 74 51534 →
57 36.776904828 192.168.200.100 192.168.200.150 TCP 74 445 → 336
58 36.776904922 192.168.200.150 192.168.200.100 TCP 60 256 → 498
59 36.776904961 192.168.200.150 192.168.200.100 TCP 74 139 → 469
60 36.776905004 192.168.200.150 192.168.200.100 TCP 60 143 → 332
61 36.776905043 192.168.200.150 192.168.200.100 TCP 74 25 → 6063
62 36.776905082 192.168.200.150 192.168.200.100 TCP 60 110 → 496
63 36.776905123 192.168.200.150 192.168.200.100 TCP 74 53 → 3728
64 36.776905162 192.168.200.150 192.168.200.100 TCP 60 500 → 548
Frame 8: 60 bytes on wire (480 bits), 60 byt
Ethernet II, Src: PCSSystemtec_fd:87:1e (08:
Address Resolution Protocol (request)
0000 08 00 27 39 7d fe 08 00 27 fd 87 1e 08
0010 08 00 06 04 00 01 08 00 27 fd 87 1e c0
0020 00 00 00 00 00 00 c0 a8 c8 64 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00

Rosso: indica un pacchetto TCP **con errore** o un pacchetto **di reset** (RST), ovvero una connessione interrotta.

Blu: utilizzato per i pacchetti TCP **di comunicazione normale**, come quelli di richiesta e risposta.

Giallo: utilizzato per il traffico **UDP** o pacchetti relativi a protocolli come DNS o HTTP.

Panoramica della Lista dei Pacchetti:

Questa è la lista principale dei pacchetti catturati, ogni riga rappresenta un pacchetto catturato, le colonne mostrano:

• **No.**: Numero del pacchetto.

• **Time**: Il tempo in cui il pacchetto è stato catturato, rispetto all'inizio della cattura.

• **Source**: Indirizzo IP di origine.

• **Destination**: Indirizzo IP di destinazione.

• **Protocol**: Il protocollo usato (TCP, ARP, HTTP, ecc.).

• **Length**: La dimensione del pacchetto in byte.

• **Info**: Dettagli specifici del pacchetto (come il numero della porta o il tipo di richiesta).

Dettagli del Pacchetto Selezionato:

Quando selezioni un pacchetto dalla lista, nella parte inferiore della finestra vedrai una descrizione dettagliata del pacchetto. Ogni livello di protocollo (Ethernet, IP, TCP, ecc.) sarà separato da una sezione espandibile.

Ecco un esempio:

• **Ethernet II**: Mostra gli indirizzi MAC di origine e destinazione.

• **Internet Protocol (IP)**: Mostra l'indirizzo IP di origine e destinazione e altre informazioni.

• **Transmission Control Protocol (TCP)**: Mostra le informazioni sul tipo di connessione TCP, come il numero di sequenza, il flag (SYN, ACK), ecc.

• **Data**: Se il pacchetto contiene dati (ad esempio una richiesta HTTP), li vedrai qui.

Come attaccano?

Traffico insolito → Se vedi un dispositivo che manda tantissimi pacchetti in poco tempo, potrebbe essere un attacco.

Errori di connessione → Molti tentativi di connessione falliti possono indicare un attacco di scansione.

Richieste strane → Se vedi pacchetti con contenuti insoliti o protocolli usati in modo strano (es. richieste DNS sospette), potrebbe esserci qualcosa di malevolo.

Come difendersi?

Cerca di capire quale dispositivo sta generando il traffico anomalo.

Blocca o isola il dispositivo sospetto.

Usa un firewall per filtrare traffico pericoloso.