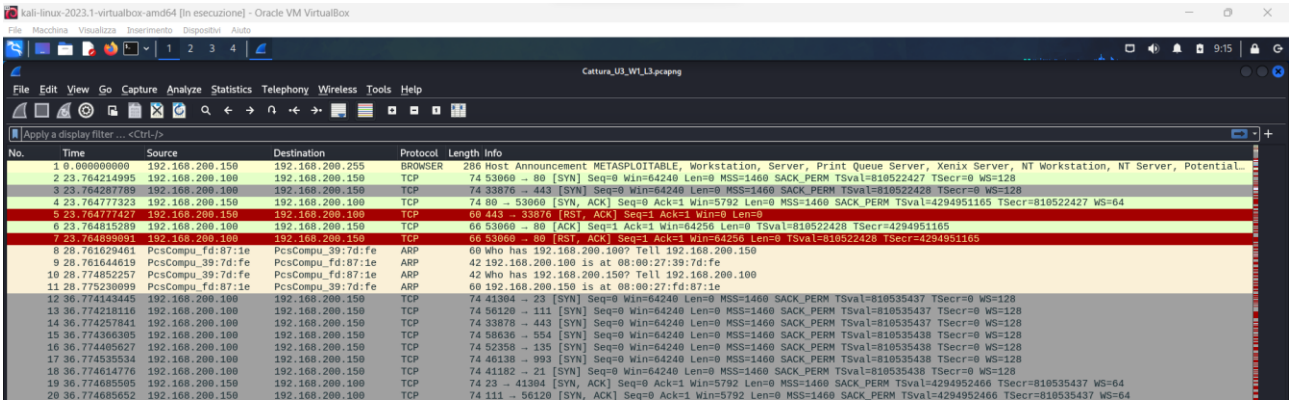
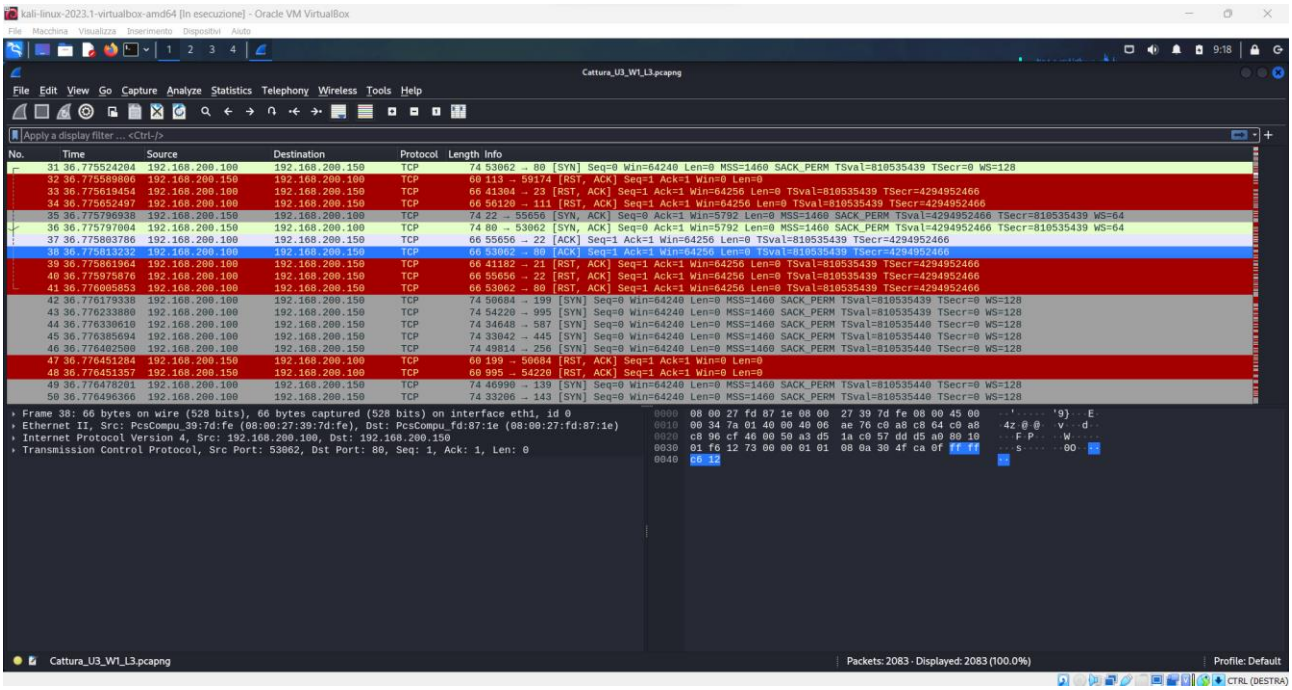
Epicode Unit 3 Day 3

L'esercizio odierno prevede lo studio di una scansione eseguita con Wireshark per individuare eventuali IoC sulla macchina scelta come bersaglio dell'attacco (Metasploitable).



Come si può notare dallo screen, una volta conclusa la fase di richieste ARP che andrà a mettere in comunicazione le due macchine (verosimilmente su rete interna), dalla macchina attaccante inizino una serie di richieste con Protocollo TCP che vanno a concludere il three-way-handshake.



Andando inoltre ad analizzare i pacchetti nel dettaglio possiamo verificare come moltissime porte (se non tutte) vengano prese "di mira" dalle richieste della macchina attaccante.

Alla luce di ciò possiamo supporre di aver intercettato una scansione di tipo "-sT" probabilmente eseguita da un tool come Nmap (se non proprio Nmap) per andare ad identificare le porte aperte sulla macchina bersaglio, probabilmente per andare poi a verificarne e sfruttarne successivamente le vulnerabilità.

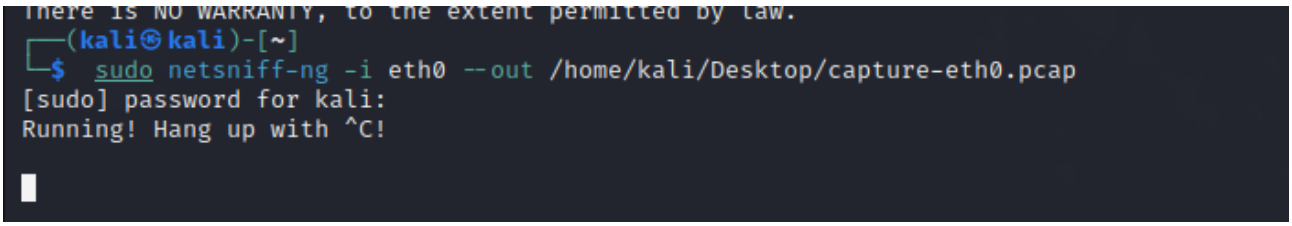
Potenziali azioni di rimedio:

Considerando le valutazioni precedentemente fatte, possiamo mitigare la minaccia in diversi modi:

- Blocco dell'Indirizzo IP da cui arrivano le richieste;
- Chiusura delle porte della macchina bersaglio sulle quali non "girano" servizi necessari per l'utente;
- Impostazione di una policy "DROP" dei pacchetti tramite una regola firewall;
- Eventuali aggiornamenti (patch) di servizi vulnerabili qualora possibile;
- Implementazione di un IDS per un eventuale "Double-Check" dei dati analizzati con Wireshark;
- Implementazione di un IPS per il blocco automatico dei paccheti (più efficace in teoria che in pratica, vista la probabilità di "falsi positivi".

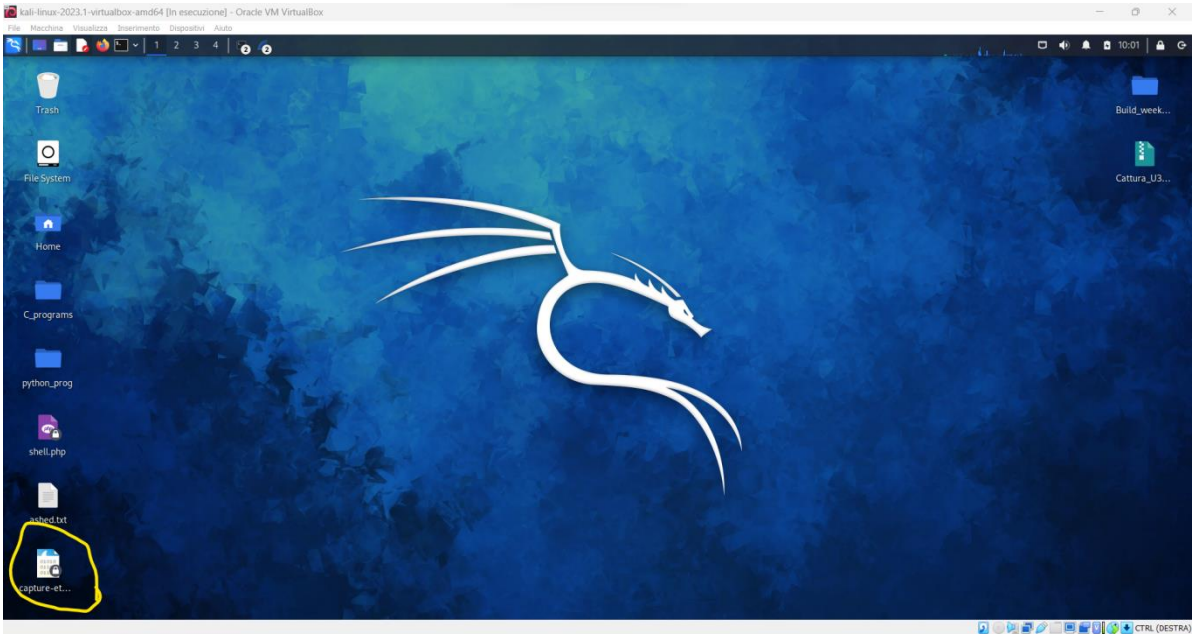
Controlli aggiuntivi:

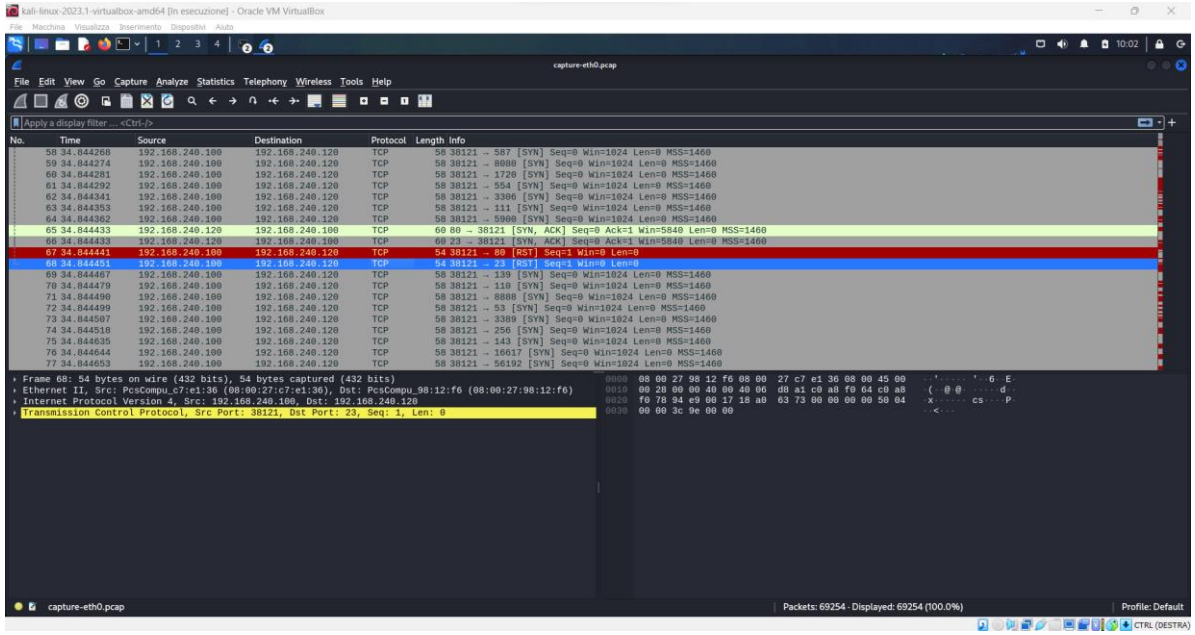
Qualora si decidesse di effettuare ulteriori controlli di Cross-Check per una maggiore sicurezza sull'affidabilità dei dati, si potrebbe inoltre decidere di utilizzare un secondo software di analisi, come ad esempio, per citarne soltanto uno, netsniff-ng.



Una volta avviato il tool, avvio una scansione di tipo –sS su nmap per riprodurre le condizioni dell'attacco. Con il comando sopra mostrato, non solo saremo in grado di visualizzare il traffico da terminale, bensì anche di consultarlo ogniqualvolta si vorrà sia da Desktop, sia da altri tool, come lo stesso Wireshark.

```
< eth0 60 1687960440s.769682562ns #44970
 [ Eth MAC (08:00:27:98:12:f6 ⇒ 08:00:27:c7:e1:36), Proto (0×0800, IPv4) ]
 [ Vendor (PCS Systemtechnik GmbH ⇒ PCS Systemtechnik GmbH) ]
 [ Eth trailer 0003c00 ]
 [ IPv4 Addr (192.168.240.120 ⇒ 192.168.240.100), Proto (6), TTL (64), TOS (0), Ver (4), IHL (5), Tlen (40), ID (0), Res (0), NoFrag (1), MoreFrag (0), FragOff (0), CSum (0×d8a1) is ok ]
 [ TCP Port (14017 ⇒ 38121), SN (0×0), AN (0×18a06373), DataOff (5), Res (0), Flags (RSTACK), Window (0), CSum (0×05e4), UrgPtr (0) ]

< eth0 60 1687960440s.769682607ns #44971
 [ Eth MAC (08:00:27:98:12:f6 ⇒ 08:00:27:c7:e1:36), Proto (0×0800, IPv4) ]
 [ Vendor (PCS Systemtechnik GmbH ⇒ PCS Systemtechnik GmbH) ]
 [ Eth trailer 0003c00 ]
 [ IPv4 Addr (192.168.240.120 ⇒ 192.168.240.100), Proto (6), TTL (64), TOS (0), Ver (4), IHL (5), Tlen (40), ID (0), Res (0), NoFrag (1), MoreFrag (0), FragOff (0), CSum (0×d8a1) is ok ]
 [ TCP Port (12014 ⇒ 38121), SN (0×0), AN (0×18a06373), DataOff (5), Res (0), Flags (RSTACK), Window (0), CSum (0×0db7), UrgPtr (0) ]

< eth0 60 1687960440s.769682659ns #44972
 [ Eth MAC (08:00:27:98:12:f6 ⇒ 08:00:27:c7:e1:36), Proto (0×0800, IPv4) ]
 [ Vendor (PCS Systemtechnik GmbH ⇒ PCS Systemtechnik GmbH) ]
 [ Eth trailer 0003c00 ]
 [ IPv4 Addr (192.168.240.120 ⇒ 192.168.240.100), Proto (6), TTL (64), TOS (0), Ver (4), IHL (5), Tlen (40), ID (0), Res (0), NoFrag (1), MoreFrag (0), FragOff (0), CSum (0×d8a1) is ok ]
 [ TCP Port (46701 ⇒ 38121), SN (0×0), AN (0×18a06373), DataOff (5), Res (0), Flags (RSTACK), Window (0), CSum (0×8637), UrgPtr (0) ]

< eth0 60 1687960440s.769682711ns #44973
 [ Eth MAC (08:00:27:98:12:f6 ⇒ 08:00:27:c7:e1:36), Proto (0×0800, IPv4) ]
 [ Vendor (PCS Systemtechnik GmbH ⇒ PCS Systemtechnik GmbH) ]
 [ Eth trailer 0003c00 ]
 [ IPv4 Addr (192.168.240.120 ⇒ 192.168.240.100), Proto (6), TTL (64), TOS (0), Ver (4), IHL (5), Tlen (40), ID (0), Res (0), NoFrag (1), MoreFrag (0), FragOff (0), CSum (0×d8a1) is ok ]
 [ TCP Port (42528 ⇒ 38121), SN (0×0), AN (0×18a06373), DataOff (5), Res (0), Flags (RSTACK), Window (0), CSum (0×9684), UrgPtr (0) ]

< eth0 60 1687960440s.769682760ns #44974
 [ Eth MAC (08:00:27:98:12:f6 ⇒ 08:00:27:c7:e1:36), Proto (0×0800, IPv4) ]
 [ Vendor (PCS Systemtechnik GmbH ⇒ PCS Systemtechnik GmbH) ]
 [ Eth trailer 0003c00 ]
 [ IPv4 Addr (192.168.240.120 ⇒ 192.168.240.100), Proto (6), TTL (64), TOS (0), Ver (4), IHL (5), Tlen (40), ID (0), Res (0), NoFrag (1), MoreFrag (0), FragOff (0), CSum (0×d8a1) is ok ]
 [ TCP Port (4313 ⇒ 38121), SN (0×0), AN (0×18a06373), DataOff (5), Res (0), Flags (RSTACK), Window (0), CSum (0×2bcc), UrgPtr (0) ]

< eth0 60 1687960440s.769682805ns #44975
 [ Eth MAC (08:00:27:98:12:f6 ⇒ 08:00:27:c7:e1:36), Proto (0×0800, IPv4) ]
 [ Vendor (PCS Systemtechnik GmbH ⇒ PCS Systemtechnik GmbH) ]
 [ Eth trailer 0003a00 ]
 [ IPv4 Addr (192.168.240.120 ⇒ 192.168.240.100), Proto (6), TTL (64), TOS (0), Ver (4), IHL (5), Tlen (40), ID (0), Res (0), NoFrag (1), MoreFrag (0), FragOff (0), CSum (0×d8a1) is ok ]
 [ TCP Port (16008 ⇒ 38121), SN (0×0), AN (0×18a06373), DataOff (5), Res (0), Flags (RSTACK), Window (0), CSum (0×fe1c), UrgPtr (0) ]
```





Come possiamo notare dagli screen soprastanti, anche in questo caso notiamo come le richieste TCP completino il three-way-handshake, confermando l'ipotesi di scansione -sT inizialmente proposta.