LABORATORIO 07 FEBBRAIO 2025 S9-L5

Threat Intelligence & IOC

Durante la lezione teorica, abbiamo visto la Threat Intelligence e gli indicatori di compromissione.

Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.

Esercizio Threat Intelligence & IOC Per l'esercizio pratico di oggi, trovate in allegato 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 simile attacco futuro

Traccia:

Per analizzare la cattura, spostate il file sulla vostra Kali Linux, e fate doppio-click, vi aprirà la cattura direttamente con Wireshark, dopo aver configurato i permessi per l'utente Kali.

Potete spostare il file sulla vostra Kali creando una cartella condivisa tra il vostro host e la Kali come la figura a destra. Vi basterà creare la cartella sul vostro sistema operativo, e configurare la cartella sulla macchina virtuale, specificando il percorso della cartella sul vostro Host ed il nome della cartella.

Da Kali potete accedere alla cartella (ed ai file in essa contenuti) navigando il file system alla directory /media. Come vedrete il nostro file è nella cartella condivisa.

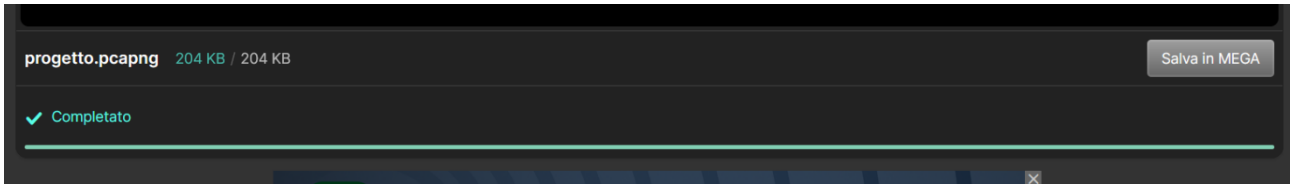
Da qui possiamo spostare il file sul desktop con il comando «mv» specificando il nome del file ed il path di destinazione, come visto nelle lezioni sul file system di Linux (il comando che abbiamo usato noi è nella figura a destra).

Successivamente assicuratevi che l'utente Kali possa aprire il file assegnando i permessi necessari.

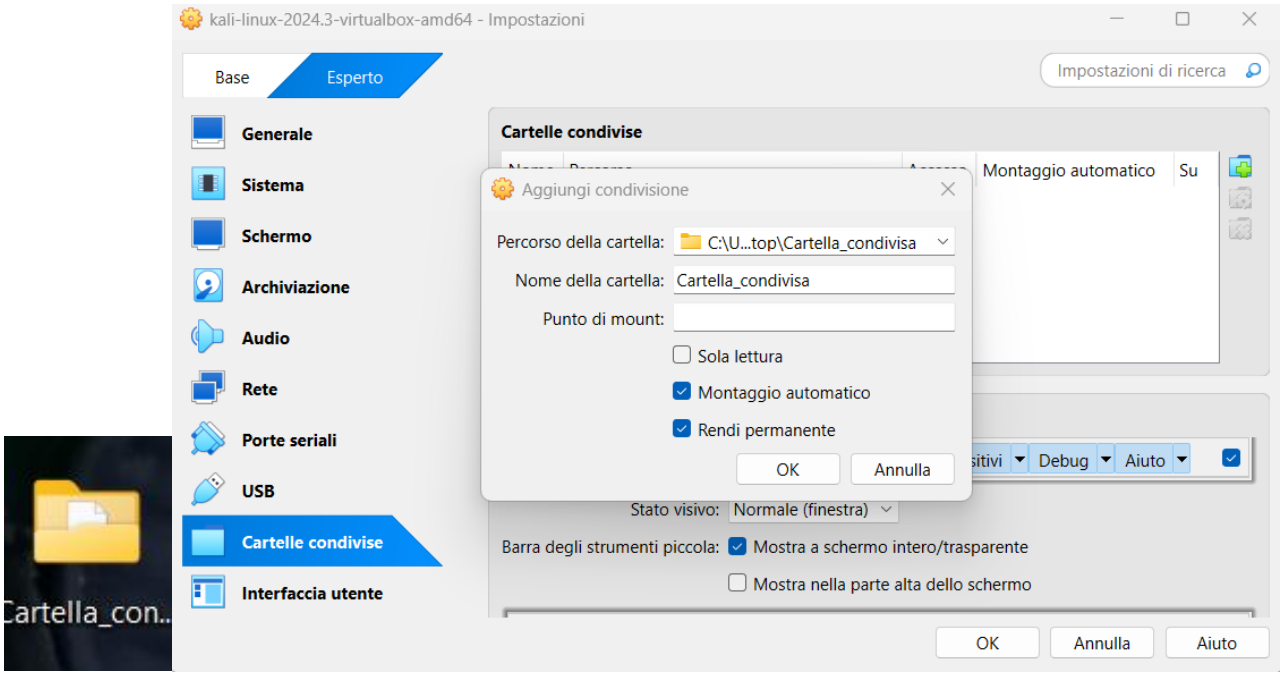
A questo punto fate doppio click per analizzare la cattura.

SVOLGIMENTO:

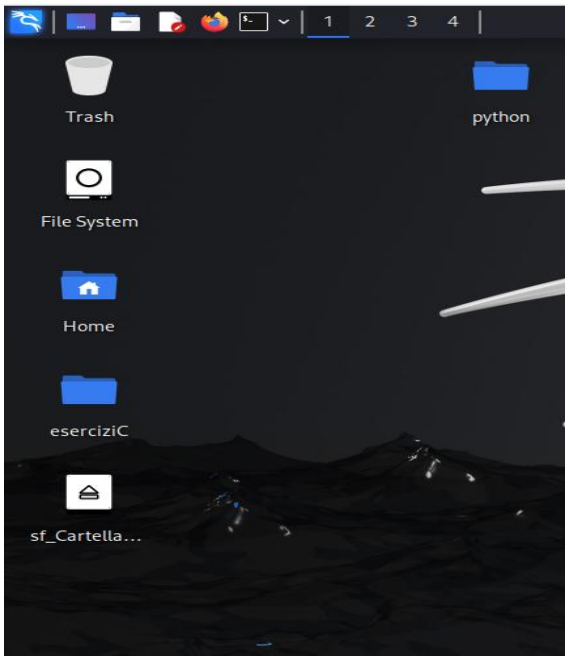
Iniziamo scaricando il file fornito.

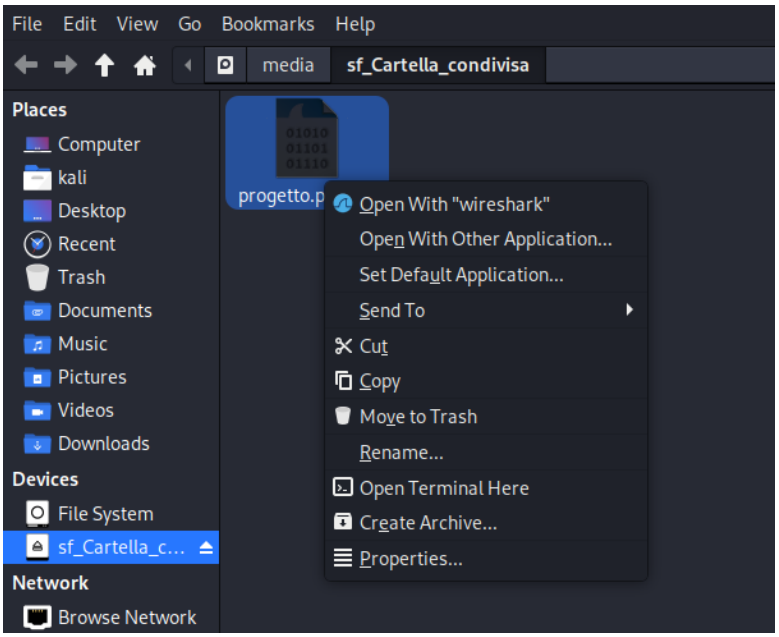


Creiamo una cartella condivisa ed aggiungiamo la condivisione tramite le impostazioni della macchina virtuale Kali.

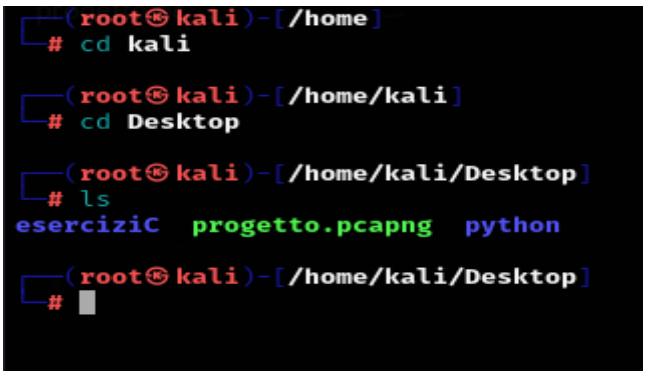


A questo punto avviamo Kali e vediamo che la cartella è comparsa sulla macchina. Possiamo aprirla e con il tasto destro abbiamo la possibilità di aprire il file con Wireshark per analizzarlo

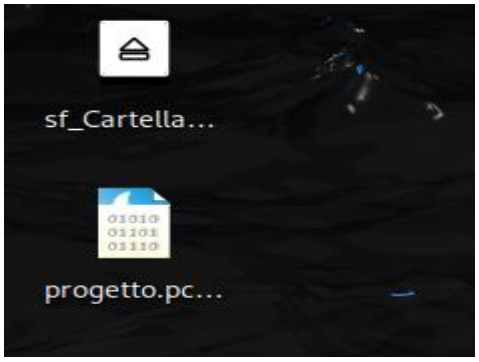




Scegliamo però di spostarci sul terminale e spostiamo il file nella directory Desktop.



Possiamo verificare che il file sia stato spostato dalla cartella condivisa al desktop.



Adesso assegniamo i permessi necessari affinché l' utente Kali possa aprire il file. Utilizziamo il comando specifico

chmod ugo+rw

che assegna i permessi di lettura e scrittura a tutti gli utenti su uno specifico file o directory.

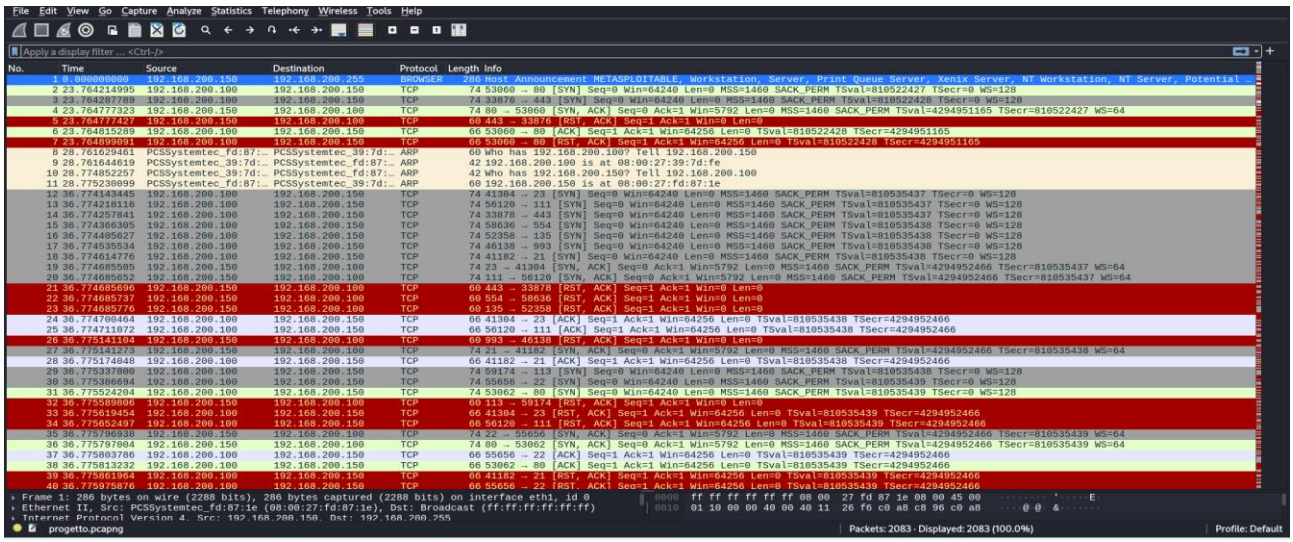
Nello specifico chmod sta per **change mode** ugo sta per **u** (**user**) **g** (**group**) **o** (**others**) e +rw aggiunge i permessi di lettura **r** e scrittura **w.**

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# chmod ugo+rw progetto.pcapng
```

A questo punto con il comando **chown (change owner)** cambiamo il proprietario del file.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# chown kali progetto.pcapng
```

Procediamo ora con l'apertura del file con il doppio click del mouse ed iniziamo ad analizzare la cattura.



Procediamo con la soluzione ai quesiti richiesti:

1: Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso.

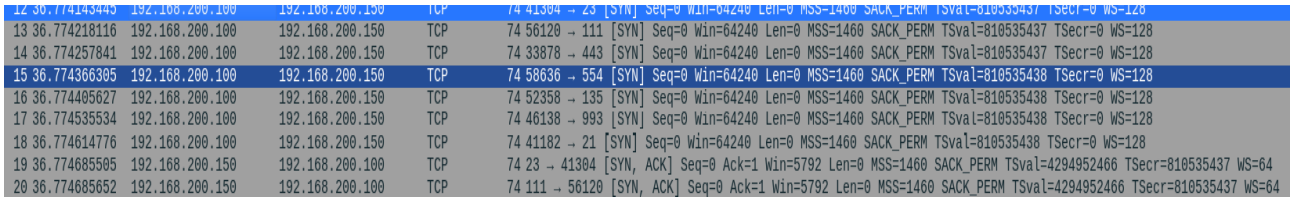
Gli IOC sono gli INDICATORI DI COMPROMISSIONE.

Da una prima occhiata possiamo stabilire che si tratti di una scansione delle porte da parte dell'attaccante con indirizzo IP 192.168.200.100 verso il target con IP 192.168.200.150

Quindi si tratta di dispositivi facenti parte della stessa rete.

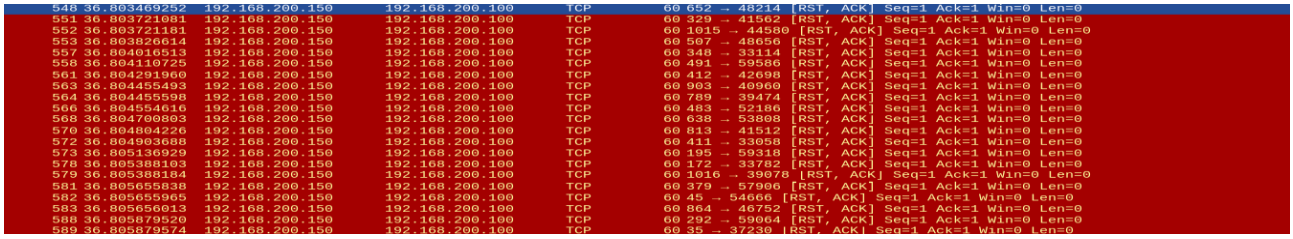
L' IP target è chiaramente una macchina Metaspoitable che è storicamente vulnerabile ed utilizzata per effettuare test e attacchi con relativa facilità tenendo molte porte aperte.

L' attaccante utilizzando il protocollo TCP invia pacchetti a tutte le porte cercando di stabilire una connessione (come possiamo vedere dai SYN inviati) per cercare eventuali porte aperte da attaccare e lo fa utilizzando a sua volta porte diverse per nascondere più possibile le sue tracce (tecnica stealth).

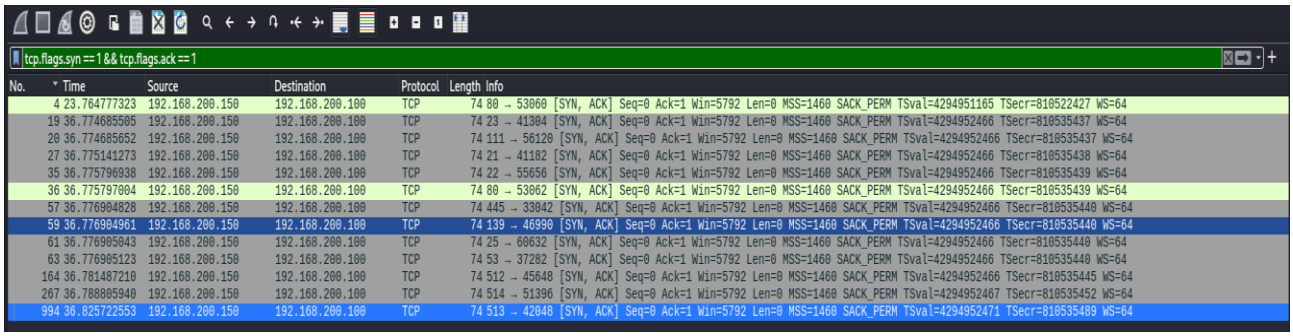


Nella maggior parte dei casi la richiesta viene rigettata come possiamo vedere non viene terminato il three-way-handshake.

A seguito dei SYN vediamo una risposta **RST ACK** che blocca la connessione immediatamente, probabilmente poiché la porta specifica è chiusa.



Applichiamo un filtro per trovare i pacchetti nei quali è stata stabilita la connessione tramite SYN-ACK.



Sebbene inizialmente è stata avviata la comunicazione, questa è stata interrotta anche in questi casi da una risposta RST ACK che

l’ha immediatamente interrotta. Probabilmente grazie a regole Firewall o ad un IDS.

Si nota quindi che ci sono varie porte aperte che possono essere attaccate e sono le seguenti.

21: FTP (File Transfer Protocol)

22: SSH (secure shell)

23: Telnet (accesso remoto)

25: SMTP (simple mail transfer protocol)

53: DNS (Domain Name System)

80: HTTP (Hypertext transfer protocol)

111: RPC (Remote Procedure Call)

139: NetBIOS (Network basic I/O system)

445: Samba (SMB server message block)

2: In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati.

Come detto il target è una macchina Metaspoitable e quindi soggetta ad attacchi su queste porte. Infatti sebbene la comunicazione è stata interrotta queste porte corrispondono a protocolli obsoleti e facilmente attaccabili. In base alle singole porte aperte trovate con la scansione effettuata in precedenza è possibile attaccare in moltissimi modi, avendo tutti questi protocolli delle vulnerabilità note ed essendo ormai obsoleti.

- Il protocollo FTP su porta 21 trasmette dati in chiaro, incluse le credenziali ed è quindi vulnerabile ad eventuali attacchi di intercettazione (sniffing) e man in the middle (MITM). Tra l'altro è anche privo di crittografia.
- Il protocollo SSH su porta 22 è di per se molto sicuro in quanto utilizza crittografia forte, l'autenticazione sicura e gli algoritmi di hashing (come SHA-2) ma deve essere configurato in modo corretto.
- Il protocollo Telnet su porta 23 è privo di crittografia e di autenticazione forte e come FTP è a rischio di MITM e sniffing.
- Il protocollo SMTP su porta 25 è responsabile dell'invio mail quindi può essere utilizzato per spam o phishing.
- Il protocollo DNS su porta 53 serve per navigare sul web utilizzando nomi degli host invece che indirizzi IP. E' vulnerabile al DNS tunneling che rappresenta una delle modalità tra le più insidiose per eludere i sistemi di difesa tradizionali, sfruttando il protocollo DNS per canalizzare dati malevoli attraverso firewall e sistemi di rilevamento o per esfiltrare dati.
- Il protocollo HTTP su porta 80 presenta vulnerabilità note in quanto le comunicazioni sono trasmesse in chiaro e quindi facilmente intercettabili.
- Il protocollo RCP su porta 111 è utilizzato per la comunicazione tra sistemi diversi e le sue vulnerabilità possono essere sfruttate per ottenere l'accesso non autorizzato o per eseguire codici malevoli.
- Il protocollo NetBIOS su porta 139 fornisce un API utilizzata per la condivisione di file, cartelle e stampanti su sistemi

Windows. Se esposta alle reti può fornire informazioni dettagliate, come nomi dei dispositivi e risorse condivise sfruttabili dagli attaccanti.

- Il protocollo Samba (o SMB) sulla porta 445 è utilizzato per la condivisione di file e stampanti tra diversi sistemi operativi. Ci sono delle configurazioni non sempre corrette che lo rendono vulnerabile, ad esempio mancanza di crittografia o esposizione in reti non protette.

3: Consigliate un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro.

Innanzitutto è bene procedere con una scansione antivirus per rilevare eventuali malware.

Bisogna poi chiudere le porte aperte se non necessarie, altrimenti utilizzare protocolli più sicuri o implementare le misure di sicurezza su quelli presenti.

- Utilizzare FTPS, invece di FTP, che utilizza crittografia avanzata e previene MITM.
- SSH: Applicare patch di sicurezza ed aggiornare il software, abilitare solo metodi di autenticazione sicuri come chiavi pubbliche o certificati, monitorare le connessioni e analizzare i log.
- Telnet è obsoleto ed è stato sostituito da SSH a causa delle sue vulnerabilità. E' quindi consigliato disabilitarlo.

- Implementare le tecniche di filtraggio e autenticazione su SMTP per ridurre il rischio di spam, assicurarsi che le comunicazioni siano crittografate utilizzando TLS, utilizzare autenticazione forte come ad esempio quella a due fattori.
- Utilizzare DNSSEC per aumentare la sicurezza dei DNS tramite firme crittografiche e scambio di chiavi.
- Preferire il protocollo HTTPS invece di HTTP che utilizza sistemi di cifratura, certificati digitali per autenticare il server e meccanismi di hashing.
- Aggiornare il protocollo RCP con implementazioni affidabili come autenticazione forte e crittografia. Configurare una regola Firewall per limitarne l'accesso non autorizzato.
- Preferire il protocollo TCP/IP o DNS a NetBIOS in quanto più sicuri e scalabili. Limitarne altrimenti l'utilizzo alle sole reti interne.
- Per quanto riguarda Samba, implementare misure di sicurezza come una robusta autenticazione e la crittografia, limitare l'accesso solo a segmenti di rete fidati, analizzare log e accessi ed effettuare aggiornamenti regolari con le ultime patch di sicurezza.

Misure preventive ulteriori per futuri attacchi possono essere quindi:

Implementazione di Firewall e IDS con accessi limitati ai soli IP autorizzati.

Aggiornamenti costanti di sistemi operativi e software di sicurezza.

Backup frequenti.