RELAZIONE
BHANTOOA RITISH

INDICE

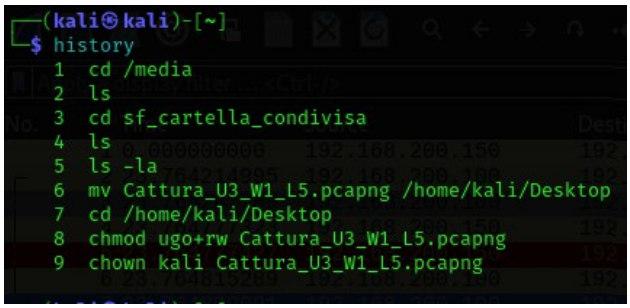
1. INTRODUZIONE ALL'ESERCIZIO

Per l'esercizio pratico di oggi, trovate in allegato una cattura di una rete effettuata con Wireshark. Analizzate la cattura attentamente e risponde ai seguenti quesiti:

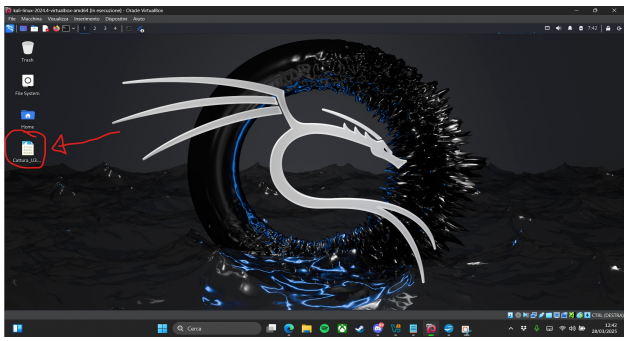
- Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso;
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati;
- Consigliate un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simeole attacco futuro.

2. SVOLGIMENTO DELL'ESERCIZIO TRAMITE WIRESHARK

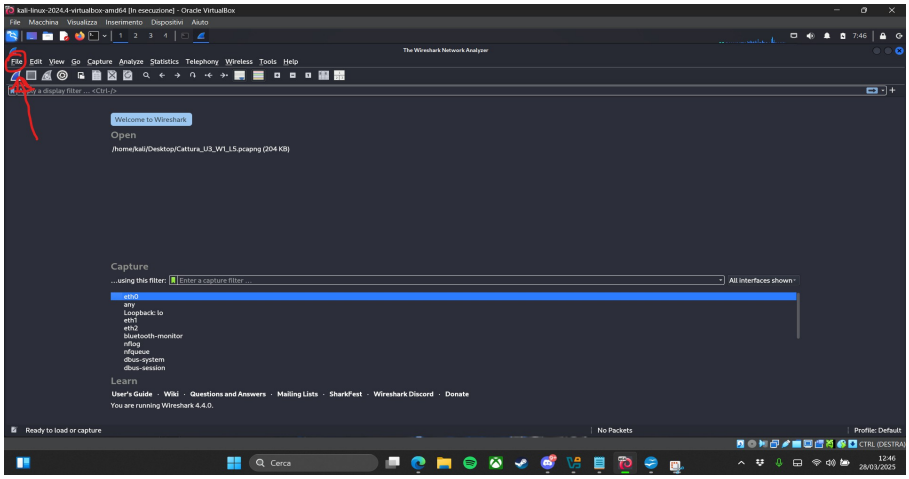
Prima di poter analizzare la cattura, creiamo una cartella, che renderemo condivisa dalle impostazioni della macchina virtuale di kali. Dopo avre creato questa cartella da terminale kali inseriamo questi comandi per fare in modo che la cartella compaia sul nostro desktop



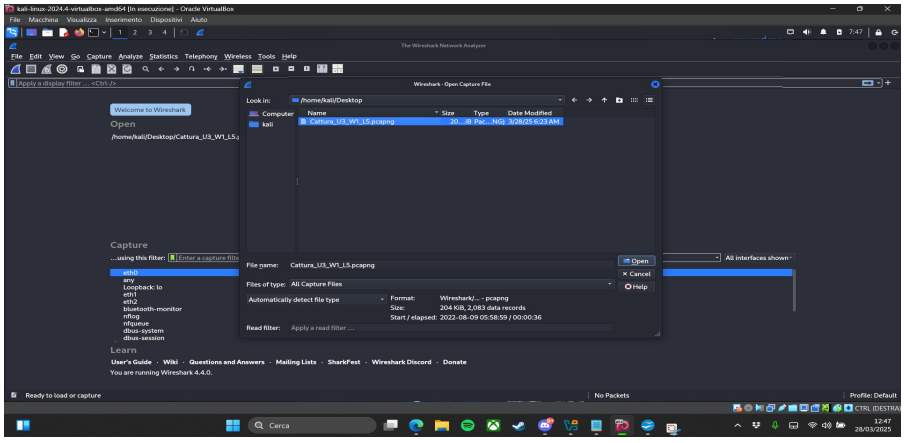
cosi che poi il file possa comparire nel desktop



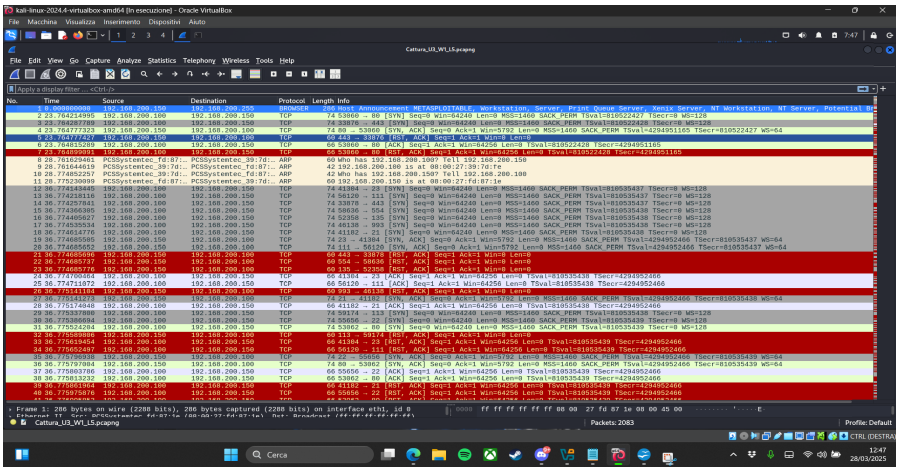
Una volta riusciti ad avere questo file, apriamo Wireshark e andiamo ad aprire la cartella condivisa



Andiamo su **File** e digitiamo su **Open** ci comparirà questa finestra, dove andremo a scegliere il file della cartella condivisa che dovrà aprire



Una volta aperto i file avremo una schermata in cui vedremo tutti i log



3. POSSIBILI IPOTESI

Dopo un'attenta analisi dell'attacco, siamo riusciti a stilare le seguenti ipotesi:

- Probabilmente l'attacco che viene eseguito è una semplice scansione delle porte.
- L'IP 192.168.200.150 risulta essere l'indirizzo del server, a sua volta quindi l'indirizzo 192.168.200.100 è l'attaccante.
- Come vediamo nella prima riga, viene fatta una scansione broadcast sugli host, quello che si espone è Metasploitable, macchina attraverso la quale poi, probabilmente, verrà fatta una scansione delle porte tramite protocollo TCP e ARP.
- Come vediamo, abbiamo delle connessioni 3 way handshake, molte connessioni vengono accettate, probabilmente anche grazie a delle porte aperte, presentando delle richieste di sincronizzazione (SYN), seguite da un risposta del destinatario (SYN-ACK), avendo poi una risposta dal mittente (ACK) e infine abbiamo la connessione stabilita e un possibile pacchetto mandato (RST-ACK). In molte righe invece viene mandata una richiesta di sincronizzazione che poi però viene fermata dall'attaccante stesso o dal server, non completando quindi il 3 way handshake.
- Dopo aver ipotizzato queste cose, possiamo quindi ipotizzare di tre possibili situazioni riguardanti l'attaccante:

1. Si tratta di un pentesting;
2. Potrebbe essere una persona all'interno di un'azienda;
3. L'attaccante è una persona al di fuori dell'azienda che cerca di accedere alla rete tramite una scansione delle porte per capire quale di queste sia aperta.

- La macchina con indirizzo 192.168.200.150 viene isolata.

4. SOLUZIONI

Nel caso in cui l'attaccante sia una persona esterna all'azienda che cerca appunto di entrare nella rete, possiamo utilizzare:

- **Firewall di rete**, la scelta più plausibile e migliore, questo decide quale traffico di rete può passare e quale è pericoloso, separando quindi il buono dal cattivo, riescono a filtrare i pacchetti, esaminando quest'ultimo, inclusi gli IP, decidendo poi il da farsi attraverso delle regole, garantendo così una sicurezza della rete migliore, gestiscono anche l'accesso remoto ai sistemi e ai software aziendali sulla rete, inoltre suddivide questa rete in reti segmentate, aiutando cosi a prevenire possibili presenze di malware e altre intrusioni.
- L'altra idea, ma meno efficace, è l'implementazione di sensori **ids/ips**, questi però come appunto detto risultano essere meno efficaci, visto che si concentrano sulla rilevazione e risposta a comportamenti sospetti all'interno del traffico già autorizzato, inoltre questi senosri richiedono una configurazione più complessa, presentano più risorse, quindi un costo più elevato rispetto ad un firewall, dato che sono più sofisticati. I sensori ids/ips sebbene offrano una protezione reattiva, non sono sempre efficaci nel prevenire le intrusioni iniziali. Anche se in molte aziende vengono usati sia firewall che senosri ids/ips per avere una sicurezza multilivell, così che il firewall fungerebbe da barriera principale, mentre gli ids/ips monitoreranno le minacce interne e fornire avvisi in caso di attività sospette.
- Un'altra idea è quella di una buona e continua **formazione del personale**, così da potersi accorgere tempestivamente di possibili intrusioni e prendere le contromisure adeguate.

Possiamo quindi dire che per avere una sicurezza maggiore, piè efficace, meno costosa e più facile da configurare, potremo implementare un firewall. Sennò per essere più sicuro potremo seguire le ultime righe di prima in cui veniva detto che molte aziende usano entrambi, avendo così, maggiore sicurezza ed efficacia, ma maggiori i costi.

5. CONCLUSIONI

In conclusione possiamo dire che grazie alla nostra lezione teorica, siamo riusciti a capire che gli IOC rappresentano gli elementi chiave nell'identificazione di eventi legati ad attacchi informatici, sia che si tratti di attacchi in corso che di incidenti già avvenuti.

Nell'esercizio di oggi siamo riusciti ad analizzare una cattura di rete effettuata con Wireshark, notando la presenza di un'attività malevole, che ci ha permesso di formulare ipotesi sull'attacco.

Infine, una volta formulate le nostre ipotesi, abbiamo pensato a dei modi per ridurre questi e possibili attacchi futuri, attraverso l'implemtazione di firewall, sensori ids/ips o una continua formazione del personale, punti fondamentali per una maggiore sicurezza della rete.