S9_L3
Unit 3 - CS0424

MATTEO BELTRAMI MARZOLINI
CYBEREAGLES

Giorno 3 – Threat Intelligence & IOC

TRACCIA

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.

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 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

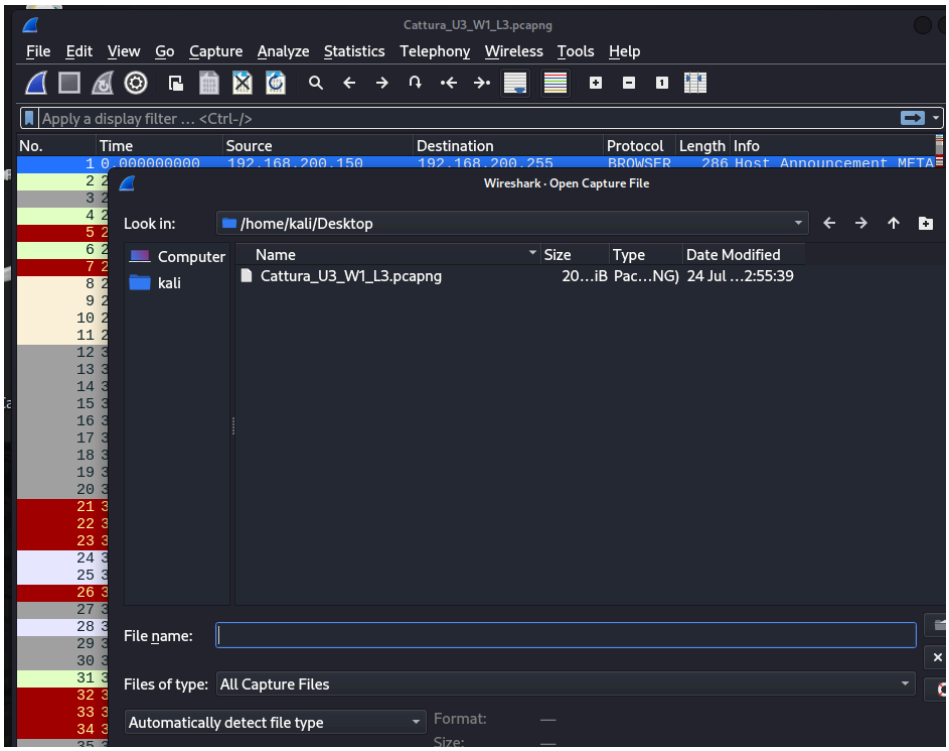
SVOLGIMENTO

Per svolgere l'esercizio come richiede la traccia, possiamo dividere il lavoro in 4 step,

1. Aprire il file su Wireshark
2. Identificare ed analizzare gli IOC
3. Le possibili ipotesi sui vettori d'attacco
4. Consigli per ridurre l'impatto dell'attacco

STEP 1: WIRESHARK

Si procede caricando il file ***Cattura_U3_W1_L3.pcapng*** su WireShark.

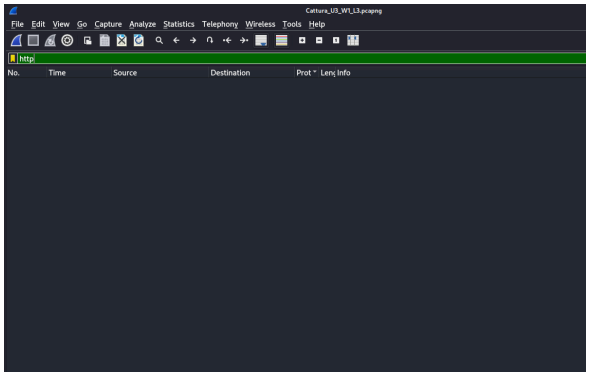


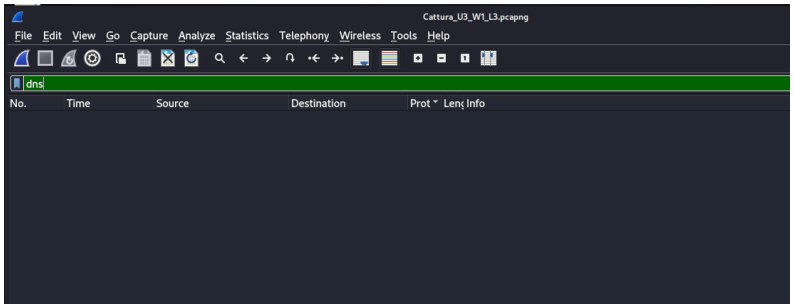
FILE > OPEN e selezionando il nostro pcapng.

STEP 2: Identificazione degli IOC

Successivamente tramite il filtro di WireShark possiamo cominciare ad esaminare i pacchetti utilizzando filtri di visualizzazione per concentrarsi su specifici protocolli o tipi di traffico (ad esempio, **http, dns, tcp, udp**).

Identificando il traffico sospetto si procede nel inserire nel filtro i vari protocolli.



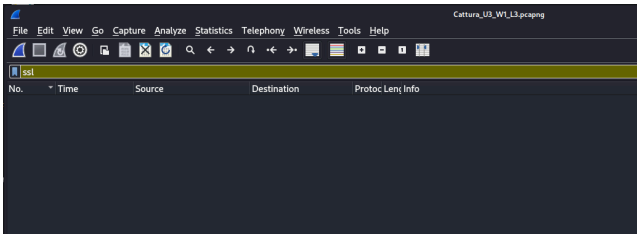


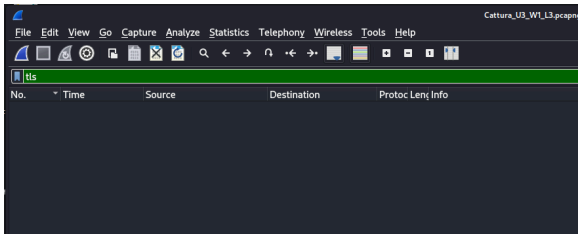
Come si può notare per **HTTP** e **DNS** non si sono trovati pacchetti, questo vuol dire che non ci sono richieste insolite o anomale verso domini sconosciuti.

Però analizzando il traffico riguardante la **porta 80**, in quanto è collegato al HTTP, scopriamo degli insoliti pacchetti, che fanno capire che c'è stata un'interazione con essa.

Prima di concentrarsi sulla porta 80 si procede nel controllare se c'è la presenza di altri pacchetti sospetti.

`ssl` e **`tls`**

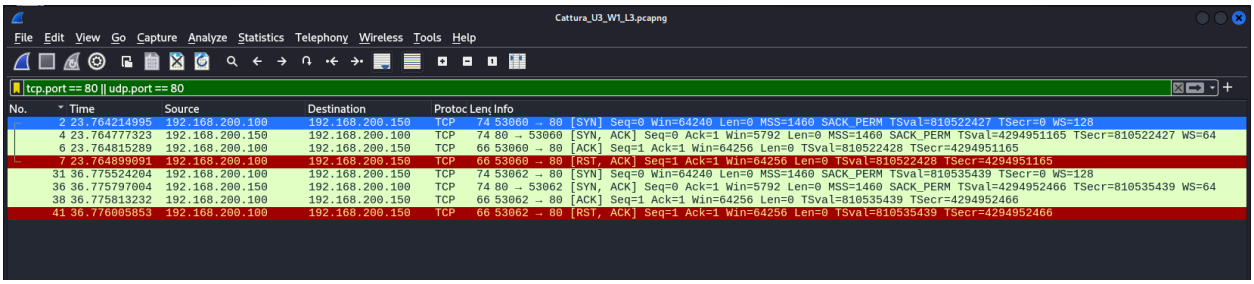




Dopo aver controllate la presenza di altri possibili pacchetti, ma senza risultati, ritorniamo sulla porta 80.

Sul filtro per cercare pacchetti riguardanti la connessione della porta 80, è stato inserito:

tcp.port == 80 || udp.port == 80



Con il quale noteremo un comportamento insolito riguardante un invio di pacchetti sulla porta 80.

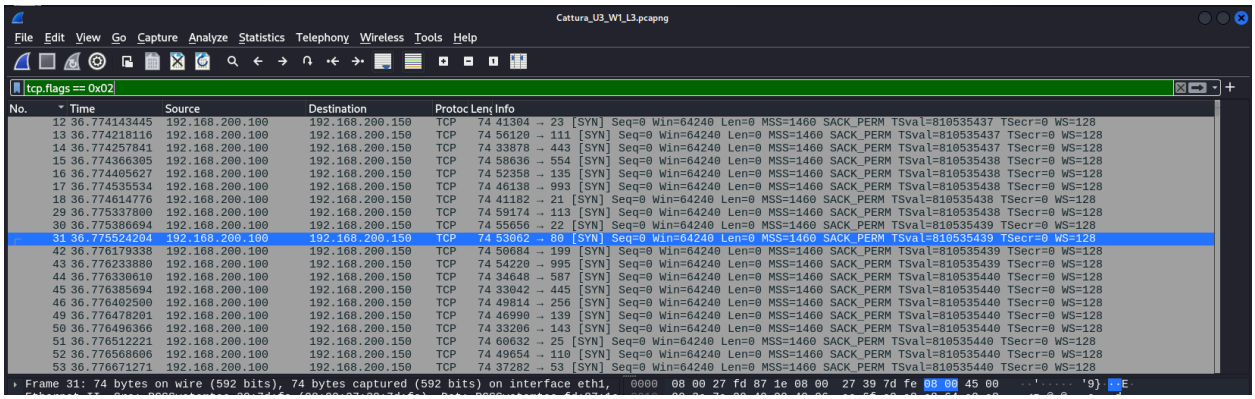
STEP 3: Identificazione del vettore d'attacco

Si procede, quindi, ad indagare quali sono i vettori di attacco.

Tra le varie possibilità possiamo controllare tramite il follow tcp, oppure impostando nei filtri GET e POST. Però in tutti i casi i risultati sono fuorvianti o senza successo.

Una possibile causa di questi insoliti pacchetti potrebbe riguardare un possibile attacco di port scanning.

Per confermare questa ipotesi, nel filtro utilizziamo ***tcp.flags == 0x02***



Noteremo infatti un quantitativo molto alto di SYN confermando che la scansione di WireShark riguarda un port scan.

Noteremo infatti anche la presenza si SYN ad altre porte, comprendendo che in questa scansione troviamo un attacco per ricercare la presenza di porte vulnerabili e specifiche. Notando inoltre le risposte della macchina, confermando la presenza di diverse porte aperte.

STEP 4: Consigli per ridurre l'impatto dell'attacco

Secondo ciò che è stato analizzato si consiglia di bloccare i possibili IP sospetti, ovvero quello presente nell'invio di pacchetti. Quindi si consiglia di installare e configurare correttamente il Firewall per evitare possibili attacchi simili in futuro e monitorando costantemente il traffico di rete per identificare ulteriori attività sospette. Eseguire un Audit e Vulnerability Scan completo sui sistemi può essere utile per identificare e correggere eventuali vulnerabilità. E non da sottovalutare, la formazione del personale IT nella rilevazione agli attacchi di rete può implementare la risposta agli incidenti per affrontare rapidamente eventuali minacce.