THREAT INTELLIGENCE & IOC

L9-L3

GIULIA FIACCHI

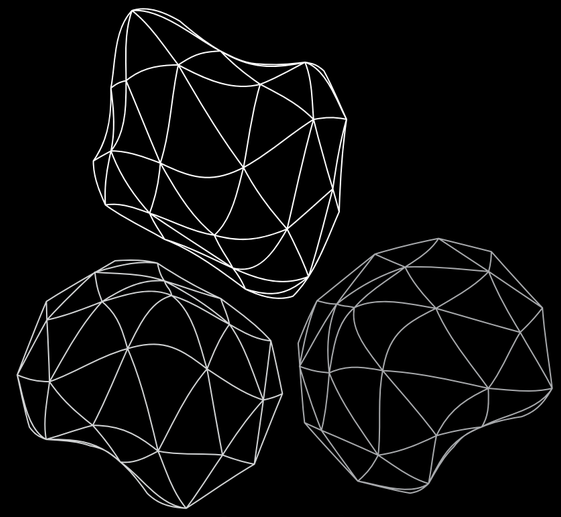
TRACCIA

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

PARTE 1

IDENTIFICARE EVENTUALI IOC

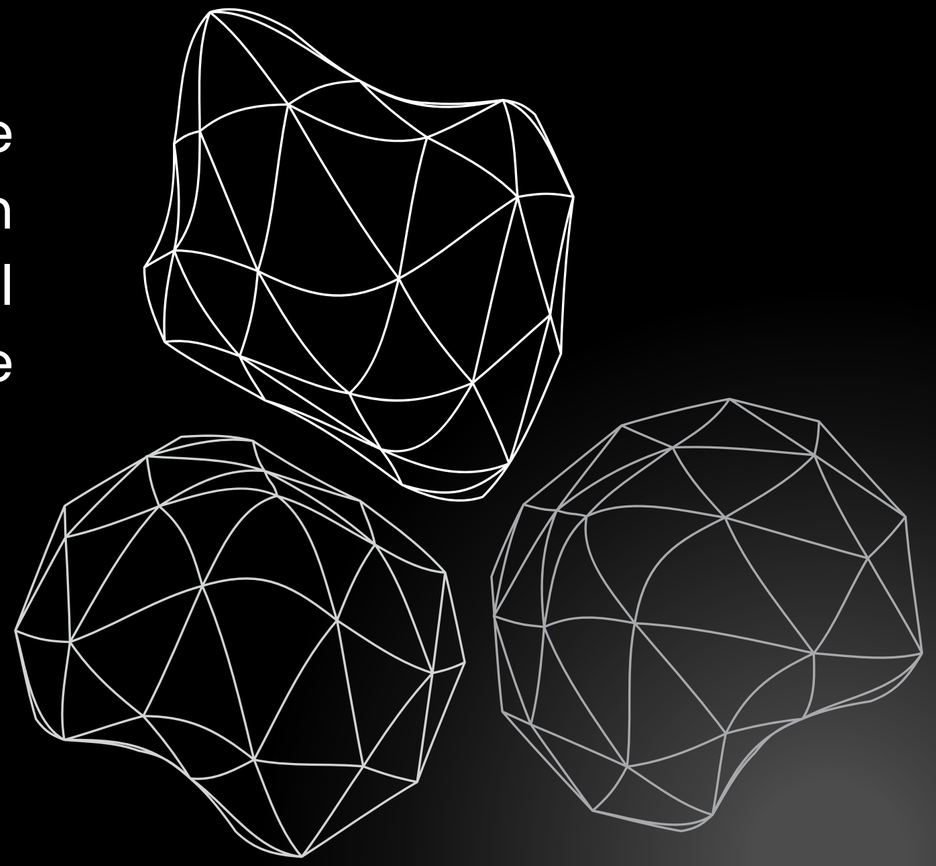


Data l'analisi del traffico di rete tramite il tool Wireshark, è possibile notare che vi sono molteplici tentantivi di connessione tramite pacchetti ARP e RST-ACK.
Il primo è utile per tentare una connessione e in particolare ciò avviene tra gli IP 192.168.200.100 e 192.168.200.150 ma, con i pacchetti RST si denota che la connessione viene interrotta (il loro compito è infatti quello di interrompere o non permettere la connessione quando sospetta).
Inoltre vi è il tentativo di connessione su porte comuni: 80 HTTP - 443 HTTPS comunemente utilizzate per il traffico web.
Molto sospetto rimane l'annuncio del pacchetto 1 in particolare dell'host 192.168.200.255 associato solitamente a Metasploitable (ambiente utilizzato per gli ambienti di test).
Ancora mostra molteplici tentativi di connessione TCP con flag SYN che non vanno a buon fine.

PARTE 2

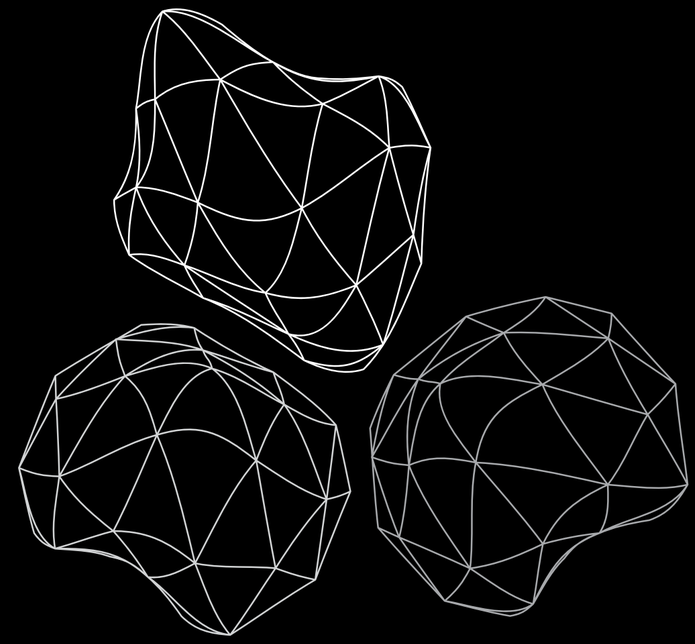
VETTORI DI ATTACCO UTILIZZATI

I possibili vettori di attacco sono il tentativo di scansione delle porte per identificare i servizi web (80, 443) con tentativi di connessione tramite brute force e anche il potenziale tentativo di intercettare traffico di rete tramite spoofing delle tabelle ARP



PARTE 3

AZIONE PER RIDURRE GLI IMPATTI DELL'ATTACCO



Le azioni consigliate per ridurre gli impatti dell'attacco sono:

- implementazione del firewall andando a bloccare i tentativi di connessione della porta 80 e 443;
- implementare sistemi di rilevamento e prevenzione delle intrusioni per monitorare e bloccare attività sospette (IDS/IPS);
- monitorare le richieste ARP;
- isolare e analizzare gli IP sospetti