ESERCITAZIONE W19D4



Threat Intelligence & IOC

Traccia:

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

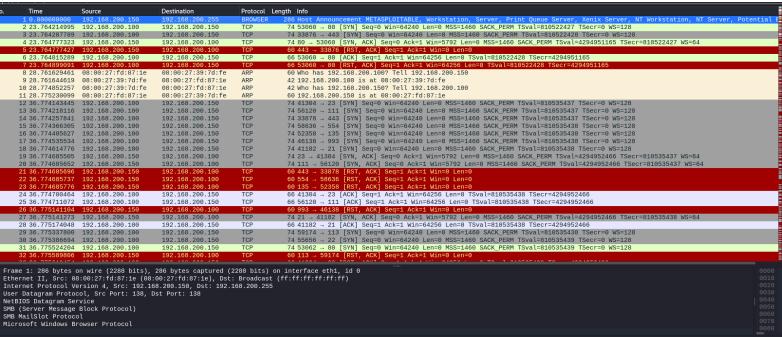
Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.

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

Cattura_U3_W1_L3.pcapng

Cattura di Wireshark contenuta nel file:



Guardando da vicino i pacchetti, notiamo un insospettabile tentativo di connessione in stile three-way handshake. Ogni porta viene sottoposta al processo, proveniente dall'indirizzo IP 192.168.200.100 e diretto verso l'IP 192.168.200.150. Questo suggerisce chiaramente un'attività di scansione delle porte sulla vittima, usando una scansione TCP. Il tipo di scansione può essere dedotto dal pacchetto inviato: un pacchetto ACK suggerisce una strategia diversa rispetto a un pacchetto RST, che segnalerebbe un abbandono del tentativo di connessione con la porta. Una soluzione potrebbe essere l'implementazione di regole nel firewall per filtrare le porte, nascondendole alle scansioni degli aggressori.