Esercitazione W19D4

Threat intelligence & IOC

Fabio Benevento - 15/03/2024

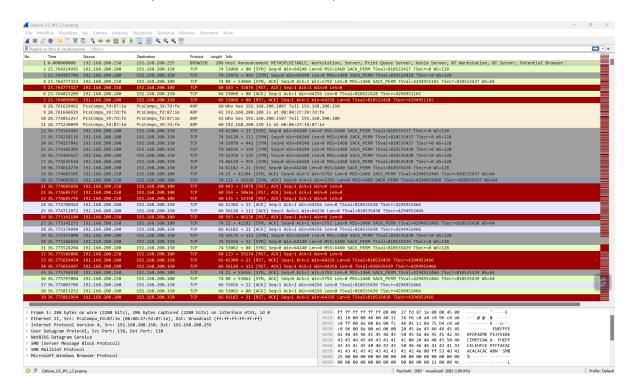
Traccia

Analizzate la cattura fornita 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

Implementazione

Analizzando la cattura con Wireshark è possibile individuare una serie di richieste TCP a distanza ravvicinata provenienti dalla macchina 192.168.200.100 verso la macchina 192.168.200.150 con porta di destinazione sempre diversa.



Ciò fa supporre che siamo in presenza di una scansione di tipo TCP da parte di un attaccante con strumenti tipo nmap volta ad individuare le porte aperte sulla macchina target.

In caso di porta aperta il target risponde con SYN+ACK (righe 35, 36 ad es.) mentre nel caso di porta chiusa la risposta è di tipo RST+ACK (righe 21, 22 e 23 ad es.).

Per ridurre gli impatti di un possibile attacco è consigliabile l'utilizzo di un firewall opportunamente configurato al fine di limitare l'accesso alla macchina solo a determinati IP sulla rete interna e/o a determinate porte.