Threat Intelligence & indicatori di compromissione (IoC)

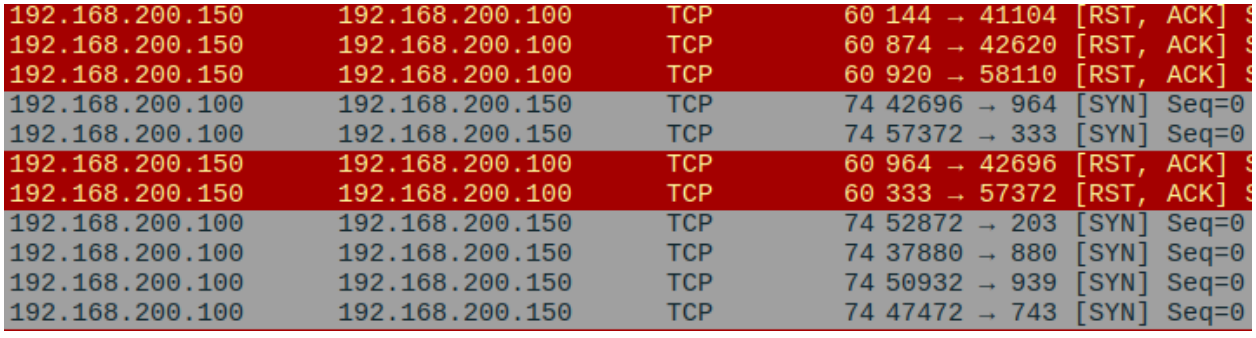
Richiesta:

● Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso
● In base agli IOC trovati, fare delle ipotesi sui potenziali vettori di attacco utilizzati
● Consigliare un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro

Strumenti: **Wireshark**

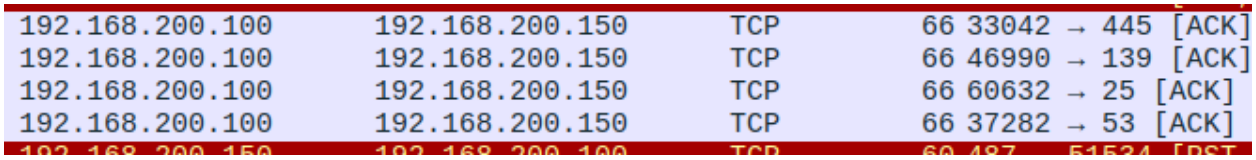
Analisi: Grazie a Wireshark, è stato possibile catturare, visualizzare e analizzare i pacchetti di dati che transitano sulla rete, in questo caso **192.168.200.0/24**.
I pacchetti rilevati provengono principalmente da 2 indirizzi IP: **192.168.200.100** e **192.168.200.150**, i quali sembrano essere appunto nella stessa rete.

Dall'analisi di Wireshark, si può notare come l'host **.100** invia tante richieste **SYN** a **192.168.200.150**, ricevendo come risposta **RST**



In questo caso, la richiesta SYN, inizierebbe l'handshake, mentre la richiesta RST significherebbe un rifiuto da parte dell'host destinatario.

Un dettaglio molto importante si può notare anche nelle richieste dello stesso host **192.168.200.100** sempre verso il target citato in precedenza, il quale ha ricevuto scansioni di tipo **ACK**, che potrebbero indicare una scansione in modalità Stealth con **Nmap**, soprattutto visto il contesto visto sopra.



Nmap è un tool che offre una scansione delle porte aperte e dei servizi attivi di un determinato host o di una rete, in questo caso dato che non esiste una connessione attiva tra i due, possiamo dedurre che si stia verificando un attacco da parte dello stesso **.100**.

Sono anche state rilevate porte aperte, in quanto il destinatario **192.168.200.150** ha risposto ad alcune scansioni con **SYN** e **ACK**, i quali completerebbero l'handshake iniziato e confermerebbero che la porta sia aperta.

Le porte aperte rilevate in questo caso sono state:

Port 445 utilizzata da Samba

Port 22 SSH

Port 21 relativa al Protocollo FTP

Port 80 che indica la presenza di un server HTTP

Port 111 per i servizi NFS

E altre porte come la **512**, **514** etc…

Interpretazione dell'analisi: L'host **192.168.200.100** ha eseguito una scansione delle porte verso il target **192.168.200.150** con l'utilizzo di Nmap, rilevando diverse porte aperte, con servizi che potrebbe essere vulnerabili se esposti senza sicurezza.
Questo potrebbe comportare dei rischi, quali:

1) Tentativi di exploit per quanto riguarda **Samba**
2) Brute-forcing verso **SSH & FTP**
3) Vulnerability scan su **HTTP**

Tecniche di mitigazione consigliate:

1) Verificare le configurazioni, gli accessi anonimi e le versioni dei servizi nelle porte sopra citate.
2) Chiudere eventuali porte con servizi non utilizzati.
3) Limitare gli accessi sui servizi come FTP, SMB e SSH.
4) Segmentare la rete e monitorare il traffico in modo da trovare eventuali accessi non autorizzati in corso.
5) Includere ulteriori misure di sicurezza come **IDS/IPS** o **WAF** a seconda della disponibilità economica per quanto riguarda il server web.