Threat Intelligence & IOC

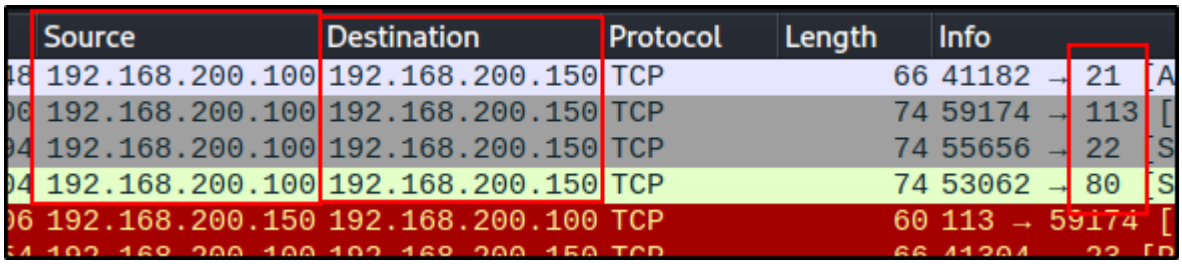
Traccia

Nell'esercizio di oggi ci viene fornita un'analisi di una cattura di rete effettuata con Wireshark. Si richiede di esaminare attentamente la cattura e rispondere alle seguenti domande:

- Identificare eventuali IOC presenti nella cattura, ovvero prove di attacchi in corso.
- Sulla base degli IOC individuati, formulare ipotesi sui potenziali vettori di attacco utilizzati nell'incidente.
- Raccomandare azioni volte a mitigare gli impatti dell'attacco.

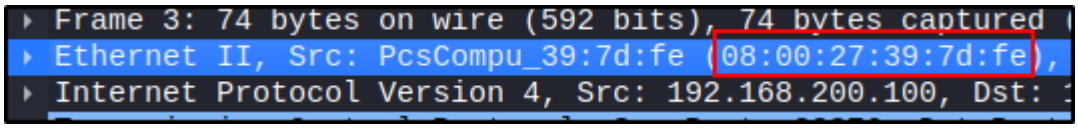
Analisi

Analizzando il traffico andiamo a notare molteplici richieste TCP proveniente dallo stesso host (192.168.200.100) verso un'altro host (192.168.200.150) distribuite su molteplici porte. Questo fà pensare ad una scansione del target con uno port scanner come Nmap



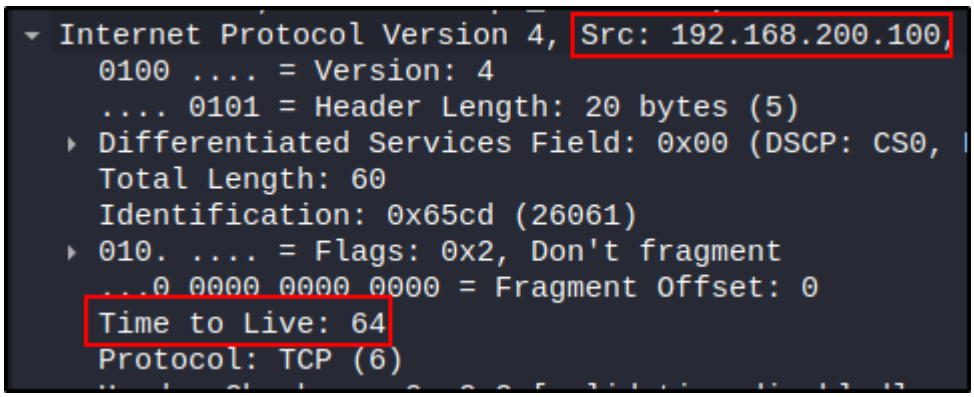
Source	Destination	Protocol	Length	Info
192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [A
192.168.200.100	192.168.200.150	TCP	74	59174 → 113 [
192.168.200.100	192.168.200.150	TCP	74	55656 → 22 [S
192.168.200.100	192.168.200.150	TCP	74	53062 → 80 [S
192.168.200.150	192.168.200.100	TCP	60	113 → 59174 [

Analizzando l'indirizzo MAC dell'attaccante notiamo che appartiene a una macchina virtuale



MAC Address	08:00:27:39:7D:FE
Vendor	PCS Systemtechnik GmbH
Address	600 Suffold St Lowell MA 01854 US
Block Size	MA-L
Block Range	08:00:27:00:00:00 - 08:00:27:FF:FF:FF
Virtual Machine	Oracle VirtualBox

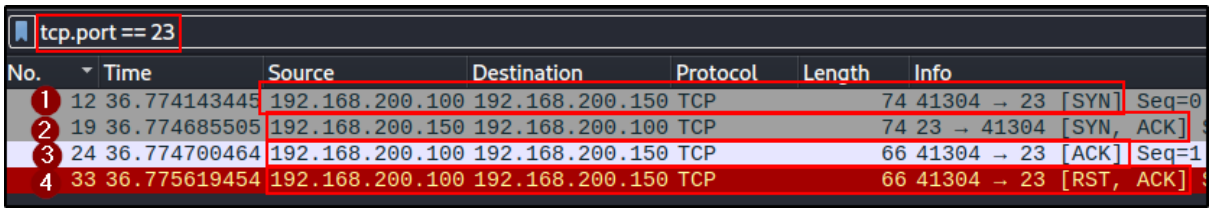
Dal TTL (Time To Live) dell'attaccante possiamo dedurre che sta usando un sistema operativo Linux poichè il suo TTL di default per pacchetti in uscita è 64 a differenza dei 128 di Windows



Prendiamo due porte come esempi che andremo ad analizzare più nel dettaglio

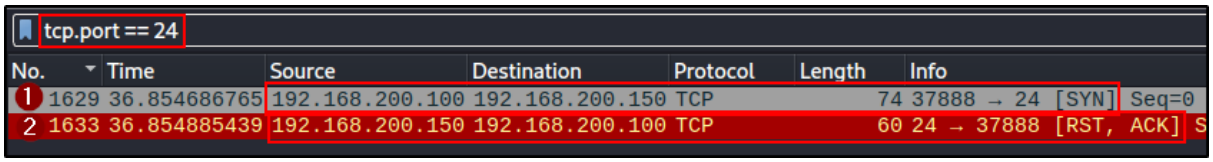
Nella porta 23 vengono scambiati i seguenti pacchetti:

1. Un pacchetto SYN da attaccante a vittima che serve ad iniziare il 3-Way Handshake necessario per iniziare a stabilire una connessione TCP
2. Un pacchetto SYN, ACK da vittima ad attaccante che funge da risposta al primo pacchetto SYN, confermando che la vittima lo ha ricevuto
3. Un pacchetto ACK da attaccante a vittima che conferma la ricezione del pacchetto SYN, ACK e procede a stabilire una connessione e relativo scambio dati fra hosts
4. Un pacchetto RST, ACK da attaccante a vittima che interrompe la connessione stabilita. Questo suggerisce un possibile comportamento da port scanner come Nmap volto a chiudere le connessioni una volta confermata l'apertura di una porta



Tramite questo scambio di pacchetti si evince che la porta 23 sul sistema vittima è aperta

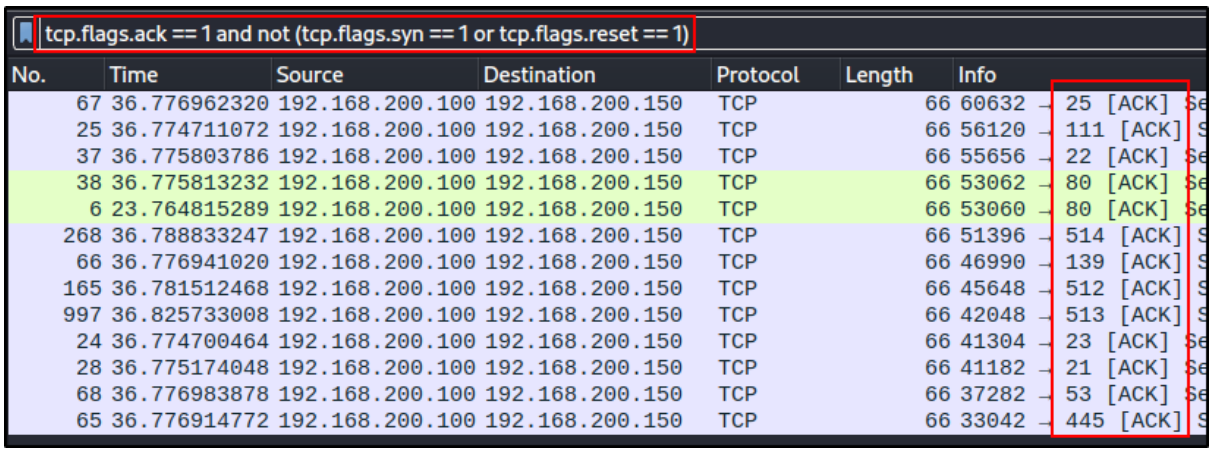
Nella porta 24 vengono scambiati i seguenti pacchetti:



1. Un pacchetto SYN da attaccante a vittima per iniziare il 3-Way Handshake
2. Un pacchetto RST, ACK da vittima ad attaccante che indica l'assenza di un servizio attivo sulla porta o un firewall che blocca il tentativo di connessione

Tramite questo scambio di pacchetti si evince che la porta 24 sul sistema vittima è chiusa

Filtrando i pacchetti ACK possiamo dedurre quali sono le porte aperte nella macchina vittima e di conseguenza i servizi comunemente associati ad esse



- 22 (SSH): Secure Shell
- 23 (Telnet): Telnet
- 25 (SMTP): Simple Mail Transfer Protocol
- 53 (DNS): Domain Name System
- 80 (HTTP): Hypertext Transfer Protocol
- 111 (RPC): Remote Procedure Call
- 139 (NetBIOS): NetBIOS Session Service
- 445 (SMB): Server Message Block
- 512 (exec): Remote Process Execution
- 513 (login): Remote Login
- 514 (syslog): Syslog

Rimedi

Per mitigare questo tipo di attacco possiamo procedere nei seguenti modi:

Inserendo una regola nel firewall che blocca tutte le richieste provenienti dall'IP dell'attaccante

Implementando un IPS/IDS che identifica e/o blocca attività sospette di scansione della rete

Limitando la frequenza di traffico tramite firewall per rallentare possibili tentativi di scansione della rete