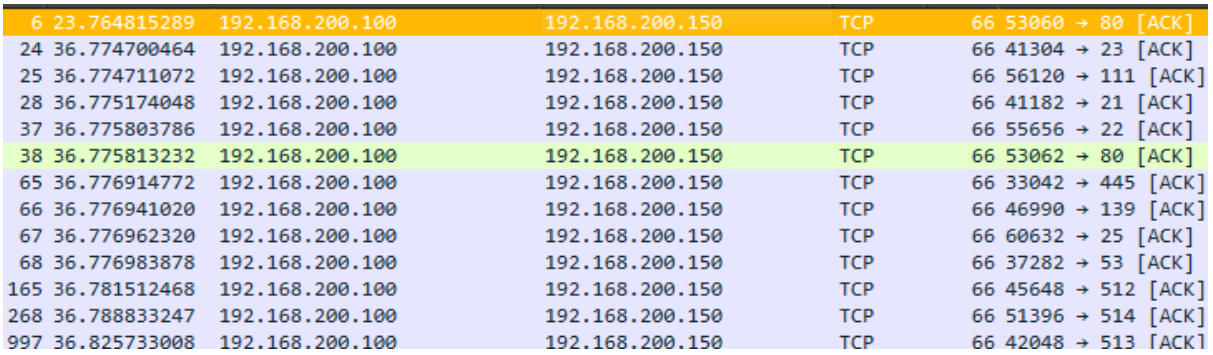
S9 L5 Esercizio Threat Intelligence & IOC

Analizzare il traffico di rete effettuato con Wireshark e:

- Identificare ed analizzare eventuali IoC
- In base agli IoC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Azioni per ridurre gli impatti dell'attacco ed eventualmente un simile attacco futuro

Analizzando il traffico dalla cattura di Wireshark individuiamo un indirizzo IP **192.168.200.100** che svolge delle attività sospette (IoC) che cerca di avviare un processo di handshake inviando un pacchetto SYN per iniziare una connessione sulle porte della Metasploitable 192.168.200.150

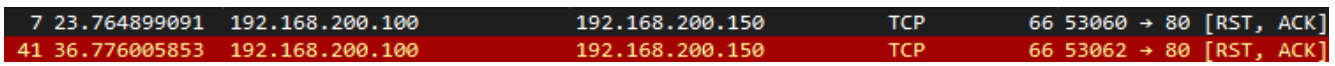
La maggior parte delle connessioni delle porte viene subito rifiutata dall' indirizzo 192.168.200.150 restituendo il flag RST-ACK, invece altre vengono accettate SYN-ACK. Così facendo handshake va avanti e viene concluso dalla risposta ACK dall' indirizzo 192.168.200.100
Inserendo questo filtro su Wireshark vediamo su quali porte: **tcp.flags == 0x10**



6	23.764815289	192.168.200.100	192.168.200.150	TCP	66 53060 → 80 [ACK]
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66 41304 → 23 [ACK]
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66 56120 → 111 [ACK]
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66 41182 → 21 [ACK]
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66 55656 → 22 [ACK]
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66 53062 → 80 [ACK]
65	36.776914772	192.168.200.100	192.168.200.150	TCP	66 33042 → 445 [ACK]
66	36.776941020	192.168.200.100	192.168.200.150	TCP	66 46990 → 139 [ACK]
67	36.776962320	192.168.200.100	192.168.200.150	TCP	66 60632 → 25 [ACK]
68	36.776983878	192.168.200.100	192.168.200.150	TCP	66 37282 → 53 [ACK]
165	36.781512468	192.168.200.100	192.168.200.150	TCP	66 45648 → 512 [ACK]
268	36.788833247	192.168.200.100	192.168.200.150	TCP	66 51396 → 514 [ACK]
997	36.825733008	192.168.200.100	192.168.200.150	TCP	66 42048 → 513 [ACK]

Abbiamo quindi le connessioni stabilite sulle porte: 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514

Analizzando il traffico notiamo anche che le connessioni vengono tutte interrotte (**RST-ACK**) proprio dall' indirizzo IP attaccante 192.168.200.100
Inserendo questo filtro su Wireshark possiamo verificare che siano interrotte:
tcp.flags.reset == 1 && tcp.flags.ack == 1 && tcp.dstport == <NR PORTA>



7	23.764899091	192.168.200.100	192.168.200.150	TCP	66 53060 → 80 [RST, ACK]
41	36.776005853	192.168.200.100	192.168.200.150	TCP	66 53062 → 80 [RST, ACK]

Essendo queste connessioni create per poi essere interrotte un possibile motivo potrebbe essere che in questo caso l' attaccante stia effettuando una **enumerazione delle porte** e dei servizi attivi.

Identificazione degli IoC:

- Traffico anomalo e elevato
- Ripetute attività di connessione e connessioni interrotte
- Richieste ARP

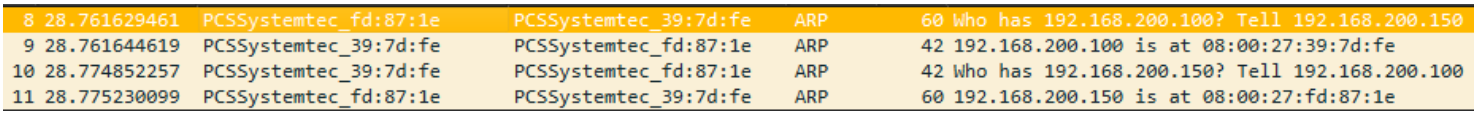
Ipotesi sui potenziali vettori di attacco:

- **Attacco SYN Flood:**
  L'attacco SYN Flood sfrutta una vulnerabilità nel processo di handshake del protocollo TCP/IP. Il client (192.168.200.100) invia ripetutamente richieste di connessione TCP con il flag SYN al server (192.168.200.150), ma non completa mai l'handshake inviando il pacchetto ACK. Di conseguenza, le richieste parziali si accumulano nelle tabelle di connessione del server, esaurendo le sue risorse. Questo causa un attacco Denial of Service (DoS), impedendo al server di gestire le connessioni legittime e saturando memoria e capacità di elaborazione.

- **Port Scanning:**
  Durante una scansione delle porte, l'attaccante invia pacchetti SYN per verificare la disponibilità delle porte del server. Se una porta è chiusa, il server risponde con un pacchetto TCP con flag RST, segnalando il rifiuto della connessione. Analizzando le risposte RST, l'attaccante può identificare quali porte sono aperte o chiuse, effettuando così una mappatura dei servizi attivi sulla macchina target per scoprire eventuali vulnerabilità.

  Utilizzando Nmap, la scansione con lo switch **-sT** si comporta in modo simile. Questo metodo utilizza la chiamata di sistema **connect()** per tentare di stabilire connessioni complete con ciascuna porta. Sebbene sia il metodo più semplice per eseguire una scansione TCP, è anche il più affidabile, poiché si basa sullo stack di rete del sistema operativo host che esegue Nmap.

- **ARP Requests sospette**: Un altra attività sospetta è lo scambio bidirezionale del protocollo ARP. Essendo il protocollo ARP utilizzato per associare un indirizzo IP con un indirizzo MAC, l' attaccante può sfruttare questa informazione per poter avviare un attacco Man-in-the-Middle.



8	28.761629461	PCSSystemtec_fd:87:1e	PCSSystemtec_39:7d:fe	ARP	60 Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d:fe	PCSSystemtec_fd:87:1e	ARP	42 192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PCSSystemtec_39:7d:fe	PCSSystemtec_fd:87:1e	ARP	42 Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PCSSystemtec_fd:87:1e	PCSSystemtec_39:7d:fe	ARP	60 192.168.200.150 is at 08:00:27:fd:87:1e

- **Possibile Malware**: Un'altra possibile causa del traffico sospetto potrebbe essere la presenza di un malware su uno dei dispositivi della rete locale.

Questo malware potrebbe generare attività dannose o anomalie, come connessioni non autorizzate o scansioni delle porte, sfruttando gli indirizzi IP della rete interna. Questo genera un elevato traffico di rete e potrebbe provocare un attacco Denial of Service (DoS) per saturare le risorse del sistema target.

Vulnerabilità e mitigazione sulle porte accessibili

21 (FTP - File Transfer Protocol): Protocollo per il trasferimento di file tra client e server.

- Trasferimento dati in chiaro, incluse credenziali.
- Vulnerabile ad attacchi di brute force.

Mitigazioni:

- Usare FTPS (FTP Secure) o SFTP per crittografare i dati.
- Configurare un firewall per limitare l'accesso solo agli IP autorizzati.
- Disabilitare gli account anonimi.
- Implementare regole di password forti e limiti di login per prevenire brute force.
- Aggiornare regolarmente il server FTP.

22 (SSH - Secure Shell): Accesso remoto sicuro a sistemi.

- Attacchi di brute force per accesso non autorizzato.
- Possibili exploit su versioni vulnerabili di OpenSSH.

Mitigazioni:

- Usare chiavi SSH con passphrase al posto delle password.
- Configurare un meccanismo di autenticazione a due fattori (2FA).
- Cambiare la porta predefinita per SSH (non è una soluzione definitiva ma riduce gli attacchi automatizzati).
- Limitare gli utenti che possono accedere via SSH.
- Abilitare solo versioni sicure di SSH e disabilita protocolli deprecati.

23 (Telnet): Protocollo per accesso remoto non sicuro.

- Tutte le comunicazioni sono in chiaro, inclusi username e password.
- Altamente vulnerabile a intercettazioni e attacchi MITM.

Mitigazioni:

- Disabilitare Telnet e usare SSH come alternativa sicura.
- Rimuovere le credenziali predefinite e verifica che Telnet non sia esposto a Internet.
- Bloccare la porta 23 a livello di firewall.

25 (SMTP - Simple Mail Transfer Protocol): Protocollo per invio di email.

- Open relay: può essere sfruttato per inviare spam.
- Attacchi di spoofing e relay abuse.

Mitigazioni:

- Configurare il server SMTP per rifiutare l'uso come relay aperto.
- Usare TLS per proteggere le comunicazioni (STARTTLS).
- Abilitare l'autenticazione per inviare email.
- Implementare filtri anti-spam e controlli contro attacchi di spoofing
- Monitorare il traffico SMTP per identificare attività sospette.

53 (DNS - Domain Name System): Risoluzione di nomi di dominio in indirizzi IP.

- DNS poisoning e spoofing.
- Ampliamento di attacchi DDoS tramite reflection.

Mitigazioni:

- Usare DNSSEC per proteggere l'integrità delle risposte DNS.
- Configurare il server DNS per limitare l'accesso solo ai client autorizzati.
- Proteggere il server da attacchi DDoS con strumenti di rate limiting.
- Usare un resolver DNS privato e aggiornato.
- Configurare il firewall per bloccare query non autorizzate.

80 (HTTP - HyperText Transfer Protocol): Protocollo per la trasmissione di pagine web.

- Comunicazione in chiaro (priva di crittografia).
- Vulnerabile a XSS, SQL injection e attacchi MITM.

Mitigazioni:

- Usare HTTPS (con certificati TLS/SSL) al posto di HTTP.
- Applicare regole di sicurezza per le applicazioni web (es. WAF - Web Application Firewall).
- Monitorare e correggere vulnerabilità nell'applicazione web (es. tramite penetration testing).
- Configurare correttamente il server web (es. header di sicurezza come HSTS, X-Content-Type-Options).
- Mantenere aggiornato il server web.

111 (RPCBind - Remote Procedure Call Bind): Associa servizi RPC alle porte.

- Esposizione di servizi RPC vulnerabili.
- Utilizzabile per enumerare servizi sulla macchina.

Mitigazioni:

- Disabilitare RPC se non necessario.
- Configurare un firewall per limitare l'accesso agli IP di fiducia.
- Aggiornare i servizi che utilizzano RPC per evitare exploit noti.
- Usare strumenti per monitorare e loggare l'accesso ai servizi RPC.

139 (NetBIOS Session Service): Condivisione file e stampanti su reti Microsoft

- Enumerazione di utenti e risorse.
- Possibile punto di ingresso per attacchi SMB.

445 (Microsoft-DS - SMB): Condivisione file e stampanti (Direct SMB).

- Vulnerabile a exploit come EternalBlue.
- Potenziale per attacchi di forza bruta su credenziali.

Mitigazioni:

- Disabilitare SMBv1 e usa versioni più recenti (SMBv2 o SMBv3).
- Configurare il firewall per bloccare l'accesso alla porta da IP non autorizzati.
- Usare un sistema di autenticazione forte (es. NTLMv2 o Kerberos).
- Disabilitare la condivisione di risorse non necessarie.
- Monitorare il traffico SMB per identificare attività sospette.

512/513/514 (Remote Execution - r services): Comandi remoti su Unix (rexec, rlogin, rsh).

- Comunicazioni non sicure (in chiaro).
- Basati su fiducia di rete, facilmente sfruttabili se mal configurati.

Mitigazioni:

- Disabilitare rexec, rlogin e rsh, sono obsoleti e insicuri.
- Usare SSH come alternativa sicura.
- Configurare il firewall per bloccare queste porte.

Azioni per mitigare l'attacco in corso:

- Configurare un filtro per i pacchetti SYN in ingresso, limitando il numero di connessioni simultanee che ogni singolo IP può avviare.
- Isolare i dispositivi potenzialmente compromessi da malware per evitare la sua diffusione nella rete.
- Essendo l' indirizzo IP parte della rete locale, verificare i log degli utenti che hanno accesso a tale dispositivo per spergiurare un attacco interno.

Azioni per prevenire futuri attacchi simili:

- Eseguire regolarmente scansioni delle porte e analisi delle vulnerabilità per individuare e correggere eventuali punti deboli della rete prima che possano essere sfruttati.
- Effettuare un monitoraggio continuo della rete per identificare e bloccare tempestivamente connessioni sospette.
- Mantenere i sistemi aggiornati con le patch di sicurezza più recenti.
- Sensibilizzare e formare il personale per riconoscere segnali e tentativi di attacco, riducendo il rischio umano.
- Implementare soluzioni di sicurezza come firewall, sistemi IDS (Intrusion Detection System) per rilevare potenziali minacce, e IPS (Intrusion Prevention System) per bloccare attivamente le intrusioni. L'adozione di una piattaforma SIEM (Security Information and Event Management) potrebbe migliorare ulteriormente il rilevamento e la risposta agli attacchi.