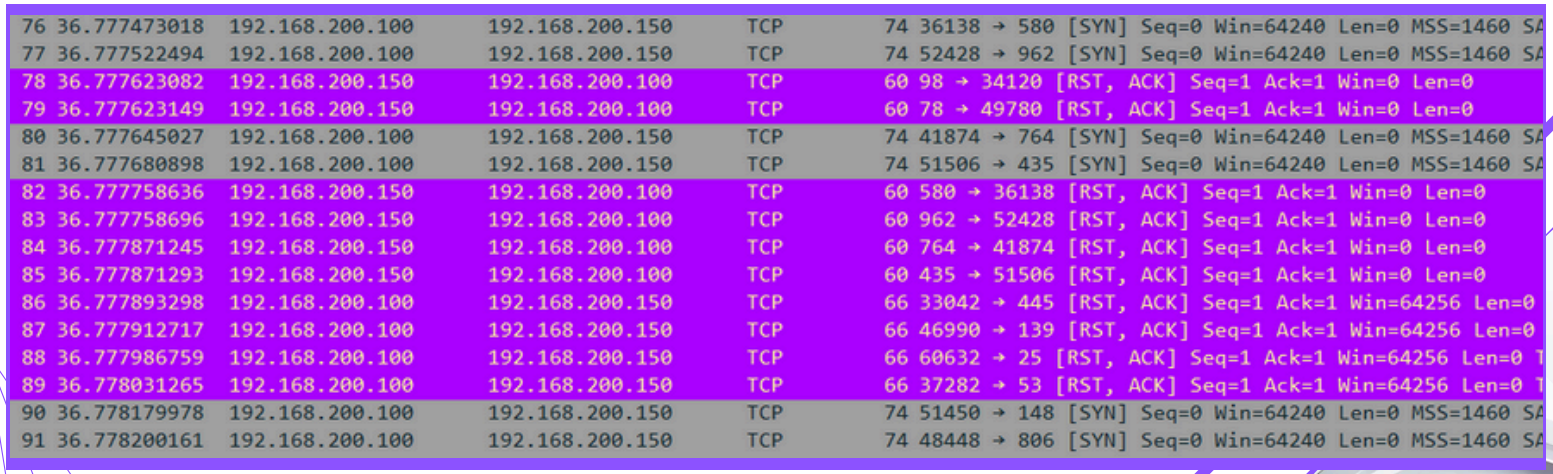
L3

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

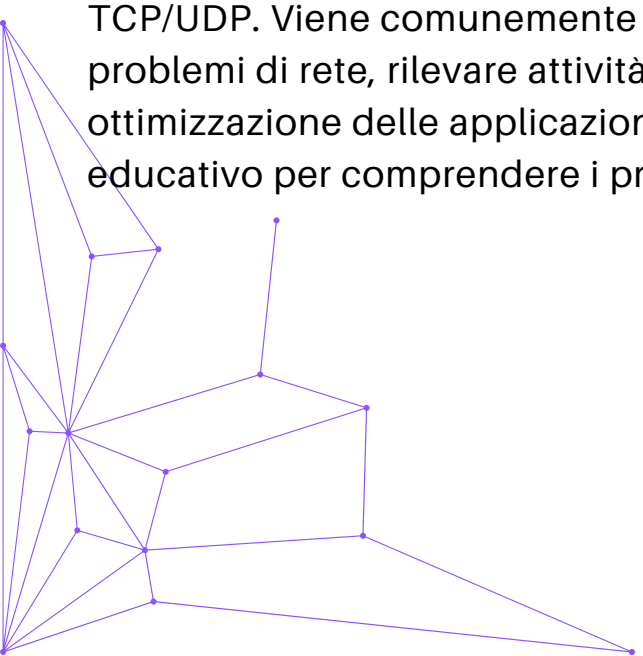


76	36.777473018	192.168.200.100	192.168.200.150	TCP	74 36138 → 580 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
77	36.777522494	192.168.200.100	192.168.200.150	TCP	74 52428 → 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
78	36.777623082	192.168.200.150	192.168.200.100	TCP	60 98 → 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79	36.777623149	192.168.200.150	192.168.200.100	TCP	60 78 → 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80	36.777645027	192.168.200.100	192.168.200.150	TCP	74 41874 → 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
81	36.777680898	192.168.200.100	192.168.200.150	TCP	74 51506 → 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
82	36.777758636	192.168.200.150	192.168.200.100	TCP	60 580 → 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83	36.777758696	192.168.200.150	192.168.200.100	TCP	60 962 → 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84	36.777871245	192.168.200.150	192.168.200.100	TCP	60 764 → 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85	36.777871293	192.168.200.150	192.168.200.100	TCP	60 435 → 51506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86	36.777893298	192.168.200.100	192.168.200.150	TCP	66 33042 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
87	36.777912717	192.168.200.100	192.168.200.150	TCP	66 46990 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
88	36.777986759	192.168.200.100	192.168.200.150	TCP	66 60632 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 T
89	36.778031265	192.168.200.100	192.168.200.150	TCP	66 37282 → 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 T
90	36.778179978	192.168.200.100	192.168.200.150	TCP	74 51450 → 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
91	36.778200161	192.168.200.100	192.168.200.150	TCP	74 48448 → 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA

IOC & Wireshark

Gli **IOC** (**Indicator Of Compromise**) sono degli indicatori, ovvero dei segnali che indicano la possibilità che un sistema informatico o una rete siano stati compromessi da attività malevole. Tali segnali vengono utilizzati per ricostruire uno storico e capire cosa è sucesso. Gli esperti di sicurezza informatica utilizzano gli ioc per individuare, riconoscere ed eliminare le minacce, tra cui malware, attacchi informatici, fughe di dati e altri tipi di compromissione della sicurezza.
La maggior parte degli incidenti di sicurezza vengono identificati grazie all'analisi del traffico di rete che mostra flussi inaspettati o comunque sospetti. Tra le tecniche di recupero flussi di rete ci sono infine i «network monitoring tools», ovvero i software utilizzati per lo sniffing delle comunicazioni su una rete come ad esempio Wireshark.

Wireshark è uno strumento di analisi del traffico di rete che cattura e visualizza i pacchetti in tempo reale ed è utilizzato da amministratori di rete, esperti di sicurezza, sviluppatori di software e studenti per diagnosticare problemi di rete, analizzare protocolli, rilevare vulnerabilità di sicurezza e comprendere il comportamento delle applicazioni di rete. Wireshark intercetta il traffico da diverse interfacce di rete, esamina dettagli dei pacchetti dai livelli più bassi ai più alti, offre filtri potenti per focalizzarsi su pacchetti specifici, supporta Windows, macOS e Linux, decodifica centinaia di protocolli e include un'interfaccia grafica intuitiva oltre a strumenti avanzati per l'analisi di flussi TCP, VoIP e conversazioni TCP/UDP. Viene comunemente utilizzato per identificare e risolvere problemi di rete, rilevare attività sospette, fare debugging e ottimizzazione delle applicazioni di rete e come strumento educativo per comprendere i protocolli e il traffico di rete.



Analisi con Wireshark

Si nota la presenza di una richiesta ARP: andando a leggere le info l'indirizzo IP 192.168.200.150 chiede chi sia 192.168.200.100, e dato che l'arp funziona al 2 livello iso/osi controlla nella mac table e come output darà l'indirizzo mac. Oltre questo possiamo già capire che l'attaccante è interno alla nostra rete.

```
emtec_39:7d:… ARP          60 Who has 192.168.200.100? Tell 192.168.200.150
emtec_fd:87:… ARP          42 192.168.200.100 is at 08:00:27:39:7d:fe
emtec_fd:87:… ARP          42 Who has 192.168.200.150? Tell 192.168.200.100
emtec_39:7d:… ARP          60 192.168.200.150 is at 08:00:27:fd:87:1e
```

La prima cosa che salta all'occhio è la presenza di due soli indirizzi IP. Inoltre l'analisi della moltitudine di richiesta TCP da parte dello stesso indirizzo IP fa pensare che non si tratti di un classico tentativo di connessione.

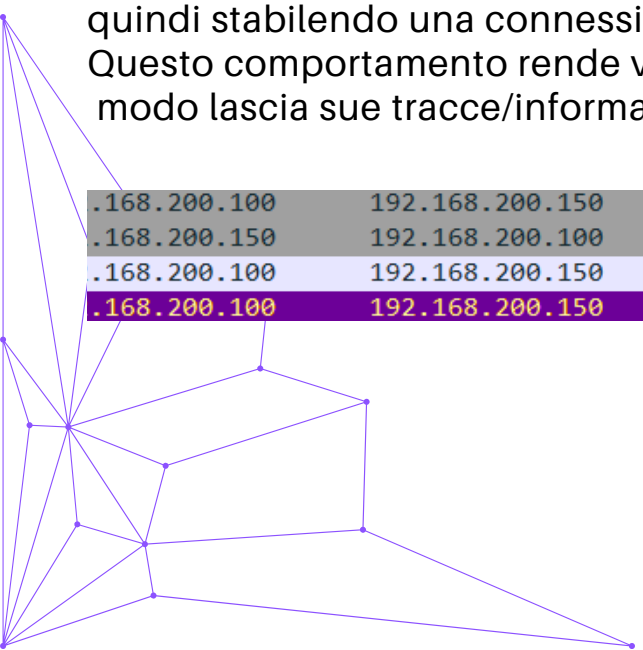
```
192.168.200.100    192.168.200.150    TCP        74 41304 → 23 [SYN]
192.168.200.100    192.168.200.150    TCP        74 56120 → 111 [SYN]
192.168.200.100    192.168.200.150    TCP        74 33878 → 443 [SYN]
192.168.200.100    192.168.200.150    TCP        74 58636 → 554 [SYN]
```

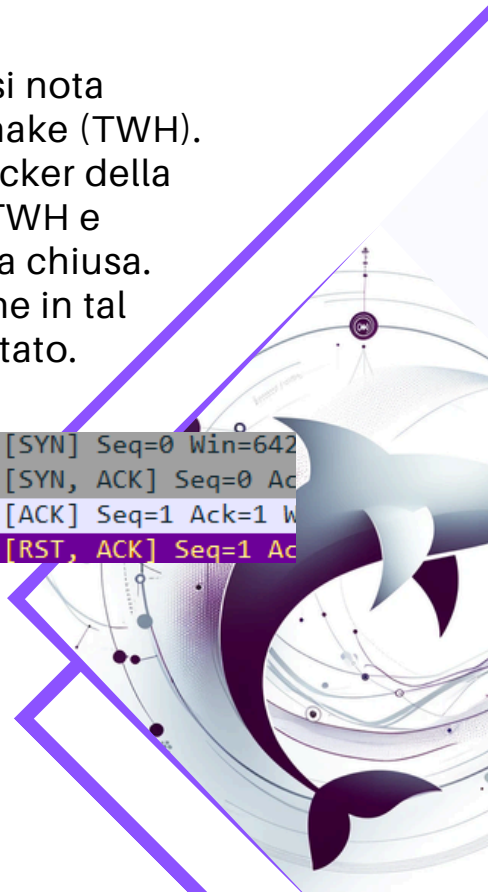
Le richieste TCP fanno una richiesta SYN: se la porta è aperta ci restituirà un SYN, ACK; se la porta sarà chiusa restituirà RST, ACK:

```
36.774685505  192.168.200.150  192.168.200.100  TCP   74 23 → 41304 [SYN, ACK] Seq
36.774685652  192.168.200.150  192.168.200.100  TCP   74 111 → 56120 [SYN, ACK] Se
36.774685696  192.168.200.150  192.168.200.100  TCP   60 443 → 33878 [RST, ACK] Se
36.774685737  192.168.200.150  192.168.200.100  TCP   60 554 → 58636 [RST, ACK] Se
36.774685776  192.168.200.150  192.168.200.100  TCP   60 135 → 52358 [RST, ACK] Se
```

Analizzando una singola porta tramite filtro di Wireshark si nota come l'attaccante abbia effettuerato il Three Way Handshake (TWH). Si può capire da tale attacco come l'attaccante sia un "hacker della domenica" siccome l'attacco viene fatto concludendo il TWH e quindi stabilendo una connessione, nonostante poi venga chiusa. Questo comportamento rende vulnerabile l'attaccante, che in tal modo lascia sue tracce/informazioni utili per essere arrestato.

```
.168.200.100    192.168.200.150    TCP    74 56120 → 111 [SYN] Seq=0 Win=642
.168.200.150    192.168.200.100    TCP    74 111 → 56120 [SYN, ACK] Seq=0 Ac
.168.200.100    192.168.200.150    TCP    66 56120 → 111 [ACK] Seq=1 Ack=1 W
.168.200.100    192.168.200.150    TCP    66 56120 → 111 [RST, ACK] Seq=1 Ac
```



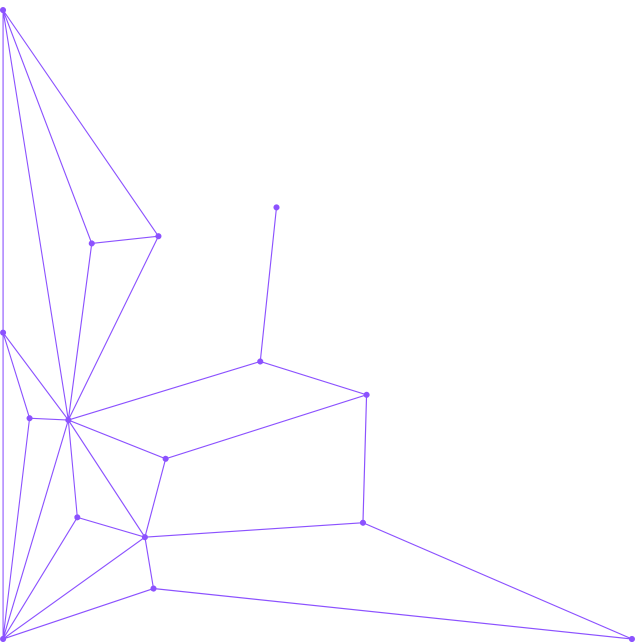


Identificazione IOC

Dalla cattura di rete fornita, si possono osservare diverse caratteristiche che indicano potenziali attività malevole. Analizziamo i dettagli per identificare gli Indicatori di Compromissione (IOC), ipotizzare i vettori di attacco e consigliare azioni per mitigare gli impatti.
Identificazione degli **IOC**

1. **Connessioni TCP RST e SYN anomale:**
   - Numerosi pacchetti **TCP** con flag **RST** (reset) e **SYN** (synchronize), che potrebbero indicare un tentativo di interrompere connessioni legittime o di creare nuove connessioni malevole.
   - Ripetute connessioni con porta sorgente e destinazione diverse ma spesso sulle stesse IP, suggerendo un pattern anomalo di comunicazione.

2. **Pattern di comunicazione:**
   - La comunicazione tra gli indirizzi IP **192.168.200.100** e **192.168.200.150** risulta sospetta, con una sequenza di pacchetti **RST**, **SYN**, **ACK** che non segue il normale comportamento di una connessione **TCP**.



Potenziali vettori d’attacco

Ipotesi sui Potenziali Vettori di Attacco

La presenza di molteplici richieste TCP indicano che l'attaccante potrebbe utilizzare strumenti di scansione delle porte, come Nmap o simili, per mappare la superficie di attacco del target. Questo tipo di scansione è spesso il preludio a tentativi di exploit su servizi vulnerabili identificati durante la fase di ricognizione. A questo proposito vengono proposti dei potenziali vettori d’attacco:

- **Attacco SYN Flood:**

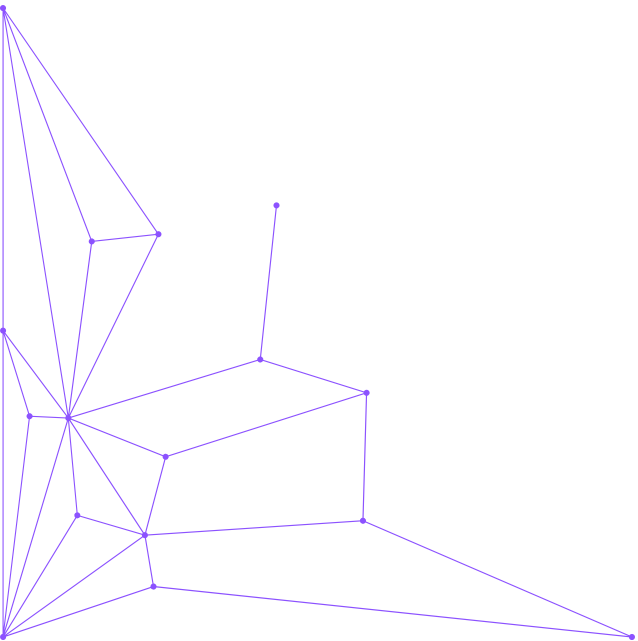
Il continuo invio di pacchetti SYN senza completare il handshake TCP può essere un indicatore di un attacco SYN flood, utilizzato per esaurire le risorse del server e impedirgli di gestire nuove connessioni legittime.

- **Scansione di Porte:**

L'alto numero di pacchetti con flag SYN e la varietà di porte coinvolte possono suggerire un'attività di scansione delle porte, in cui un attaccante cerca di identificare porte aperte e vulnerabili.

- **Attacco DDoS:**

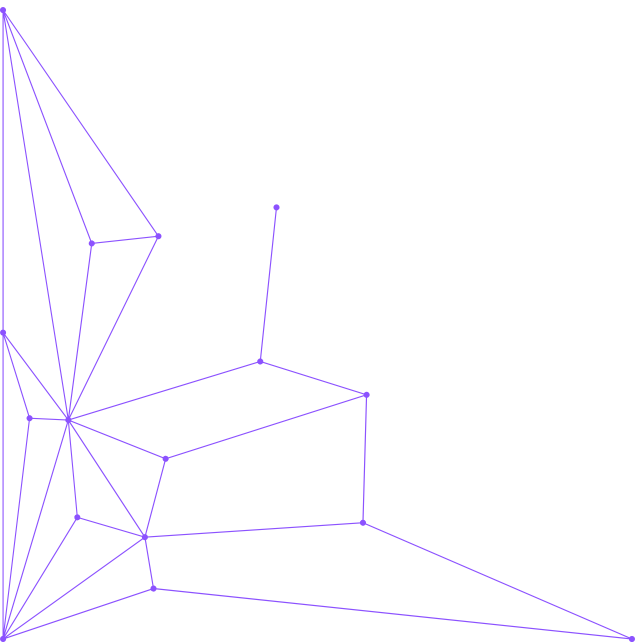
La presenza di numerosi pacchetti RST può indicare un tentativo di sovraccaricare il sistema con richieste eccessive, interrompendo le connessioni legittime.



Prevenzione

Azioni Consigliate per Ridurre gli Impatti dell'Attacco

- Implementare Filtraggio degli Indirizzi IP:
  - Configurare il firewall per bloccare gli indirizzi IP sospetti (192.168.200.100 e 192.168.200.150) se non appartengono a dispositivi autorizzati.
- Abilitare Sistemi di Rilevamento delle Intrusioni (IDS):
  - Utilizzare IDS per monitorare e rilevare pattern anomali di traffico e bloccare automaticamente le connessioni sospette.
- Limitare le Connessioni Incomplete:
  - Configurare il server per limitare il numero di connessioni incomplete (handshake TCP non completati), riducendo l'impatto degli attacchi SYN flood.
- Monitoraggio Costante del Traffico di Rete:
  - Implementare un sistema di monitoraggio del traffico di rete per identificare rapidamente qualsiasi attività sospetta e rispondere tempestivamente.
- Aggiornamento delle Politiche di Sicurezza:
  - Rivedere e aggiornare le politiche di sicurezza per includere misure specifiche contro i tipi di attacco identificati, come DDoS e scansioni di porte.



CONCLUSIONI

Durante il monitoraggio della rete, sono state identificate evidenze di Indicatori di Compromissione (IOC), in particolare richieste TCP ripetute. Questo comportamento anomalo suggerisce la possibilità di un attacco in corso.
Un'analisi più dettagliata dei log di rete ha rivelato che l'indirizzo IP 192.168.200.100 sta effettuando una scansione sul target 192.168.200.150. Tale attività è tipica di una fase di ricognizione, in cui l'attaccante cerca di individuare porte e servizi aperti per sfruttare eventuali vulnerabilità.
L'evidenza delle richieste TCP ripetute indica che l'attaccante potrebbe utilizzare strumenti di scansione delle porte, come Nmap o simili, per mappare la superficie di attacco del target. Questo tipo di scansione è spesso il preludio a tentativi di exploit su servizi vulnerabili identificati durante la fase di ricognizione.
Per ridurre l'impatto dell'attacco e prevenire ulteriori tentativi di compromissione, si consiglia di implementare immediatamente delle policy di firewall che blocchino tutte le richieste provenienti dall'IP dell'attaccante (192.168.200.100). Questo intervento impedirebbe all'attaccante di continuare la scansione e di ottenere ulteriori informazioni sulle porte e sui servizi in ascolto sul target 192.168.200.150.
In sintesi, l'adozione di misure di blocco a livello di firewall rappresenta un'azione tempestiva ed efficace per contrastare le attività malevole in corso, proteggendo così l'integrità e la sicurezza della rete.