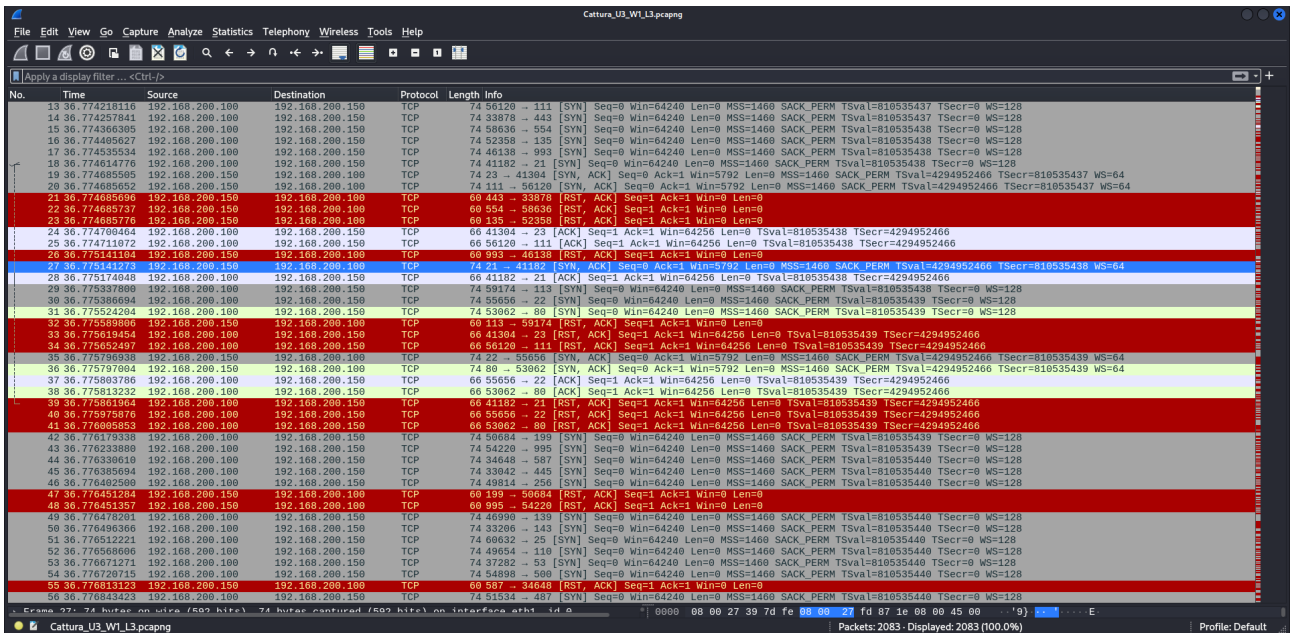
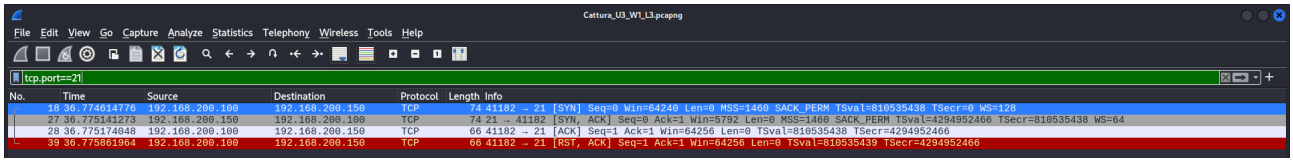


Analizzando i dati forniti dalla cattura effettuata tramite Wireshark, possiamo notare come l'IP 192.168.200.100 stia tentando di effettuare delle connessioni TCP verso diverse porte dell'IP 192.168.200.150, il quale si trova nella stessa rete.
Analizzando gli IOC (Indicator of Compromise), possiamo notare come L'IP sorgente interrompa la connessione una volta che il server gli ha dato la disponibilità alla connessione, non permettendo di effettuare così una connessione TCP completa.
Questo suggerirebbe, ad esempio, un attacco di scansione delle porte utilizzando il SYN Scan (Half-Open Scan) di Nmap.
Questa tecnica invia un pacchetto SYN per iniziare una connessione, ma non completa il "three-way handshake". Questo può essere fatto con Nmap usando l'opzione -sS.
Non completando la connessione, l'attaccante riduce la probabilità di essere rilevato dai sistemi di sicurezza e dai log del server. Questo approccio permette di ottenere informazioni sulle porte aperte senza compromettere la propria anonimità. Non completare la connessione significa che l'attaccante può scansionare molte porte in un breve lasso di tempo. La scansione di porte SYN richiede meno risorse rispetto all'apertura di connessioni TCP complete. La mancata completa connessione lascia meno tracce nei log di rete, rendendo più difficile per gli amministratori di rete identificare la scansione come un'attività sospetta



Prendendo come esempio un tentativo di connessione alla porta 21 (nello screenshot qui sopra), possiamo notare come L'IP sorgente invii una richiesta di connessione (SYN), ricevendo una risposta dall'IP destinatario (SYN, ACK). A quel punto, l'IP sorgente sembra voler continuare il tentativo di connessione (ACK), ma subito dopo interrompe la connessione (RST, ACK), evitando così di effettuare una connessione completa. Per giungere alla conclusione che un servizio su una porta sia attivo, gli basta che il server gli risponda in modo positivo al tentativo di connessione.

Azioni Immediate per Ridurre l'Impatto dell'Attacco Attuale

1. **Monitoraggio del Traffico di Rete:**

   Utilizzo di strumenti di monitoraggio della rete per identificare il traffico sospetto. Analisi dei log dei firewall e dei router per rilevare un aumento anomalo delle richieste SYN.

2. **Bloccare l'Indirizzo IP Attaccante**:

   Per evitare ulteriori attacchi da un determinato IP, se questo è identificabile, lo si può bloccare tramite regole di firewall.

3. **Aumentare le Regole di Timeout**:

   Aumentare il timeout dei pacchetti SYN, così da limitare la possibilità di stabilire una connessione in caso di scansione rapida.

4. **Aggiornare e Configurare i Firewall**:

   Configurare i firewall correttamente per gestire le richieste SYN. Alcuni firewall possono bloccare automaticamente le scansioni delle porte o implementare il rate limiting per ridurre la velocità delle richieste.

Azioni a Lungo Termine per Prevenire Attacchi Futuri

1. **Segmentazione della Rete**:

   Implementare una segmentazione della rete per limitare l'accesso a determinate risorse. Ciò può rendere più difficile per un attaccante effettuare una scansione efficace dell'intera rete.

2. **Implementare IDS/IPS**:

   Utilizzare sistemi IDS/IPS per monitorare e rispondere a comportamenti sospetti in tempo reale. Questi sistemi possono rilevare modelli di scansione e rispondere automaticamente.

3. **Educazione e Formazione del Personale:**

   Formare il personale IT e i team di sicurezza riguardo le tecniche di scansione delle porte e le best practice di sicurezza.

4. **Regole di Rate Limiting**:

   Implementare politiche di rate limiting sui firewall per limitare il numero di richieste SYN che un singolo IP può inviare in un determinato intervallo di tempo.