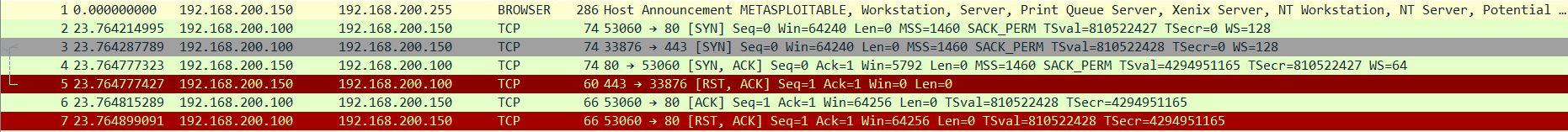
IOC (indicatore di compromissione)

**IOC (indicatore di compromissione)**

Sono utilizzati come segnali o indicatori che possono essere monitorati per rilevare e rispondere a potenziali minacce alla sicurezza. Monitorati tali dati si può ricostruire uno storico e capire la natura dell’attacco e cosa è successo.



1. Identificare eventuali IOC, ovvero evidenze di attacchi in corso

**Come vediamo nell’immagine sopra riportata Wireshark (riga 5 e 7)**

**Sniffa un ack di risposta particolare il REST ACK. Questo fa terminare**

**in modo improprio le connessioni TCP. Inoltre si notano che gli IP fanno parte**

**della stessa rete, questo vuol dire che il black hat è collegato alla network dell’azienda**

1. In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati

**L’ipotesi è che si tratti di un TCP Reset attack:**

**Un attacco TCP Reset Attack è una forma di attacco informatico in cui un aggressore invia pacchetti TCP RST (Reset) per interrompere in modo improprio una connessione TCP. Questi pacchetti RST vengono inviati con l'intento di terminare la connessione o interrompere la comunicazione in corso.**

**Questo può portare a interruzioni nella comunicazione e compromettere l'integrità della connessione. Tale attacco può essere utilizzato per interrompere servizi, creare confusione nella rete o compromettere la disponibilità dei servizi online.**

**Questo tipo di attacco può essere usato per scopi diversi:**

**DOS (Denial Of Service)**

**MIMT (Man In The Middle)**

1. Consigliate un’azione per ridurre gli impatti dell’attacco

**Per proteggersi da attacchi di reset TCP, è importante implementare misure di sicurezza, come l'uso di firewalls, la crittografia delle comunicazioni e la verifica dell'integrità dei pacchetti per rilevare e prevenire attività sospette. Inoltre implementare sicurezza a livello fisico (dato che in questo caso l’attacco è avvenuto dall’interno) monitorare ingressi e uscite di gente sospetta, migliorare sistema di sorveglianza e la sicurezza dei badge, monitorare i file di log e assicurarsi ogni dipendente abbia i permessi corrispettivi, infine assicurarsi che la sala server sia inaccessibile da personale non autorizzato.**