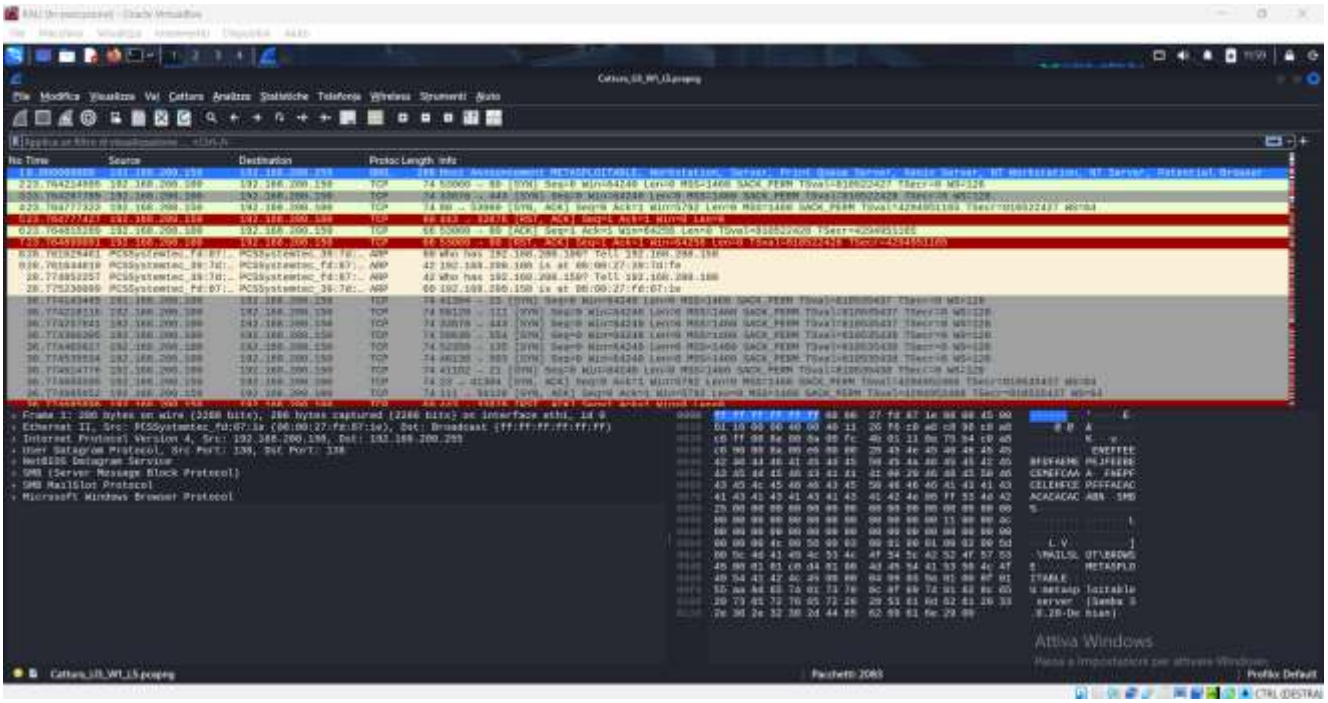
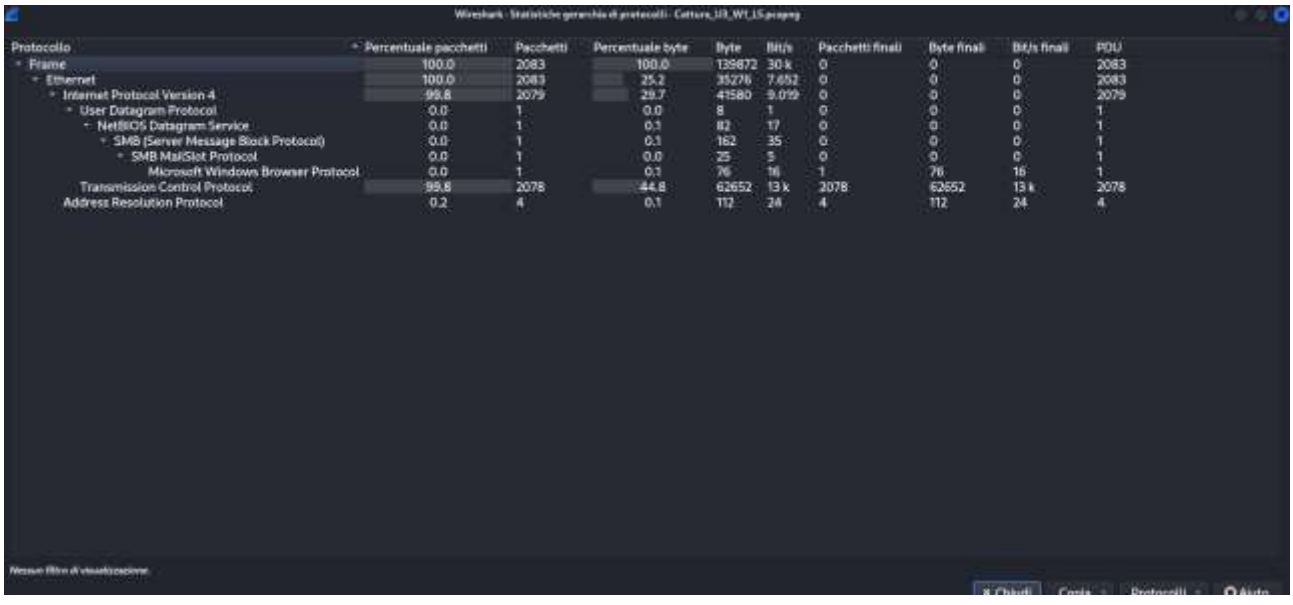
Threat Intelligence & IOC(progettoS9L5)

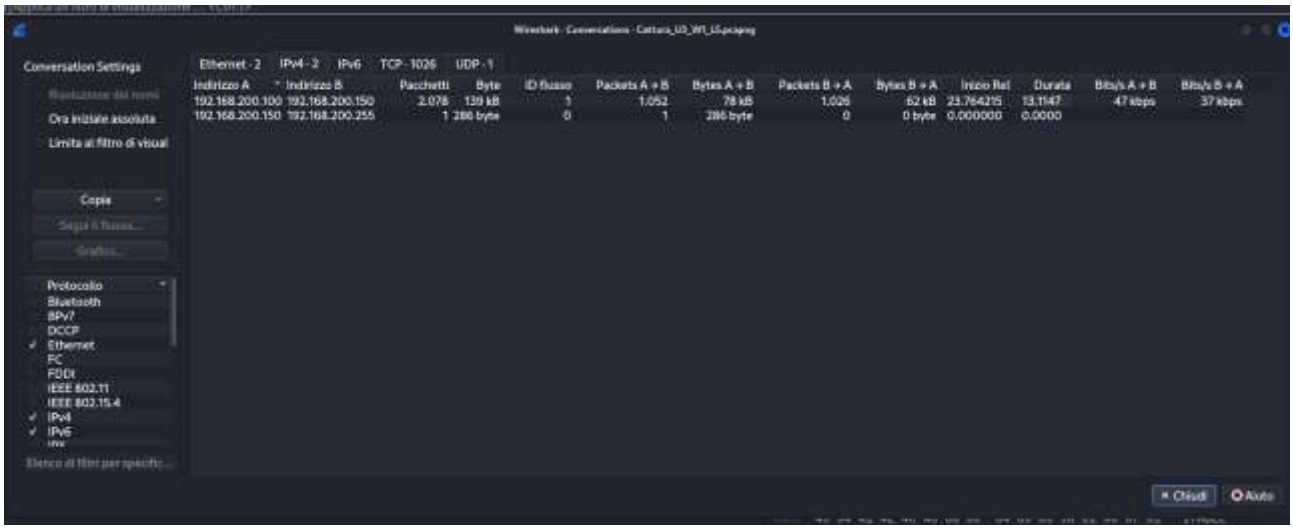


Lo scopo di questa analisi è esaminare una cattura di traffico di rete .pcapng per identificare potenziali Indicatori di Compromissione (IOC), formulare ipotesi sui vettori di attacco e proporre azioni di mitigazione e prevenzione.

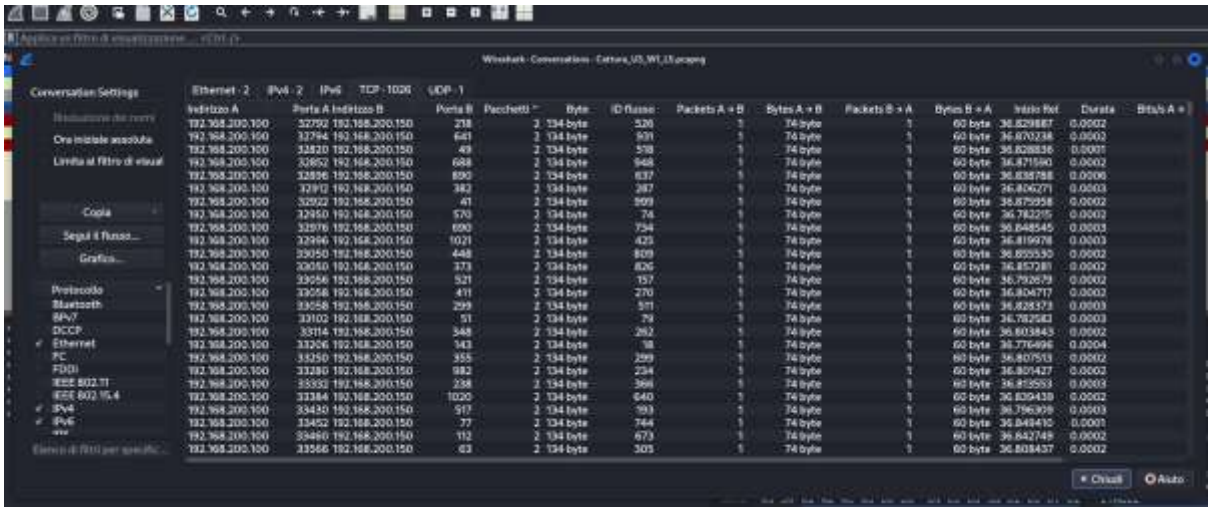
Ho iniziato con la Gerarchia dei protocolli e ha rivelato che la maggior parte del traffico nella cattura è basata su **IPv4** e, all'interno di questo, su **TCP (99.0%)**. Altri protocolli come UDP, ARP, SMB e NetBIOS sono presenti in percentuali minime. Quindi ci suggerisce un traffico di rete standard con un focus su comunicazioni tramite connessione.



Vedendo le conversazioni a livello IPv4 ci dice che la stragrande maggior parte del traffico si concentra tra due indirizzi IP interni alla stessa sottorete: **192.168.200.100** e **192.168.200.150**



Invece le conversazioni TCP ,da qui, è stato confermato che 192.168.200.100 è la sorgente che avvia la maggior parte delle connessioni verso 192.168.200.150 su diverse porte.



Alcune porte di destinazione su 192.168.200.150 mi hanno fatto attirare l'attenzione ovvero:

- **Porta 445 (SMB):** Un servizio comune per la condivisione file Windows, che è usato anch come bersaglio.
- **Porta 381:** Una porta insolita per una rete IT standard, che è associata a dispositivi specifici.

Mi sono concentrato tra 192.168.200.100 e 192.168.200.150.

Porta 381 Il traffico mostra un handshake TCP (SYN, SYN, ACK) seguito immediatamente da un reset (RST) da parte di 192.168.200.100. Ha indicato che il servizio sulla porta 381 su 192.168.200.150 è in ascolto ma la connessione è stata interrotta subito dopo la sua instaurazione, senza scambi.

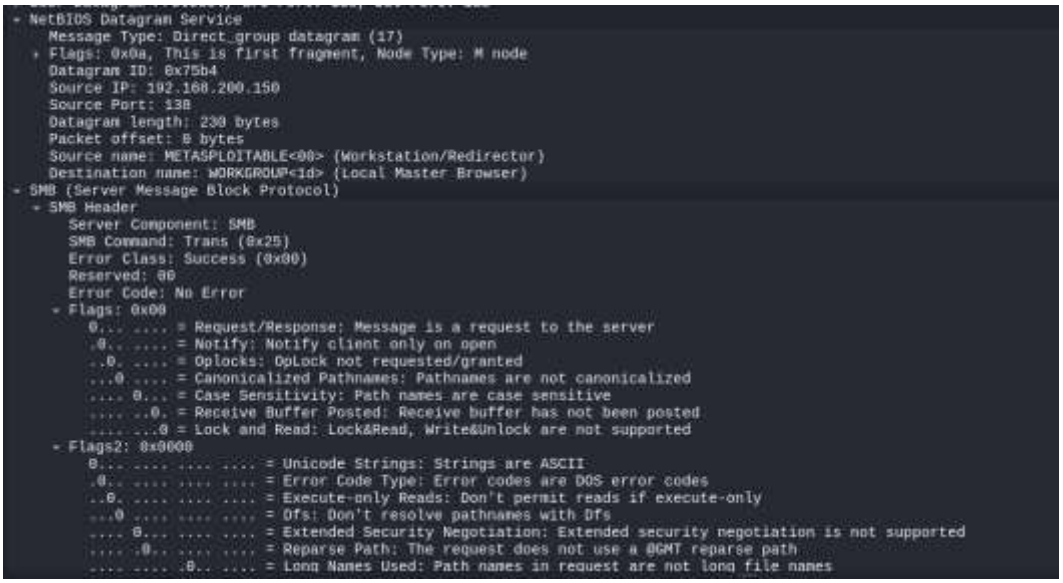
Porta 445 (SMB) la connessione TCP è stata stabilita con successo. Un'analisi approfondita dello stream TCP non ha rivelato alcuno scambio di dati applicativi SMB significativo dopo l'handshake. La connessione viene poi chiusa.

Questo comportamento ripetuto di "connetti e chiudi subito" su diverse porte indica chiaramente una scansione delle porte da parte di 192.168.200.100 per capire quali servizi sono attivi su 192.168.200.150

Il più importante Indicatore di Compromissione (IOC) scoprendolo analizzando un pacchetto di annuncio di rete presente nella cattura

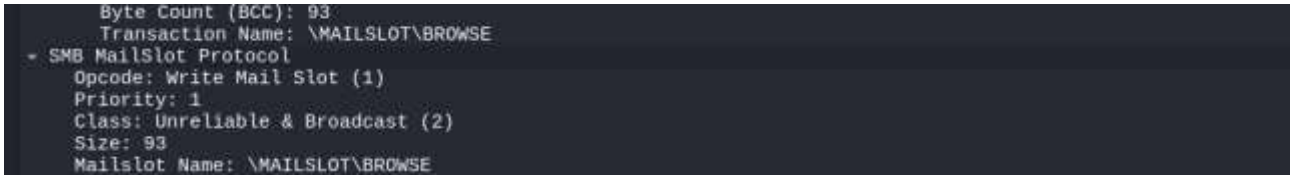
Questo pacchetto ha rivelato che l'indirizzo 192.168.200.150 si identificava come "METASPLOITABLE". Metasploitable è una macchina virtuale creata apposta per essere vulnerabile e viene usata per test di attacchi e sicurezza(ma noi facciamo finta). Ci conferma che 192.168.200.150 è un bersaglio progettato per essere attaccato.

Esamino un pacchetto che appartiene al "NetBIOS Datagram Service". Vedo che si tratta di un datagramma di tipo "Direct group datagram" e la sua dimensione è di 230 byte. La cosa interessante è che la sorgente è 192.168.200.150 e si riferisce a "metasploitable" con la destinazione "workgroup" qui mi fa pensare che si tratti di una VM

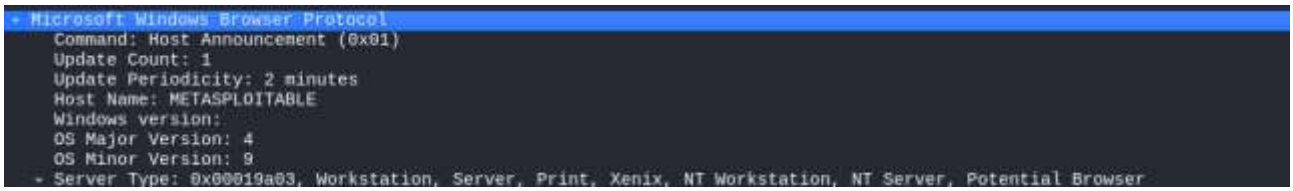


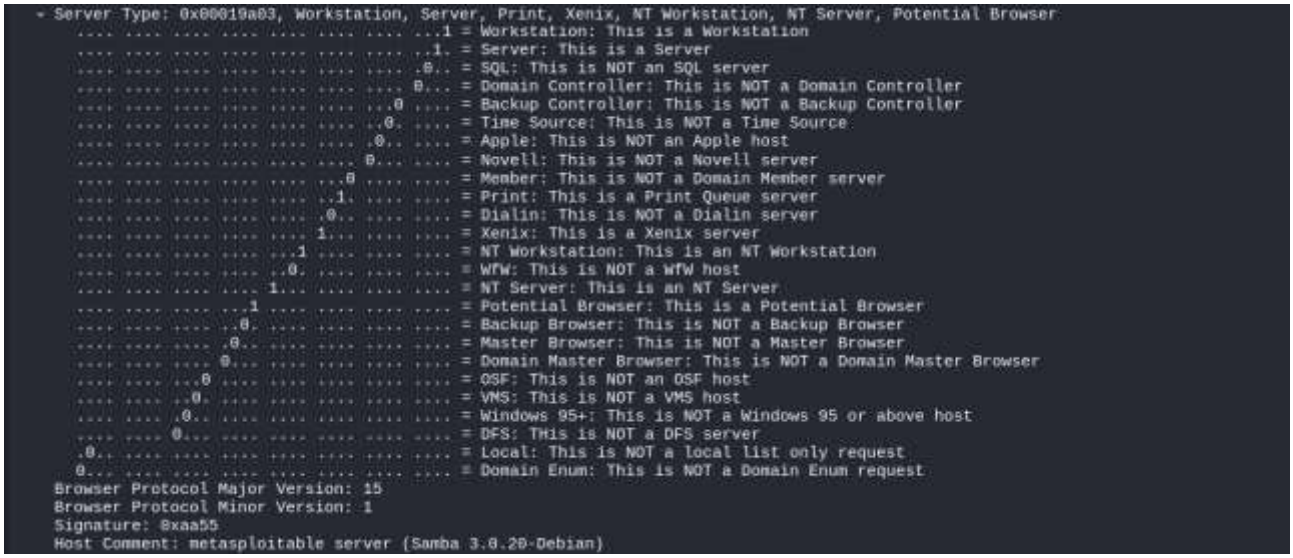
Abbiamo SMB All'interno dello stesso pacchetto. Vedo che il comando è un "Trans (0x25)" e l'operazione ha avuto successo. Analizzando i flag, noto alcune cose,indicando che è una richiesta inviata al server e che le stringhe utilizzate sono in formato ASCII.

Andando avanti mi mostra l'attività legata al SMB MailSlot Protocol. Qui indica che il sistema metasploitable sta scrivendo a un mailslot specifico per scopi di Browse di rete.



Il "Host Comment" “metasploitable server (Samba 3.0.20-Debian)" è la conferma: METASPLOITABLE.





IPOTESI: Dato che 192.168.200.150 è una macchina Metasploitable, l'aggressore 192.168.200.100 e quindi sta cercando di sfruttare le sue vulnerabilità note. Sulle porte come la **381** l'attaccante potrebbe tentare exploit specifici per quei servizi. Sulla **porta 445 (SMB)**, qui ci sono tentativi di indovinare le password per accedere alle condivisioni, o tramite comandi a distanza.

Qui l'attaccante sta cercando il modo migliore per entrare nel sistema.

CONSIGLI PER RIDURRE GLI IMPATTI E PREVENIRE ATTACCHI FUTURI: La prima cosa che farei è isolare la macchina 192.168.200.150 dalla rete. Essendo una macchina volutamente vulnerabile, rappresenta un rischio abbastanza alto e potrebbe compromettere altri sistemi.

Bisogna mantenere tutti i sistemi e i programmi sempre aggiornati con le ultime patch di sicurezza. Chiudere le porte, almeno quelle non necessarie in modo da non avere altri punti deboli. Configurare sempre il firewall per bloccare il traffico. Fare una segmentazione di rete con le

VLAN cosi’ da dividere la rete in sezioni più piccole e isolate ed essere piu’ protetti. Usare password complessi. Attivando IDS/IPS per mettere in rete una maggiore prevenzione delle intrusioni per bloccare automaticamente le scansioni. Infine controllare sempre log di sistema e il traffico di rete per vedere se ci sono attività abbastanza sospette.