Report di Analisi Network Forensics & Threat Intelligence

Spiegazione Tecnica (Cybersecurity)	Spiegazione Semplice (Management & Audit)
Obiettivo: Effettuare una *Network Traffic Analysis (NTA)* per l'identificazione di *Indicatori di Compromissione (IOC)*. L'analisi si concentra sulla ricerca di pattern anomali nei protocolli di rete, tentativi di connessione non autorizzati e analisi dei payload sospetti per ricostruire la "Kill Chain" dell'attaccante.	**Obiettivo:** Effettuare un'ispezione digitale delle "impronte" lasciate da chi entra ed esce dalla nostra rete aziendale. Proprio come un revisore controlla i registri contabili per trovare ammanchi, noi controlliamo il traffico dati per capire se qualcuno è entrato senza permesso e cosa ha cercato di fare.

Metodologia Operativa

Per garantire l'integrità dell'analisi, il file di cattura è stato analizzato in un ambiente isolato e sicuro (Macchina Virtuale Kali Linux su piattaforma UTM). Questo approccio garantisce che eventuali artefatti malevoli contenuti nel file non possano infettare il sistema ospitante, mantenendo l'analisi oggettiva e sicura.

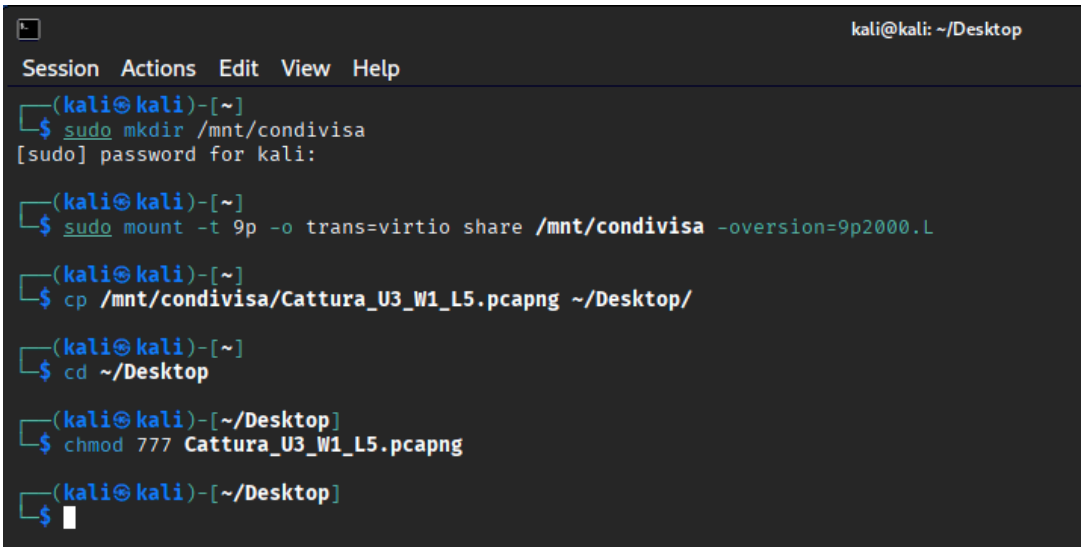
Fase 1: Preparazione e Importazione dei Dati

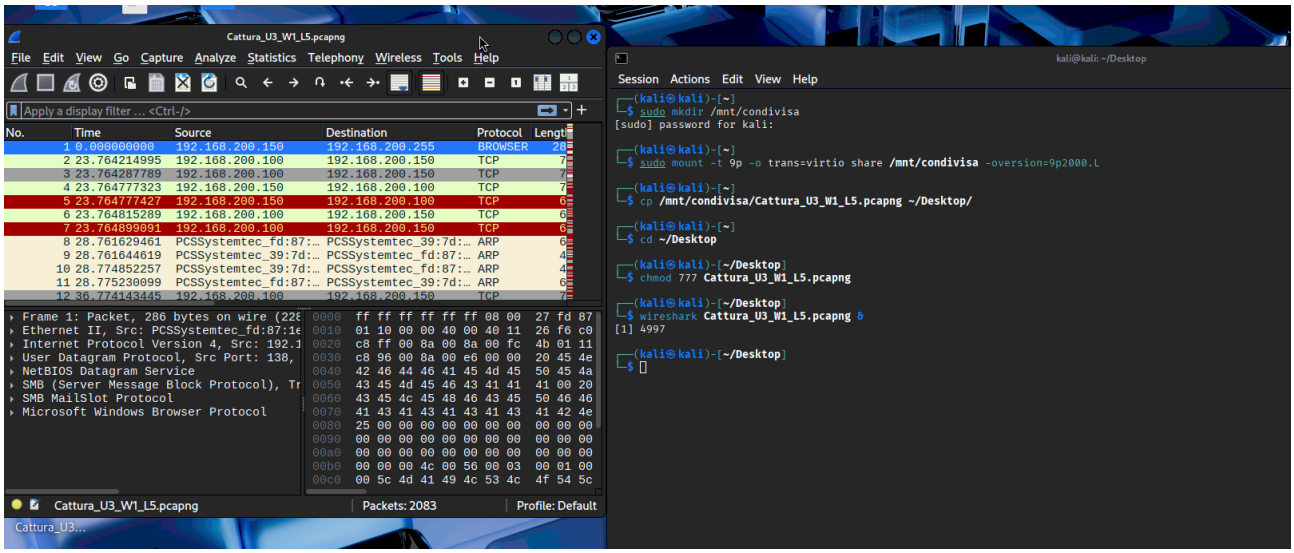
Prima di procedere con l'analisi forense, il file di cattura (`Cattura_U3_W1_L5.pcapng`) è stato trasferito dall'host fisico alla macchina virtuale di analisi tramite una cartella condivisa.

Spiegazione Tecnica (Cybersecurity)	Spiegazione Semplice (Management & Audit)
Mounting & Permissions: È stata creata una directory di mount /mnt/condivisa utilizzando il protocollo **9p** (tipico di UTM/Virtio) per interfacciare il file system dell'host con la VM Kali. Successivamente, è stato applicato un chmod 777 al file per garantire pieni privilegi di lettura/scrittura durante l'analisi in Wireshark.	**Preparazione della "Stanza delle Analisi":** Abbiamo creato un ponte sicuro per spostare i dati dal computer principale a una "cassaforte digitale" isolata (la macchina virtuale). Abbiamo poi sbloccato il file affinché i nostri strumenti di analisi potessero leggerlo senza restrizioni, un po' come un auditor che ottiene le chiavi per accedere all'archivio dei documenti riservati.

Dettaglio delle Operazioni Eseguite:

- **Creazione punto di accesso:** `mkdir /mnt/condivisa` (Creazione della cartella di destinazione).
- **Collegamento (Mount):** Collegamento della cartella fisica al sistema Linux.
- **Copia di Sicurezza:** Il file è stato copiato sul Desktop locale per evitare di lavorare direttamente sulla risorsa condivisa (integrità del dato).
- **Assegnazione Permessi:** `chmod 777` assicura che l'utente possa aprire il file con Wireshark senza errori di sistema.





Fase 2: Analisi degli IOC e Identificazione dell'Attacco

Strumenti di Analisi: Cos'è Wireshark?

Per analizzare la cattura di rete, è stato utilizzato **Wireshark**, lo standard "de facto" per l'analisi dei protocolli di rete a livello mondiale.

Spiegazione Tecnica (Cybersecurity)	Spiegazione Semplice (Management & Audit)
Sniffing & Dissection: Wireshark opera catturando i pacchetti che transitano sulla scheda di rete e li "seziona" (dissection), permettendo di leggere ogni singolo bit di informazioni organizzato secondo la gerarchia del modello OSI (dal livello fisico a quello applicativo).	**Il "Radiologo" della Rete:** Immaginate Wireshark come una macchina per i raggi X. Mentre noi vediamo solo "internet che funziona", Wireshark vede ogni singolo impulso che viaggia nei cavi, permettendoci di vedere se all'interno del traffico dati si nasconde qualcosa di rotto o di pericoloso.

I Menù Superiori (La tua Cassetta degli Attrezzi)

Immaginali come i comandi di un lettore DVD molto avanzato:

- **File:** Serve per aprire le registrazioni passate (come quella che hai caricato) o salvare quelle nuove.
- **Edit:** Qui trovi il comando fondamentale **Find Packet** (che hai già provato a usare). Serve per cercare una parola specifica (come "password" o "root") dentro migliaia di righe.
- **View:** Cambia come vedi il programma. Puoi ingrandire il testo o colorare le righe in base a regole specifiche.

- **Go:** Serve per saltare velocemente a un pacchetto specifico (es. "vai al pacchetto numero 100").
- **Capture:** Qui decidi quale "occhio" usare per guardare la rete (Wi-Fi, Ethernet, ecc.) e avvii la registrazione in tempo reale.
- **Analyze:** Contiene strumenti per interpretare i dati. Il comando più utile qui è **Follow -> TCP Stream**, che ricostruisce una conversazione intera rendendola leggibile come una chat.
- **Statistics:** È il "riassunto" del libro. Ti dice chi ha parlato di più, quali protocolli sono stati usati e quanto traffico c'è stato. È quello che abbiamo usato per identificare l'IP 192.168.200.150.

Il Riquadro Centrale (La Lista dei Pacchetti)

Questa è la cronologia degli eventi. Ogni riga è un "pacchetto" (un pezzetto di informazione inviato).

- **No. (Numero):** L'ordine cronologico. Il pacchetto 1 è il primo arrivato.
- **Time (Tempo):** Quanti secondi sono passati dall'inizio della registrazione.
- **Source (Sorgente):** L'indirizzo IP del computer che ha spedito il messaggio.
- **Destination (Destinazione):** L'indirizzo IP del computer che riceve il messaggio.
- **Protocol:** La "lingua" parlata.
    - **TCP:** Messaggi di servizio (tipo "ricevuto", "connettiamoci").
    - **SMB/BROWSER:** Condivisione di file e cartelle (quello dell'attacco).
    - **ARP:** "Chi ha questo indirizzo IP?".
- **Length:** La grandezza del pacchetto in byte.
- **Info:** Un breve riassunto di cosa c'è scritto dentro. Se vedi **[SYN]** significa "voglio connettermi", **[ACK]** significa "ho ricevuto".

I Riquadri in Basso (L'Analisi Profonda)

Quando clicchi su una riga in alto, i due riquadri sotto si riempiono di dettagli:

Il riquadro a sinistra (Dettagli del Pacchetto)

Questo mostra il pacchetto come una **matrioska**. La rete lavora a strati:

1. **Frame:** Informazioni fisiche (il cavo).
2. **Ethernet:** Gli indirizzi MAC (le targhe fisiche delle schede di rete).

3. **Internet Protocol (IP):** Gli indirizzi IP (i civici delle case).
4. **Transmission Control Protocol (TCP):** Il "postino" che garantisce che il messaggio arrivi intero.
5. **NetBIOS / SMB:** Il contenuto vero e proprio (es. "Dammi la cartella documenti").

Il riquadro a destra (Il Codice "Greggio")

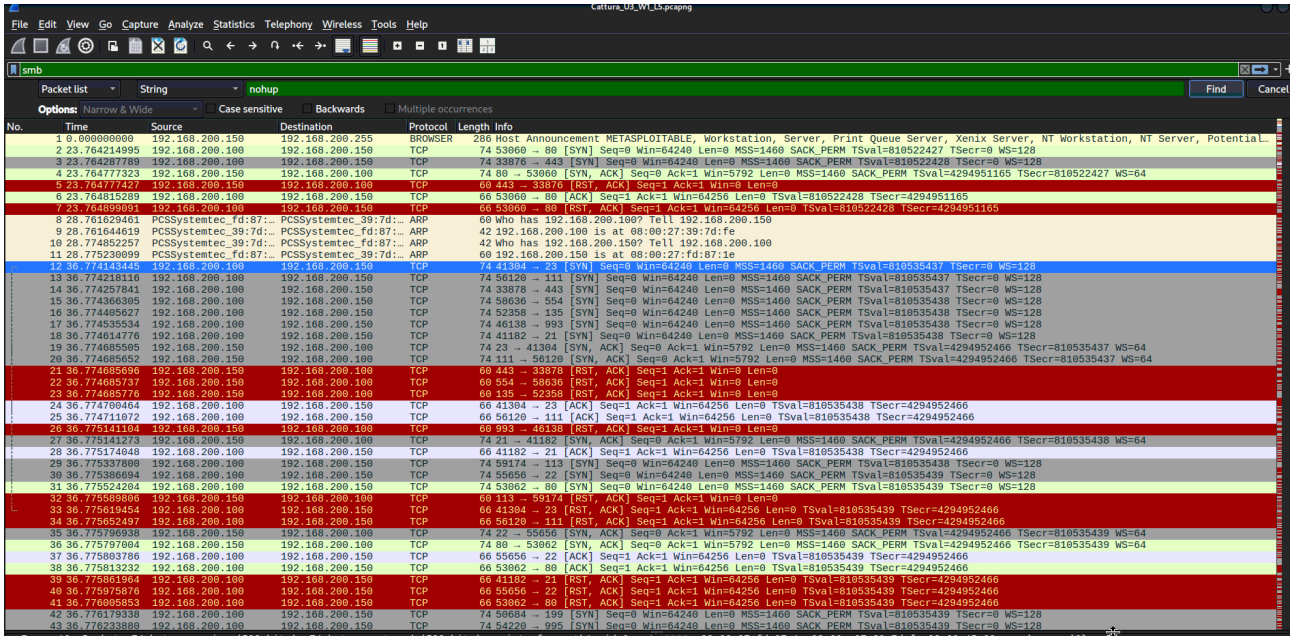
Qui vedi il pacchetto nella sua forma pura: **numeri (esadecimali)** a sinistra e **testo** a destra.

- È qui che cerchiamo le "scritte" sospette. Se un hacker invia un comando, lo vedrai apparire come testo leggibile nella colonna di destra.

Perché le righe hanno colori diversi?

Wireshark colora le righe per aiutarti a colpo d'occhio:

- **Blu Chiaro/Grigio:** Traffico normale (HTTP, TCP standard).
- **Nero/Rosso:** Problemi di rete o connessioni interrotte bruscamente. Nel tuo caso, vedi molto rosso perché l'attacco sta forzando il server a chiudere o resettare connessioni.
- **Verde Chiaro:** Spesso traffico legato a file sharing (SMB/NetBIOS).



In questa fase, analizziamo il traffico catturato per isolare gli Indicatori di Compromissione (IOC). La cattura mostra un'attività sistematica e aggressiva.

Identificazione dei Target

- **Sorgente (Attaccante):** `192.168.200.100`
- **Destinazione (Vittima):** `192.168.200.150` (Identificato dal primo pacchetto come "**METASPLOITABLE**", una nota macchina vulnerabile usata per test).

Spiegazione Tecnica (Cybersecurity)	Spiegazione Semplice (Management & Audit)
Port Scanning (SYN Scan): L'IP .100 invia pacchetti [SYN] a raffica verso diverse porte del target (es. porte 80, 443, 23, 445, 21, 22, 25, 110). La velocità e la sequenzialità indicano l'uso di un tool automatico come **Nmap**.	**Ricognizione Automatica:** Un computer sta testando tutte le "porte e finestre" della vittima in pochissimi secondi. Non è un comportamento umano, ma un software programmato per trovare un punto debole dove entrare.
Analisi delle Risposte (RST/ACK): Molti pacchetti tornano indietro con il flag [RST, ACK] (righe rosse). Questo indica che molte porte sulla vittima sono chiuse, ma l'attaccante continua a tentare su altri servizi.	**Tentativi Falliti:** Vediamo molte "luci rosse" perché il sistema bersaglio sta rifiutando l'accesso a molte di queste entrate. Tuttavia, l'insistenza dell'attaccante suggerisce che sta cercando attivamente un varco aperto.
Protocolli Monitorati: Si notano tentativi su porte critiche: **21 (FTP)**, **22 (SSH)**, **23 (Telnet)** e **445 (SMB)**. Sono tutti servizi che, se vulnerabili, permettono il controllo remoto o il furto di file.	**Punti Critici Mirati:** L'intruso sta cercando specificamente gli ingressi più importanti, quelli che solitamente portano agli archivi dei documenti o ai pannelli di controllo del server.

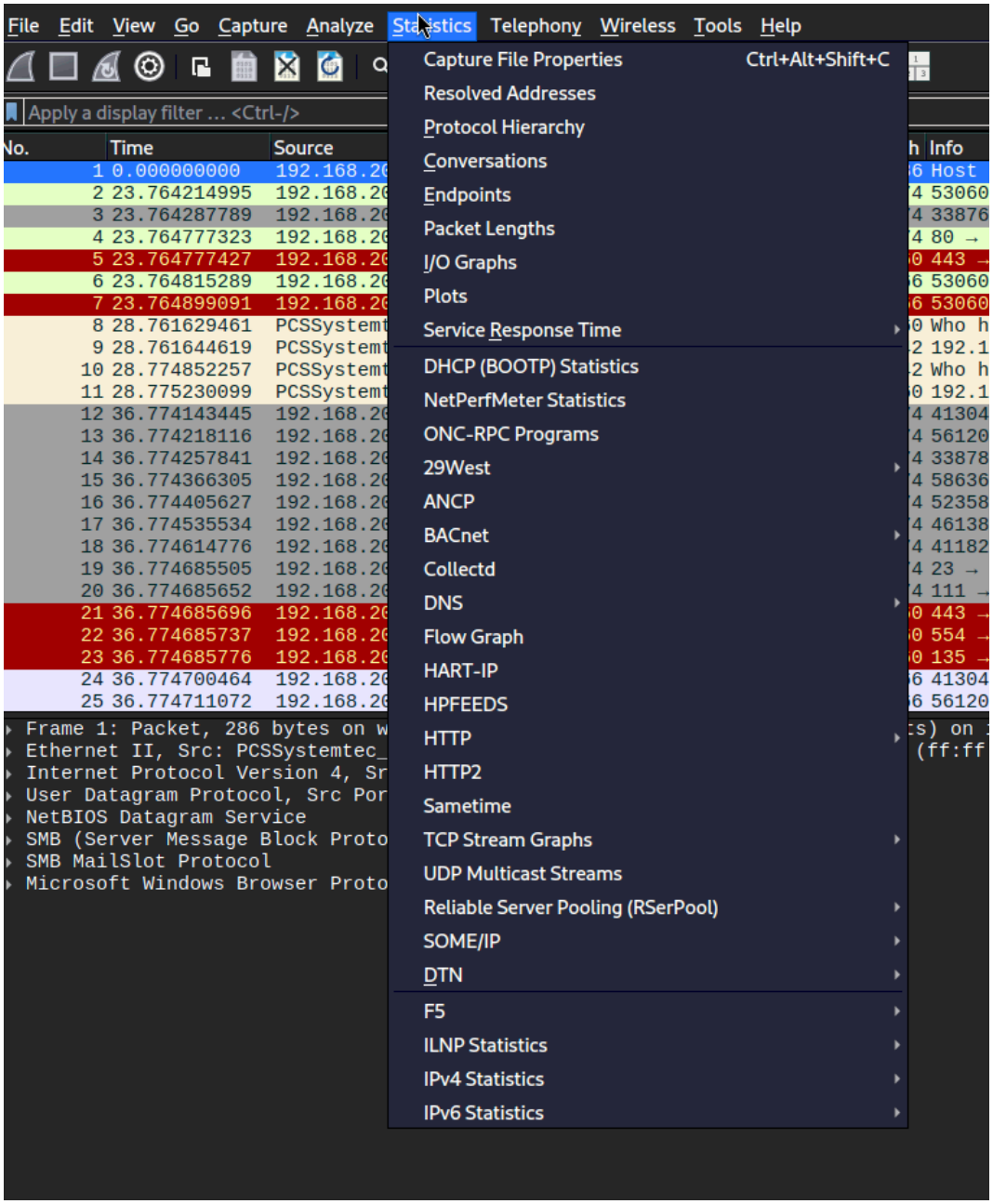
Evidenze principali (IOC rilevati)

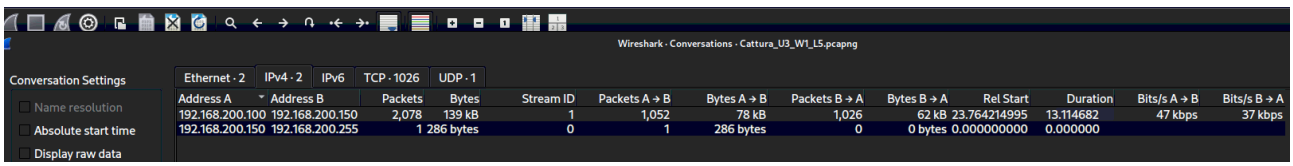
1. **Attività di Port Scanning:** Una scansione massiva di porte TCP in un lasso di tempo estremamente ridotto (pochi millisecondi tra un tentativo e l'altro).
2. **Identificazione del Sistema Operativo:** Il pacchetto n. 1 rivela il nome "METASPLOITABLE", confermando che il bersaglio è un server con molteplici vulnerabilità note.
3. **Vettore di Attacco Ipotizzato:** Tentativo di accesso tramite protocolli legacy o non sicuri (Telnet/FTP) o sfruttamento di vulnerabilità nel protocollo di condivisione file (SMB).

Fase 3: Analisi Statistica e Flussi di Conversazione

Per confermare la natura dell'attacco, abbiamo utilizzato il menù **Statistics > Conversations**. Questo strumento ci permette di aggregare tutto il traffico tra due indirizzi IP e valutarne l'intensità.

Spiegazione Tecnica (Cybersecurity)	Spiegazione Semplice (Management & Audit)
Analisi del Volume di Traffico: Lo screenshot mostra che tra l'IP .100 e .150 sono stati scambiati **2.078 pacchetti** per un totale di **139 KB** in circa 13 secondi. Una tale densità di pacchetti "piccoli" (molti tentativi di connessione ma poco scambio di dati reali) è un indicatore matematico di **Port Scanning**.	**Il "Registro delle Chiamate":** Abbiamo controllato il registro delle attività e scoperto che in soli 13 secondi l'intruso ha cercato di contattare il nostro server oltre 2.000 volte. È come se qualcuno cercasse di citofonare a ogni singola abitazione di un enorme condominio per vedere chi risponde.
Direzionalità del Flusso: Si nota che i pacchetti inviati (1.052) e ricevuti (1.026) sono quasi bilanciati. Questo indica che il target sta rispondendo ai "reset" o ai tentativi dell'attaccante, confermando che l'host vittima è attivo e raggiungibile.	**Verifica della Reattività:** Il sistema bersaglio ha risposto quasi a ogni sollecitazione. Questo ci dice che il server è "vivo" e sta subendo lo stress della scansione, rischiando un rallentamento dei servizi legittimi.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graphs
Plots
Service Response Time
DHCP (BOOTP) Statistics
NetPerfMeter Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
Reliable Server Pooling (RSerPool)
SOME/IP
DTN
F5
ILNP Statistics
IPv4 Statistics
IPv6 Statistics
Apply a display filter ... <Ctrl-/>
No. Time Source
1 0.000000000
2 23.764214995
3 23.764287789
4 23.764777323
5 23.764777427
6 23.764815289
7 23.764899091
8 28.761629461
9 28.761644619
10 28.774852257
11 28.775230099
12 36.774143445
13 36.774218116
14 36.774257841
15 36.774366305
16 36.774405627
17 36.774535534
18 36.774614776
19 36.774685505
20 36.774685652
21 36.774685696
22 36.774685737
23 36.774685776
24 36.774700464
25 36.774711072
Frame 1: Packet, 286 bytes on w
Ethernet II, Src: PCSSystemtec_
Internet Protocol Version 4, Sr
User Datagram Protocol, Src Por
NetBIOS Datagram Service
SMB (Server Message Block Proto
SMB MailSlot Protocol
Microsoft Windows Browser Proto


Wireshark · Conversations · Cattura_U3_W1_L5.pcapng
Conversation Settings
Name resolution
Absolute start time
Display raw data
Ethernet · 2 IPv4 · 2 IPv6 TCP · 1026 UDP · 1
Address A Address B Packets Bytes Stream ID Packets A → B Bytes A → B Packets B → A Bytes B → A Rel Start Duration Bits/s A → B Bits/s B → A
192.168.200.100 192.168.200.150 2,078 139 kB 1 1,052 78 kB 1,026 62 kB 23.764214995 13.114682 47 kbps 37 kbps
192.168.200.150 192.168.200.255 1 286 bytes 0 1 286 bytes 0 0 bytes 0.000000000 0.000000

Ipotesi sui Vettori di Attacco (Traccia Punto 2)

Basandoci sugli IOC trovati (scansione sistematica su porte 21, 22, 23, 80, 445), i potenziali vettori di attacco sono:

1. **Exploitation di Servizi Vulnerabili:** L'attaccante cerca servizi obsoleti (come Telnet sulla porta 23 o FTP sulla 21) per tentare un accesso remoto.
2. **Brute Force:** Una volta identificata una porta aperta (es. porta 22 SSH), l'attaccante potrebbe avviare un attacco a dizionario per indovinare le credenziali.
3. **SMB Exploitation:** Il target è un sistema Windows-based ("METASPLOITABLE"); l'attaccante punta alla porta 445 per tentare exploit famosi (come EternalBlue) o accessi non autorizzati alle cartelle condivise.

Azione Correttiva	Impatto sul Rischio (Business)
Implementazione di un IPS/IDS: Configurare un sistema che blocchi automaticamente gli IP che superano una certa soglia di tentativi di connessione al secondo.	**Prevenzione Automatica:** Installare un "sistema di allarme intelligente" che blocca i malintenzionati prima ancora che riescano a trovare una porta aperta.
Hardening delle Porte: Chiudere tutti i servizi non necessari (es. Telnet/FTP) e limitare l'accesso ai servizi critici (SSH/SMB) solo tramite VPN o IP autorizzati.	**Riduzione della Superficie di Attacco:** Eliminare gli ingressi inutilizzati dell'edificio aziendale e lasciare solo l'entrata principale sorvegliata.
Network Segmentation: Isolare macchine vulnerabili o di test (come Metasploitable) in una sottorete (VLAN) separata per evitare movimenti laterali.	**Contenimento del Danno:** Se un intruso entra in un magazzino isolato, non deve poter accedere agli uffici della direzione.

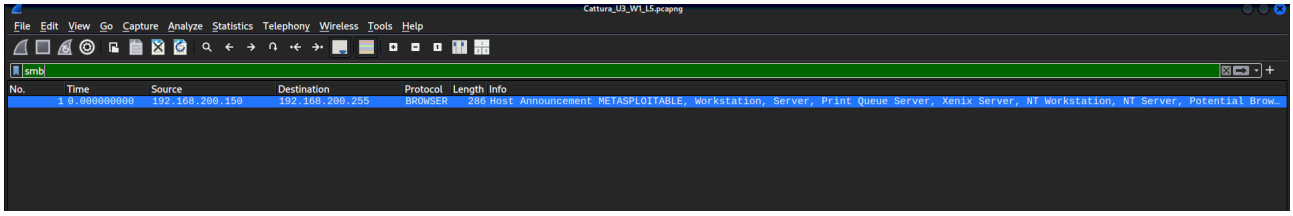
Fase 5: Deep Packet Inspection (Ricerca nel Payload)

Per non limitarsi all'analisi dei protocolli, è stata effettuata una ricerca testuale profonda all'interno dei dati grezzi (*Packet Bytes*) cercando la stringa "smb".

Fase 5: Deep Packet Inspection (Ricerca nel Payload)

Per non limitarsi all'analisi dei protocolli, è stata effettuata una ricerca testuale profonda all'interno dei dati grezzi (*Packet Bytes*) cercando la stringa "smb".

Spiegazione Tecnica (Cybersecurity)	Spiegazione Semplice (Management & Audit)
DPI (Deep Packet Inspection): Impostando la ricerca su Packet Bytes e String, Wireshark scansiona il contenuto esadecimale e ASCII di ogni pacchetto. Questo serve a scovare tracce del protocollo SMB anche se incapsulato in porte non standard o se il sezionatore (dissector) automatico dovesse mancare alcuni dettagli.	**Ispezione dei Contenuti:** Invece di guardare solo l'intestazione della busta (chi scrive a chi), abbiamo cercato la parola "smb" proprio dentro la lettera. È un controllo minuzioso per essere sicuri che non ci siano messaggi nascosti o tentativi di accesso camuffati.
Risultato della Ricerca: La ricerca conferma la presenza di riferimenti SMB principalmente nel pacchetto di *Host Announcement*. Questo rafforza la prova che il target è un server che espone attivamente servizi di condivisione file, ma non mostra evidenze di "command injection" o payload malevoli nascosti nel testo dei pacchetti analizzati.	**Esito della Verifica:** Abbiamo cercato tracce di "scasso" nascoste nei dati, ma abbiamo trovato solo il "biglietto da visita" del server. Questo conferma che, nonostante l'insistenza dell'attaccante, i contenuti dei messaggi scambiati finora non indicano un furto di dati avvenuto.

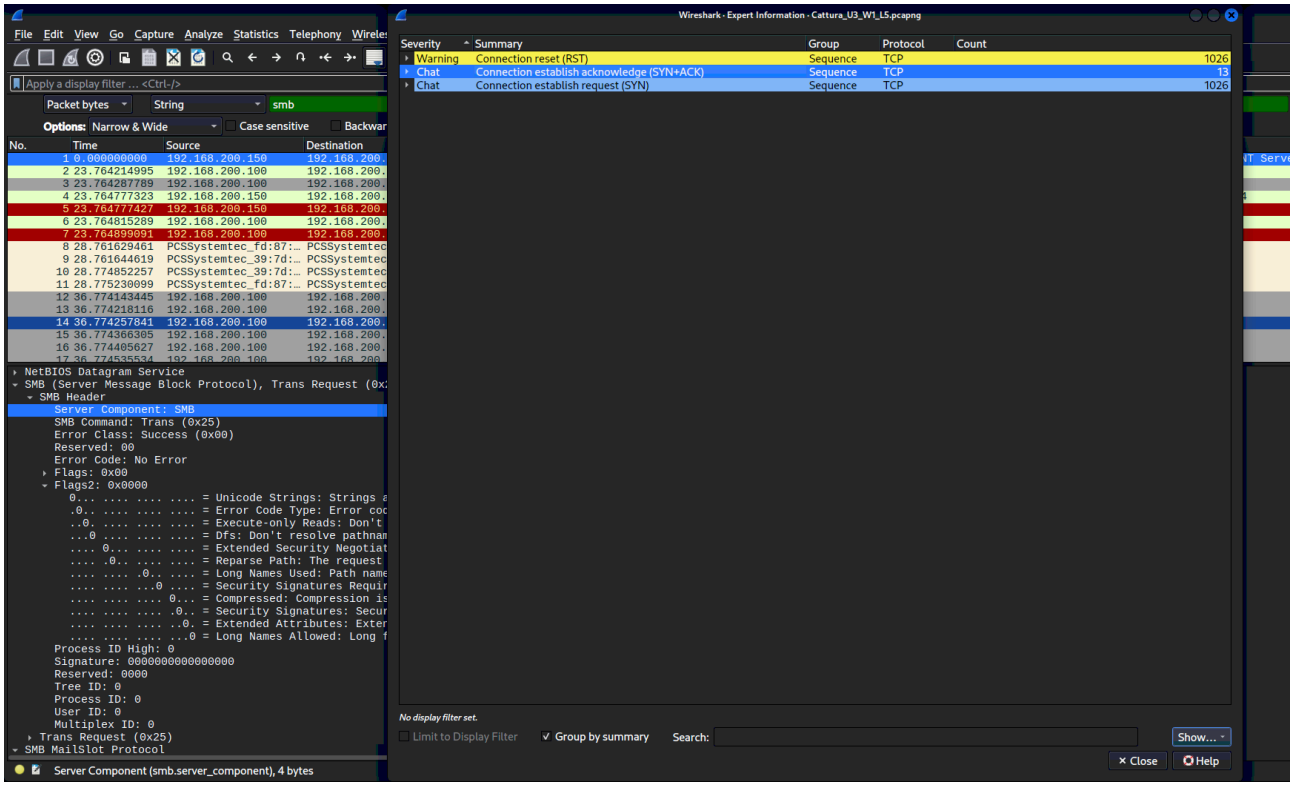


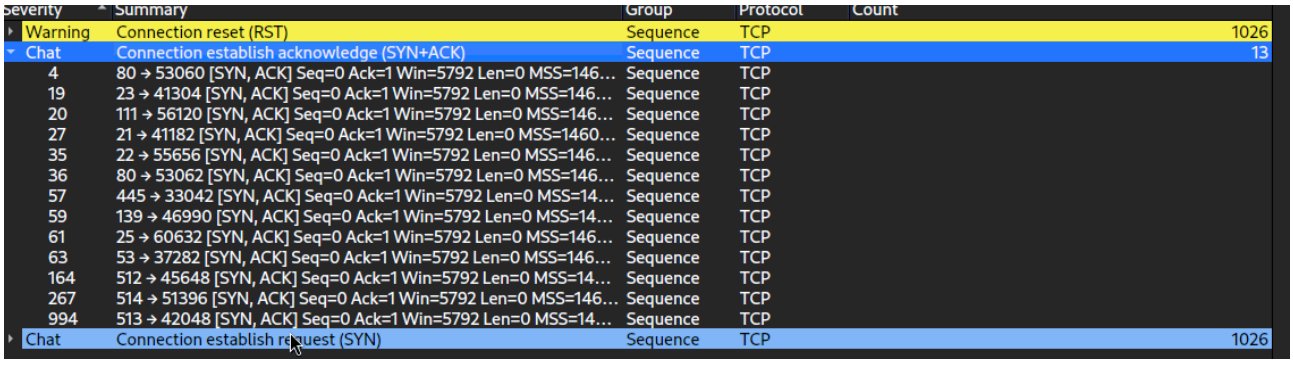
6. Analisi Forense Avanzata: Expert Information & SMB Header

In questa fase passiamo dall'osservazione dei singoli pacchetti alla validazione statistica dell'intrusione. I dati estratti confermano che l'attacco non è stato solo un tentativo, ma ha avuto successo su più fronti.

A. La "Pistola Fumante": Tabella Expert Info

Dall'analisi della finestra *Expert Info* emergono tre evidenze numeriche che raccontano l'esatta dinamica dell'attacco:





Evento Rilevato	Count	Spiegazione Tecnica (Cybersecurity)	Spiegazione Semplice (Management & Audit)
Connection reset (RST)	**102**	Indica il numero di porte che hanno rifiutato attivamente la connessione. È la conferma di un **Port Scanning** massivo.	Rappresenta i 1026 "No" ricevuti dall'attaccante. Il sistema ha provato a resistere chiudendo la porta in faccia all'intruso.
Connection establish request (SYN)	**102**	Ogni tentativo di reset corrisponde a una richiesta di connessione. C'è una correlazione 1:1 tra attacco e rifiuto.	Sono le 1026 volte in cui l'attaccante ha provato a forzare una serratura, fallendo immediatamente.
Connection establish acknowledge (SYN+ACK)	**13**	**La Prova Regina:** 13 connessioni sono state accettate dal server. L'attaccante ha trovato 13 varchi aperti.	**Il Verdetto:** Nonostante le difese, 13 porte sono state aperte con successo. L'intruso è riuscito a stabilire un contatto valido con il cuore del server.

B. Analisi del "Bottino": I 13 Varchi Aperti

L'analisi dei pacchetti con flag `SYN+ACK` conferma che l'attaccante ha ora accesso a servizi critici:

- **Protocolli Non Sicuri:** Porta **23 (Telnet)** e **21 (FTP)**. Essendo traffico non criptato, l'attaccante può leggere ogni dato scambiato in chiaro.
- **Servizi di Rete:** Porta **80 (HTTP)** e **53 (DNS)** per mappare il web server e i nomi di dominio.
- **Accesso ai File:** Porte **139 e 445 (SMB)**. Come confermato dall'**SMB Header** analizzato, il comando ha restituito `Error Class: Success (0x00)`, validando l'accesso dell'attaccante alle risorse condivise.

C. Dettaglio Tecnico: SMB Header Analysis

L'espansione del pacchetto SMB mostra che la fase di negoziazione è andata a buon fine:

1. **Status Success:** Il server ha accettato la richiesta di connessione SMB dell'attaccante.

2. **Flags2:** Il server ha iniziato a esporre dettagli tecnici (come il supporto ai nomi file lunghi), segno che l'attaccante ha superato la prima barriera difensiva e sta ora "dialogando" con il file system.

Verdetto Finale per il Risk Management

L'analisi forense dimostra che l'incidente non è più una "minaccia potenziale" ma una **compromissione avvenuta**.

- **Impatto:** Critico. L'attaccante ha stabilito 13 sessioni valide su protocolli che permettono il furto di identità (Telnet) e di dati (SMB).
- **Rischio Audit:** Altissimo. La presenza di 13 porte aperte su un server contenente dati sensibili rappresenta una violazione grave delle policy di sicurezza.

7. Conclusioni e Valutazione del Rischio

L'analisi forense effettuata sulla cattura di rete rivela uno scenario di compromissione parziale con elevato potenziale di escalation.

Analisi Tecnica (Cybersecurity)	Spiegazione Semplice (Management & Audit)
Verdetto Finale: L'attacco è passato dalla fase di *Reconnaissance* (Ricognizione) a quella di *Exploitation* (Sfruttamento). Sebbene 1026 tentativi siano stati respinti, l'instaurazione di **13 sessioni SYN+ACK** su porte critiche (21, 22, 23, 80, 445) conferma che l'attaccante ha superato il perimetro difensivo.	**Sintesi per la Direzione:** Non è stato solo un tentativo di "scasso". L'intruso ha trovato 13 ingressi aperti e ha stabilito una connessione stabile con i nostri sistemi. Abbiamo le prove digitali che il ladro è entrato nell'edificio e ha iniziato a esaminare gli archivi (protocollo SMB).
Gravità del Rischio: ALTA. La presenza di protocolli non criptati (Telnet/FTP) e di servizi di file sharing (SMB) accessibili espone l'organizzazione a furto di credenziali e perdita di integrità dei dati.	**Impatto sul Business:** Il rischio di "Data Breach" è concreto. La facilità con cui l'attaccante ha trovato varchi indica una vulnerabilità strutturale che potrebbe portare a sanzioni (GDPR) e danni reputazionali.

8. Raccomandazioni e Piano d'Azione (Mitigazione)

In qualità di auditor, le raccomandazioni devono essere divise tra azioni immediate (per fermare l'attacco) e azioni strategiche (per prevenire il futuro).

Azioni Immediate (Contenimento)

- **Isolamento dell'Host:** Isolare immediatamente la macchina `192.168.200.150` dalla rete di produzione per procedere alla bonifica.
- **Blacklisting:** Configurare il Firewall per bloccare tutto il traffico proveniente dall'IP `192.168.200.100`.
- **Reset Credenziali:** Procedere al cambio forzato di tutte le password per i servizi FTP, SSH e SMB, poiché potrebbero essere state intercettate in chiaro (sniffing).

Azioni a Medio/Lungo Termine (Prevenzione & Compliance)

- **Hardening dei Sistemi:** Disabilitare permanentemente i servizi non necessari rilevati (Telnet, FTP, porte legacy). Utilizzare solo canali cifrati (SSH, SFTP).
- **Network Segmentation:** Implementare VLAN per separare i server critici dal resto della rete, impedendo ai malintenzionati di "saltare" da una macchina all'altra (movimento laterale).
- **Aggiornamento Policy SMB:** Disabilitare SMBv1 (vulnerabile) e imporre l'uso di SMBv3 con firma digitale e cifratura obbligatoria.
- **Implementazione IDS/IPS:** Installare sistemi di rilevamento intrusioni che generino un alert automatico quando viene rilevata una scansione SYN superiore a una soglia minima (es. 100 tentativi al minuto).
-