Report 06/02/2026 Cristiano Samuel Vanvitelli

Threat Intelligence & IOC

Executive Summary

Il presente report illustra le fasi di acquisizione e analisi del traffico di rete tra due macchine in un ambiente di laboratorio controllato. L'attività ha avuto inizio con la preparazione dell'ambiente di lavoro su piattaforma **Kali Linux**, dove si è proceduto alla modifica dei privilegi di accesso e della proprietà del file di cattura (**.pcapng**) .

Si è passato all'analisi con **Wireshark** per esaminare nel dettaglio i flussi di traffico generati tra l'host attaccante e il target durante la sessione di acquisizione.

Obiettivo

Analizzare il traffico, evidenziare i tipi di attacchi in corso e quali possibili strumenti sono stati utilizzati e proporre strategie di mitigazione per prevenire un attacco futuro.

Strumenti Laboratorio

- **Kali:** macchina host
- **Wireshark:** tool analisi del traffico di rete

Fase1 – Creazione e upload cartella condivisa

*Fig.1 Creazione cartella condivisa

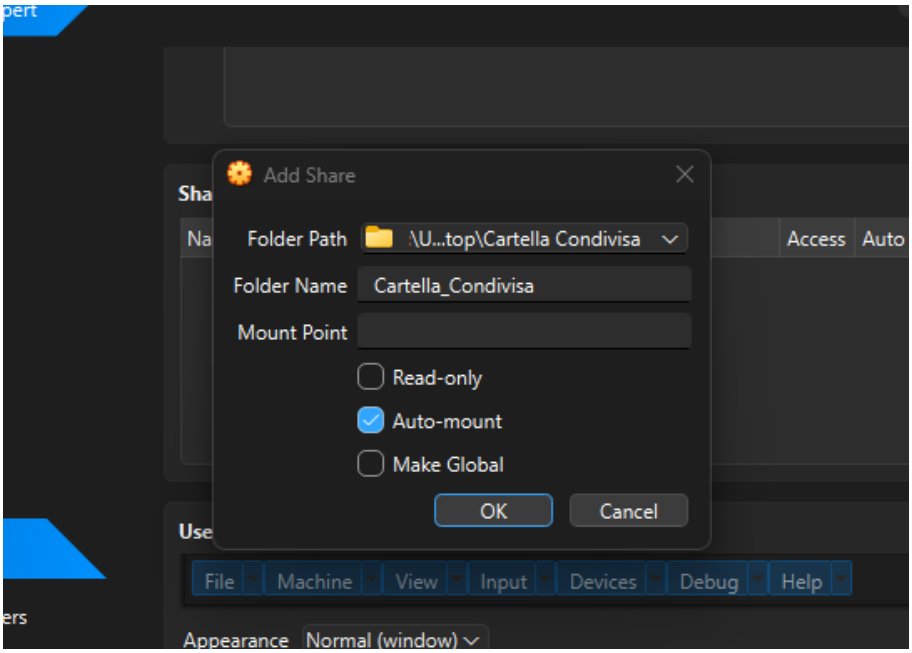

*Fig.2 Upload cartella condivisa

In fase preliminare all'analisi, è stata predisposta una cartella condivisa contenente il file di cattura (pcap); quest'ultimo è stato poi importato in Kali Linux per lo studio dei pacchetti.

Una volta configurata, si è proceduto al boot della Kali per eseguire i passaggi successivi dell'analisi.

Fase2 – Configurazione e Gestione Permessi Cartella Condivisa su Kali

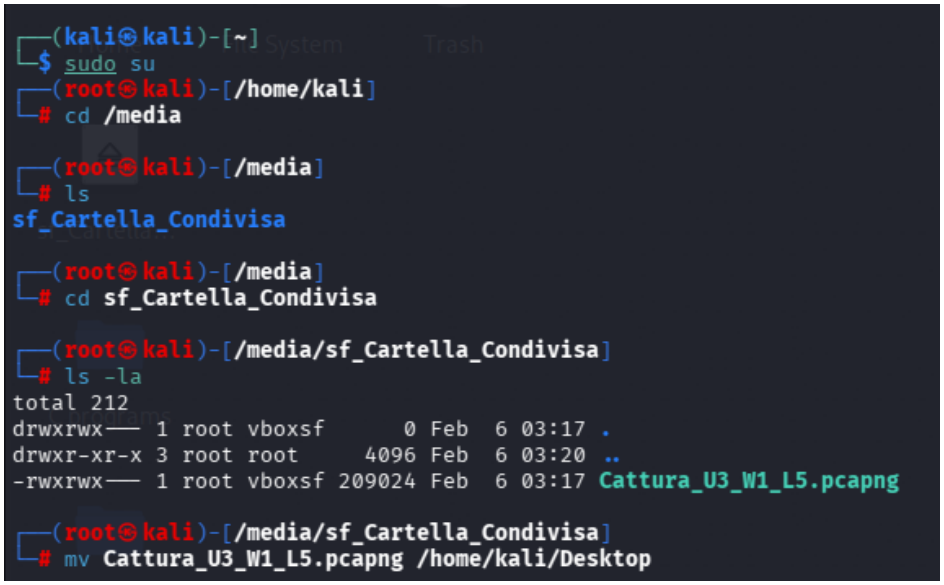

Fig.3 Trasferimento file sul desktop kali

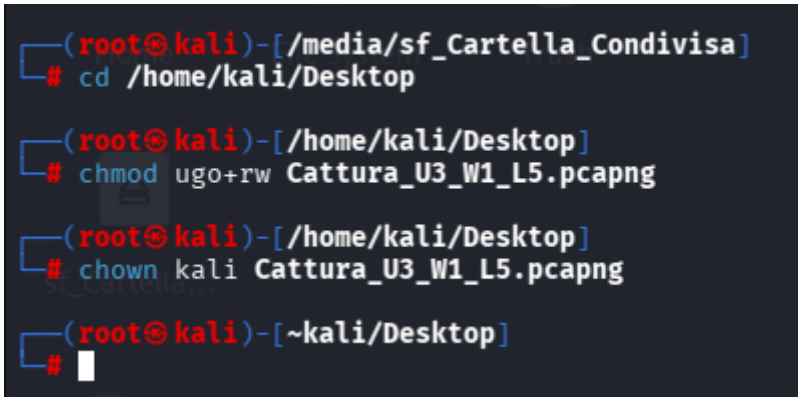

Fig.4 Modifica dei permessi sul file di cattura.

Prima di avviare l'analisi con **Wireshark**, il file è stato trasferito sul desktop di Kali. Successivamente, sono stati configurati i permessi necessari per garantirne l'accesso e l'apertura tramite il suddetto software.

Fase3 – Analisi Wireshark

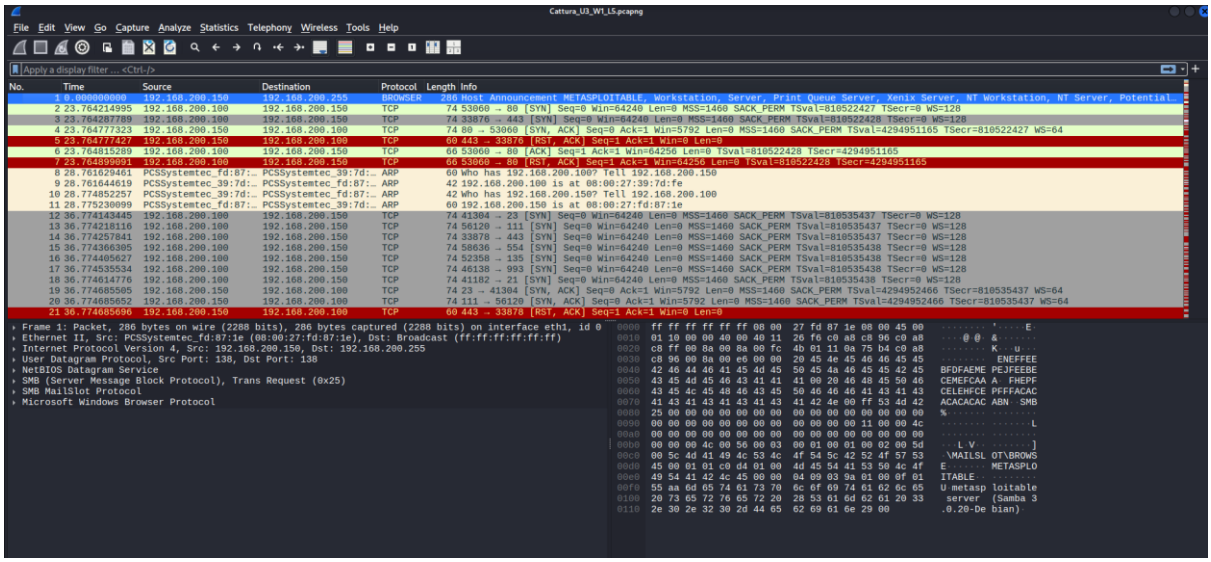

Fig.5 Analisi Wireshark

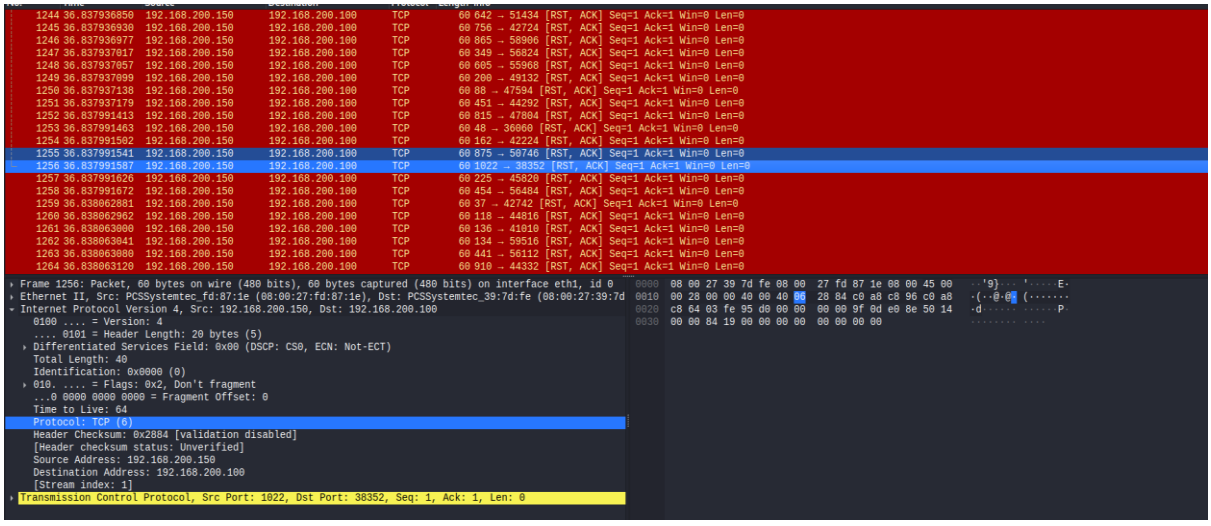

Fig.6 Analisi Wireshark

All'apertura del file su Wireshark, è stata immediatamente riscontrata un'elevata densità di traffico.

Il server **Metasploitable** (**192.168.200.150**) ha inizialmente inviato un messaggio di **broadcast**, rivelando dettagli critici sulla propria versione (**Samba 3.0.20-Debian**), nota per **Samba msfrpc Remote Code Execution** con codice **CVE-2007-2447**.

L'attaccante (**192.168.50.100**) ha risposto a questa informazione eseguendo le seguenti fasi:

1. **ARP Request:** È stata inviata una **richiesta ARP** per risolvere l'indirizzo MAC e confermare l'indirizzo IP della vittima all'interno della rete locale.
2. **SYN Flood:** Una volta identificato il target, l'attaccante ha avviato un **SYN Attack**. Questa tecnica consiste nell'invio di pacchetti SYN verso molteplici porte del server senza finire mai il **Three way Handshake** (tipico segnale di scansione). L'analisi tramite **Wireshark** ha evidenziato inoltre un'elevata densità di pacchetti (**RST, ACK)** inviati dal target in risposta, indicando che le porte interrogate erano **chiuse** o protette.

Conclusione

L'analisi del traffico suggerisce l'esecuzione di un'attività di **footprinting** attraverso un possibile tool come **Nmap.** Tale scansione ha portato all'identificazione dei servizi attivi e alla mappatura delle porte aperte sul server target **Metasploitable** .

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -p- -T5 192.168.200.150
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-06 11:30 -0500
Nmap scan report for 192.168.200.150
Host is up (0.0025s latency).
```

**Fig.7 possibile comando nmap simulato*

Il comando mostrato risulta plausibile con l'analisi perché:

1. **-sS**: effettua una **SYN scan**, il che spiega le connessioni mai completate verso la macchina target.

2. **-p-**: scansiona l'intero **range di porte**, confermando una mappatura completa sulla macchina.
3. **-T5**: determina **l'aggressività** della scansione, confermando una **raffica costante** di richieste rilevata nel traffico.

In conclusione, il documento dimostra come l'utilizzo di **Wireshark** sia indispensabile per trasformare flussi di dati in informazioni su possibili minacce.

Mitigazione

Per ridurre le possibilità di questi attacchi, si consiglia:

1. **Aggiornamento e Patching del Software:** in questo caso aggiornare la versione del server della **metasploitable.**
2. **Configurazione Firewall:** Configurare un **Firewall** o sistemi **IDS/IPS** per rilevare e bloccare automaticamente gli IP che effettuano scansioni rapide su porte multiple.
3. **Implementazione di VLAN:** Implementare delle VLAN per isolare i server critici dal traffico client generale.