Relazione: Estrazione di un Eseguibile da un File PCAP

Introduzione

Questo laboratorio si è concentrato sull'analisi del traffico di rete catturato in un file PCAP (Packet Capture) e sull'estrazione di un file eseguibile scaricato durante quella sessione . L'analisi a livello di pacchetto è fondamentale per comprendere le transazioni di rete, complementando l'analisi dei log. Utilizzeremo la macchina virtuale CyberOps Workstation e lo strumento Wireshark per esaminare un file PCAP preesistente e recuperare un file eseguibile .

Parte 1: Analisi dei Registri Pre-acquisiti e delle Acquisizioni del Traffico

Il file PCAP che analizzeremo è nimda.download.pcap, che contiene i pacchetti relativi al download del (presunto) malware Nimda, catturati in un'attività precedente. Per coerenza, utilizzeremo la copia del file presente nella directory /home/analyst/lab.support.files/pcaps .

Sebbene tcpdump sia uno strumento potente per l'analisi da riga di comando, l'interfaccia grafica di Wireshark semplifica molte operazioni . È importante notare che entrambi gli strumenti utilizzano lo stesso formato di file PCAP, quindi i file creati con uno possono essere aperti con l'altro .

1.1 Apertura del File PCAP in Wireshark

Per prima cosa, abbiamo navigato nella directory contenente il file PCAP e ne abbiamo verificato la presenza :

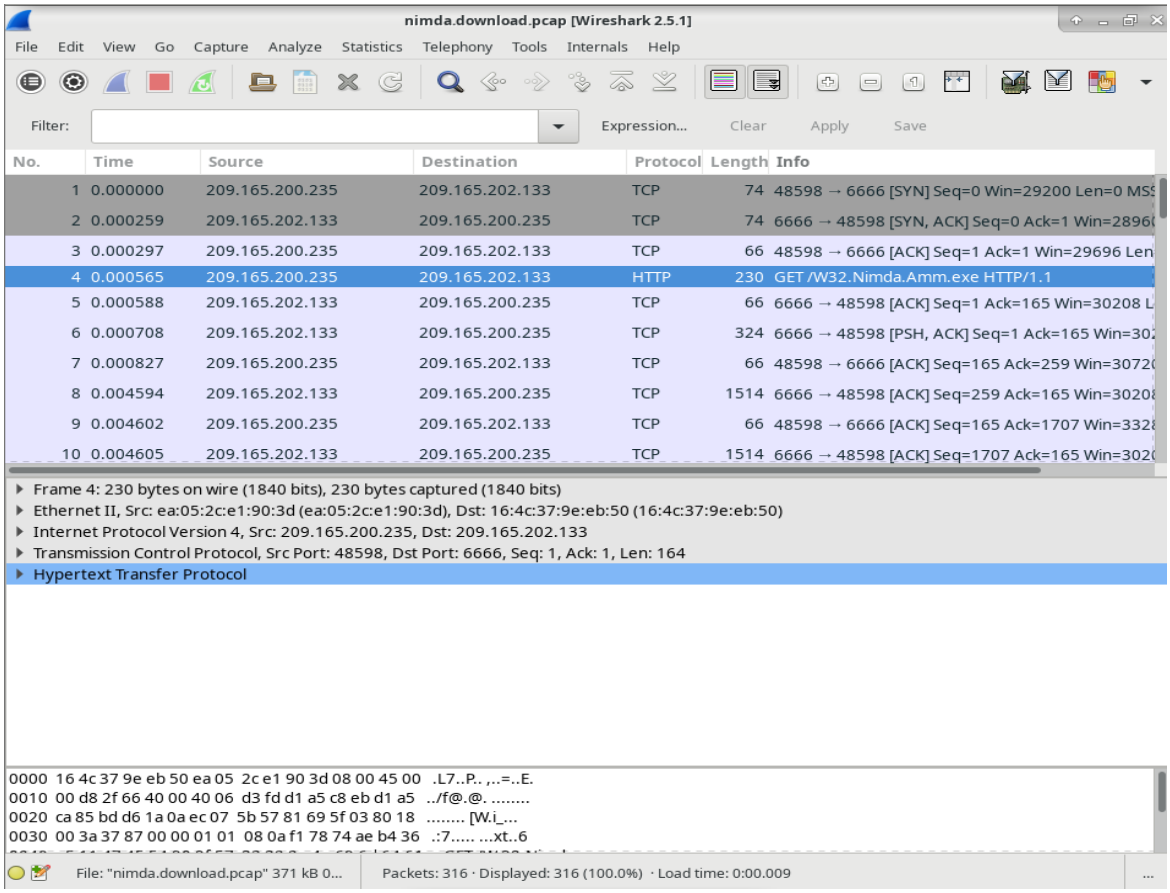
```
[analyst@secOps ~]$ cd lab.support.files/pcaps
[analyst@secOps pcaps]$ ls -l
total 4028
-rw-r--r-- 1 analyst analyst  371462 Mar 21  2018 nimda.download.pcap
-rw-r--r-- 1 analyst analyst 3750153 Mar 21  2018 wannacry_download_pcap.pcap
```

Successivamente, abbiamo aperto il file nimda.download.pcap utilizzando Wireshark con il comando wireshark-gtk nimda.download.pcap &. Il simbolo & permette di eseguire Wireshark in background, mantenendo libero il terminale .

```
[analyst@secOps pcaps]$ wireshark-gtk nimda.download.pcap &
```

1.2 Analisi Iniziale dei Pacchetti

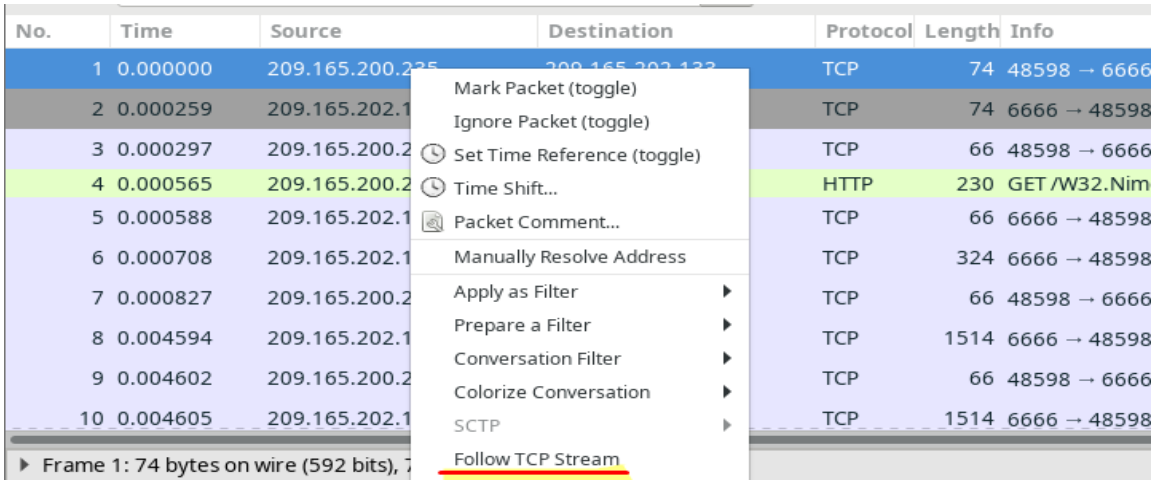
Wireshark mostra i pacchetti catturati in sequenza . Abbiamo selezionato il quarto pacchetto. Questo pacchetto corrisponde alla richiesta HTTP GET per il file eseguibile. Espandendo i dettagli del protocollo HTTP nel pannello inferiore di Wireshark, possiamo osservare le informazioni della richiesta .



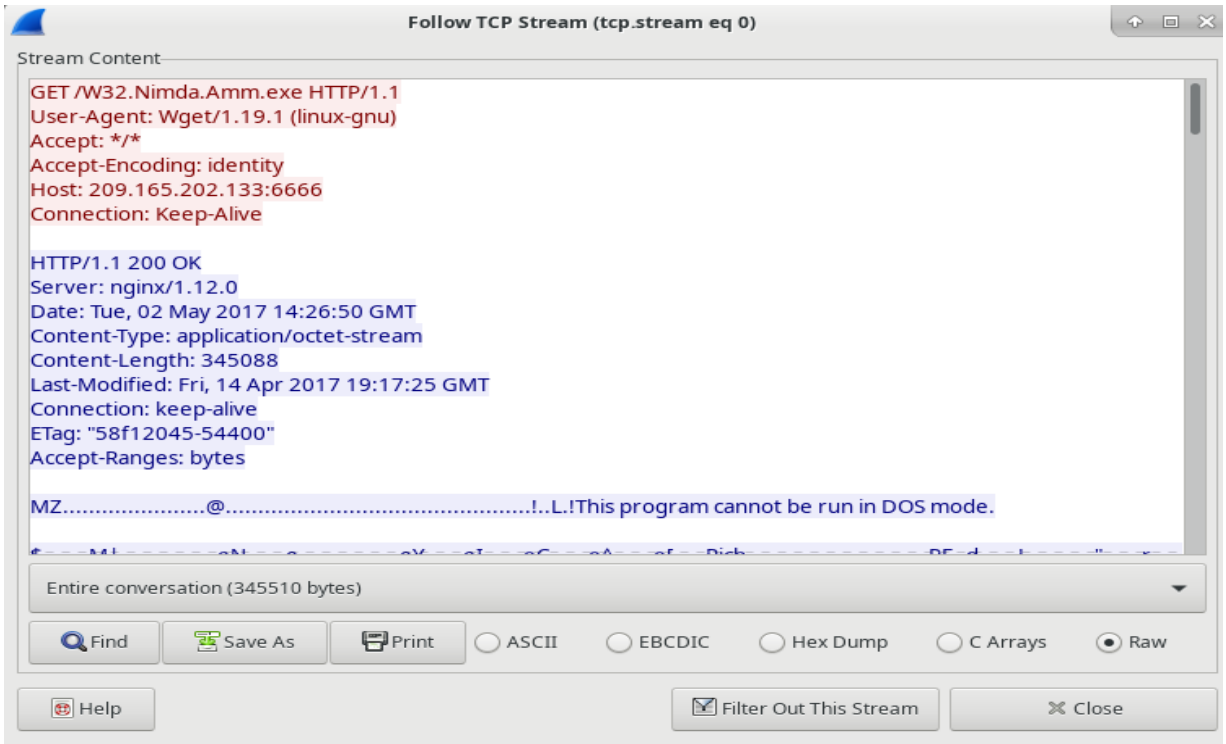
I primi tre pacchetti (non mostrati in dettaglio qui, ma visibili nello screenshot sopra) rappresentano l'handshake TCP a tre vie (SYN, SYN-ACK, ACK) che stabilisce la connessione tra il client (209.165.200.235) e il server (209.165.202.133) sulla porta 6666 . Il quarto pacchetto è la richiesta GET /W32.Nimda.Amm.exe HTTP/1.1 inviata dal client al server.

1.3 Seguire il Flusso TCP

Poiché HTTP opera sopra TCP, possiamo usare la funzione "Segui flusso TCP" di Wireshark per ricostruire l'intera conversazione e visualizzare i dati scambiati . Abbiamo selezionato il primo pacchetto (il pacchetto SYN iniziale), fatto clic con il pulsante destro del mouse e scelto Segui > Flusso TCP .



Wireshark ha aperto una nuova finestra mostrando l'intero contenuto del flusso TCP . La parte iniziale mostra le intestazioni della richiesta HTTP e le intestazioni della risposta HTTP 200 OK del server , seguite dai dati effettivi del file .



La parte inferiore della finestra contiene una serie di simboli e caratteri apparentemente casuali, intervallati da alcune parole leggibili. Questi non sono "rumore", ma la rappresentazione testuale del contenuto binario del file eseguibile

scaricato . Wireshark tenta di interpretare i byte binari come caratteri ASCII, e il risultato è quello visualizzato. Le parole leggibili (come "This program cannot be run in DOS mode.", visibile nello screenshot) sono stringhe di testo effettivamente presenti all'interno del codice eseguibile, spesso utilizzate per messaggi all'utente o altre funzionalità del programma. Un analista esperto può talvolta ricavare informazioni utili da queste stringhe.

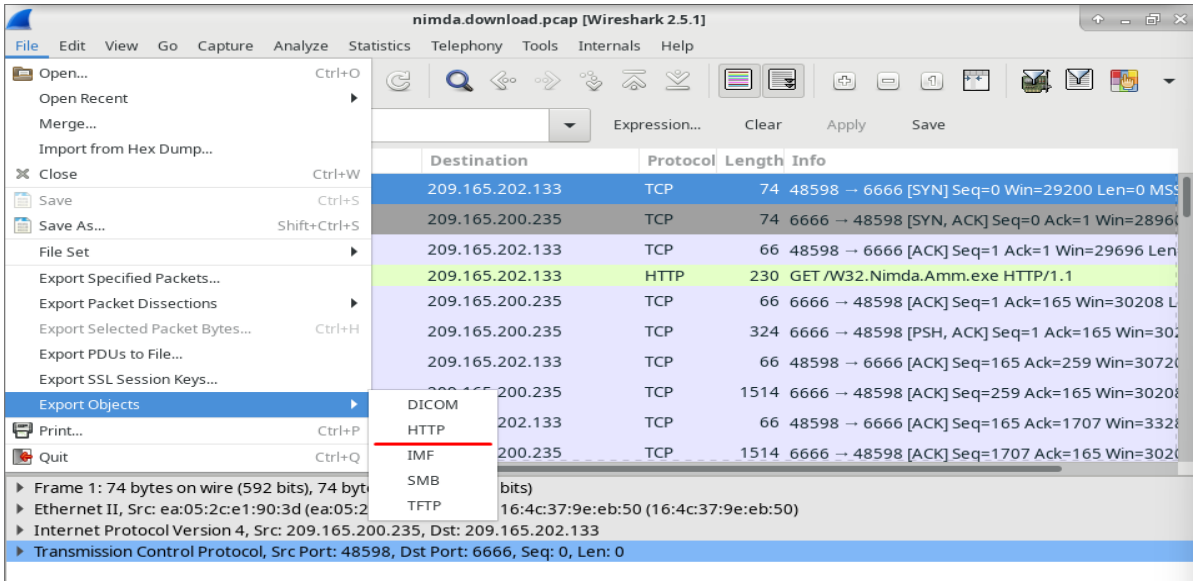
Il laboratorio specifica che, nonostante il nome, il file non è il vero worm Nimda, ma un altro eseguibile rinominato per motivi di sicurezza. Esaminando le stringhe leggibili presenti nel flusso TCP (specialmente scorrendo fino alla fine della finestra, azione non mostrata nello screenshot ma descritta nel testo), si potrebbe identificare il file come cmd.exe di Microsoft Windows

Parte 2: Estrarre i File Scaricati da PCAP

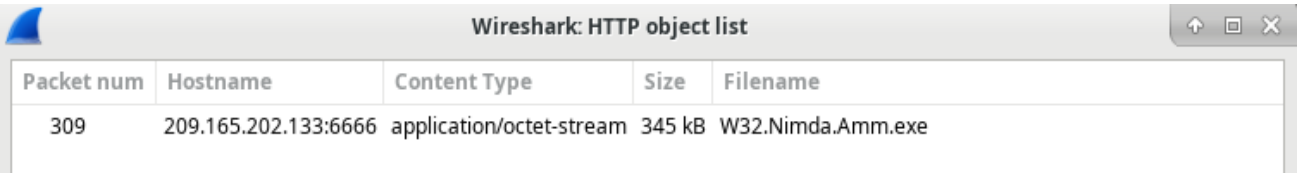
Avendo confermato la presenza del file eseguibile all'interno del flusso TCP catturato, il passo successivo è estrarlo dal file PCAP per poterlo analizzare ulteriormente.

2.1 Esportazione degli Oggetti HTTP

Sappiamo che il download è avvenuto tramite HTTP. Wireshark può identificare ed esportare oggetti trasferiti tramite questo protocollo. Abbiamo selezionato nuovamente il pacchetto 4 (la richiesta HTTP GET) e abbiamo navigato nel menu: File > Esporta Oggetti > HTTP .



Wireshark ha analizzato il PCAP e ha presentato una finestra "Elenco oggetti HTTP" con tutti gli oggetti rilevati nel traffico HTTP . In questo caso specifico, è stato trovato un solo oggetto: il file W32.Nimda.Amm.exe



Questo file è l'unico presente perché la cattura dei pacchetti è stata avviata immediatamente prima del download e fermata subito dopo, senza includere altro traffico HTTP .

2.2 Salvataggio e Verifica del File Estratto

Abbiamo selezionato la riga corrispondente al file W32.Nimda.Amm.exe nella finestra "Elenco oggetti HTTP" e abbiamo cliccato sul pulsante "Salva con nome" . Abbiamo navigato fino alla directory home dell'utente (/home/analyst) e abbiamo salvato il file lì.

Per verificare che il file fosse stato salvato correttamente, siamo tornati alla finestra del terminale, ci siamo spostati nella directory /home/analyst e abbiamo elencato i file con ls -l :

```
[analyst@secOps pcaps]$ cd /home/analyst
[analyst@secOps ~]$ ls -l
total 376
-rw-r--r-- 1 root     root       5764 Apr  9 08:56 capture.pcap
drwxr-xr-x 2 analyst analyst    4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst    4096 Mar 22  2018 Downloads
-rw-r--r-- 1 analyst analyst       9 Apr 14 06:03 file1new.txt
lrwxrwxrwx 1 analyst analyst       9 Apr 14 06:06 file1symbolic -> file1.txt
-rw-r--r-- 2 analyst analyst       5 Apr 14 06:04 file2hard
-rw-r--r-- 2 analyst analyst       5 Apr 14 06:04 file2new.txt
drwxr-xr-x 9 analyst analyst    4096 Jul 19  2018 lab.support.files
drwxr-xr-x 3 root     root       4096 Mar 26  2018 second_drive
-rw-r--r-- 1 analyst analyst  345088 Apr 14 06:39 W32.Nimda.Amm.exe
```

L'elenco conferma la presenza del file W32.Nimda.Amm.exe nella directory home.

2.3 Identificazione del Tipo di File e Passi Successivi

Per ottenere maggiori informazioni sul file estratto, abbiamo utilizzato il comando file :

```
[analyst@secOps ~]$ file W32.Nimda.Amm.exe
W32.Nimda.Amm.exe: PE32+ executable (console) x86-64, for MS Windows
```

L'output conferma che si tratta di un file eseguibile per Windows a 64 bit (formato PE32+) .

A questo punto, un analista di sicurezza procederebbe con l'analisi del malware . Il passo successivo più probabile sarebbe spostare il file W32.Nimda.Amm.exe in un ambiente isolato e controllato (una sandbox), tipicamente una macchina virtuale dedicata . In questo ambiente sicuro, l'eseguibile verrebbe lanciato per osservarne il comportamento: quali risorse utilizza, quali connessioni di rete tenta di stabilire, quali modifiche apporta al sistema operativo, ecc. Esistono strumenti specifici per facilitare questo monitoraggio . In alternativa, o in aggiunta, l'analista potrebbe caricare il file su servizi di analisi online come VirusTotal, che eseguono il file in ambienti controllati e

forniscono un report dettagliato sul suo comportamento e sulla sua classificazione da parte di diversi motori antivirus.

Conclusione

Questo laboratorio ha illustrato con successo il processo di analisi di un file PCAP contenente il download di un file eseguibile tramite HTTP. Utilizzando Wireshark, siamo stati in grado di ispezionare i pacchetti, ricostruire il flusso TCP per visualizzare il contenuto trasferito e, infine, utilizzare la funzione di esportazione degli oggetti HTTP per estrarre il file eseguibile dal traffico di rete catturato. Questo processo è fondamentale per recuperare campioni di malware o altri file di interesse da analisi di rete forensi o da monitoraggio del traffico.