

Introduzione

L'analisi del traffico di rete è una delle attività più critiche e raffinate nell'ambito della cybersecurity. Ogni dato che attraversa una rete digitale viene encapsulato in pacchetti, trasportato attraverso protocolli definiti e registrato in log che possono diventare la chiave per comprendere attacchi, infezioni o attività sospette. In un mondo in cui la sicurezza informatica è costantemente minacciata da malware, **APT (Advanced Persistent Threats)**, data breaches e attacchi mirati, saper leggere, interpretare e ricostruire eventi attraverso un file **PCAP** significa possedere una delle competenze più strategiche nella difesa informatica.

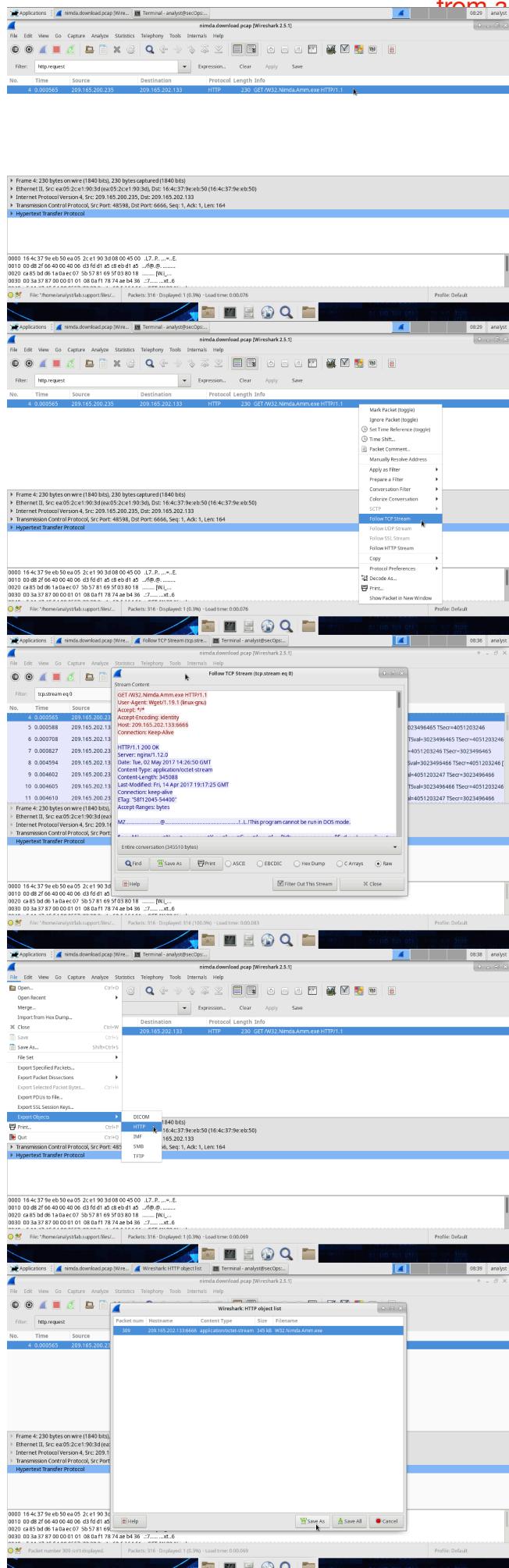
Questo report documenta con precisione ogni passaggio necessario per individuare, estrarre e analizzare un file eseguibile nascosto in un file di cattura di pacchetti di rete. L'indagine è stata condotta in un ambiente Linux isolato, utilizzando Wireshark per l'analisi dettagliata e strumenti di sistema per la verifica e classificazione del file estratto. L'obiettivo non è solo quello di ricostruire il percorso di un potenziale malware, ma anche di riflettere sul significato di tali attività nel contesto più ampio della sicurezza delle informazioni, della threat intelligence e della capacità di risposta a incidenti informatici.

Svolgimento

Dopo l'accesso alla **CyberOps Workstation VM**

il primo passo è stato quello di localizzare il file di cattura di pacchetti da analizzare. L'uso del comando `cd lab.support.files/pcaps` ha permesso di navigare nella directory contenente i file di cattura, mentre `ls -l` ha confermato la presenza del file `nimsa.download.pcap`, il principale oggetto di indagine. La verifica dell'integrità del file ha confermato che la sua dimensione era coerente con una sessione di traffico reale contenente dati significativi.

Per procedere con l'analisi, è stato avviato **Wireshark**, con la possibilità tramite il comando `wireshark nimsa.download.pcap` & da terminale oppure ricercando l'applicazione. Una volta caricato il file, è stato necessario individuare potenziali pacchetti di trasferimento di file, con particolare attenzione al protocollo **HTTP**, spesso utilizzato per la distribuzione di malware. Applicando il filtro `http.request`, è stato possibile isolare le richieste HTTP presenti nel traffico e identificare una richiesta **GET** relativa



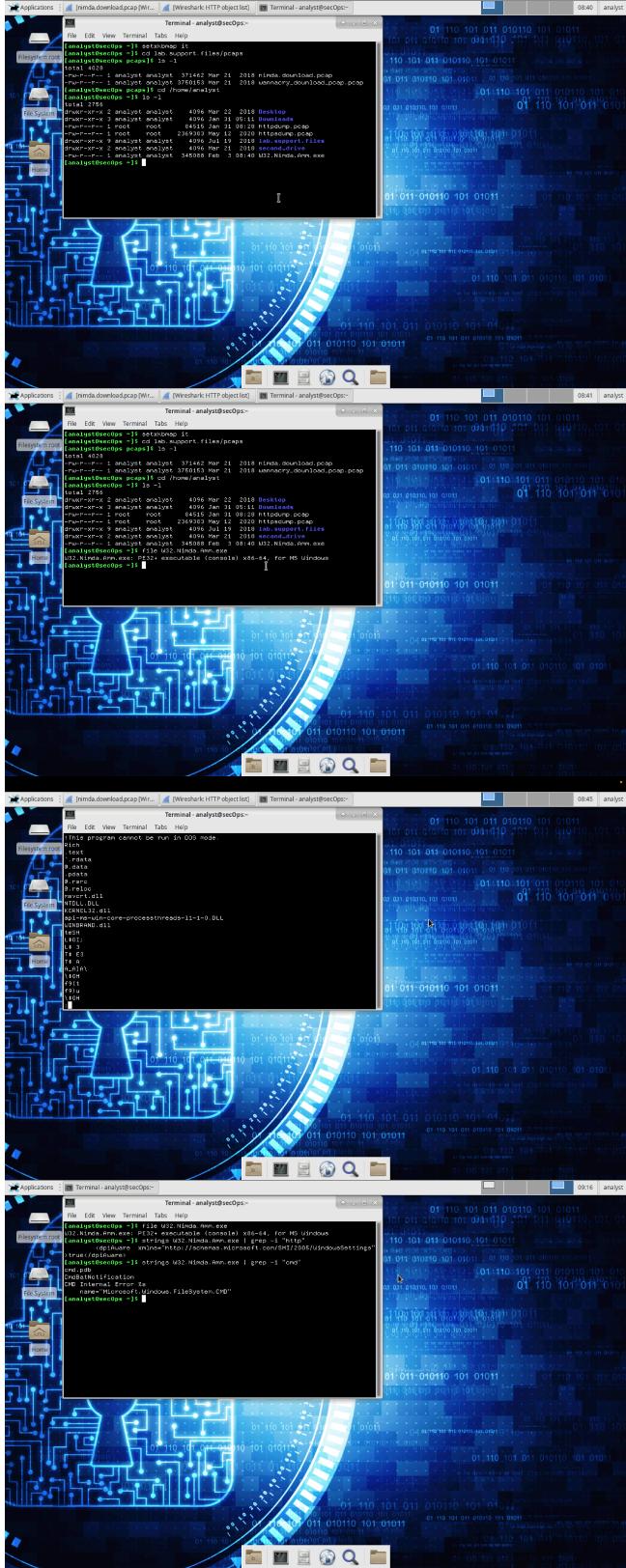
al file *W32.Nimda.Amm.exe*. Questo ha immediatamente sollevato sospetti, poiché il nome stesso del file richiesto suggerisce un possibile collegamento con il noto *worm Nimda*, una delle minacce informatiche più distruttive della sua epoca.

Per ricostruire il contesto completo della richiesta e confermare il trasferimento dell'eseguibile, è stata utilizzata la funzione **Follow TCP Stream** di Wireshark, che ha consentito di visualizzare l'intero flusso di dati tra client e server. Scorrendo all'interno della sessione **TCP**, è stato possibile osservare il contenuto binario del file eseguibile, confermando che il file era stato scaricato come parte della comunicazione registrata.

L'estrazione del file è stata effettuata utilizzando la funzione *Export Objects → HTTP* di Wireshark. Dopo aver individuato *W32.Nimda.Amm.exe* nella lista degli oggetti HTTP catturati, il file è stato salvato nella directory */home/analyst/* e la sua presenza è stata confermata con *ls -l*.

Una volta estratto, l'eseguibile è stato sottoposto a una prima analisi statica per comprenderne la natura. Il comando file *W32.Nimda.Amm.exe* ha rivelato che si trattava di un eseguibile **PE32+ per Windows a 64 bit**, suggerendo immediatamente la necessità di un'analisi più approfondita. L'uso del comando *strings* *W32.Nimda.Amm.exe* ha permesso di estrarre stringhe di testo leggibili dal file binario, rivelando riferimenti a funzioni di sistema Windows come **KERNEL32.DLL** e **NTDLL.DLL**, oltre a possibili comandi **CMD** interni. La presenza della stringa "**Microsoft.Windows.FileSystem.CMD**" ha rafforzato il sospetto che il file eseguibile potesse eseguire comandi malevoli sul sistema.

L'intero processo ha dimostrato in modo pratico e metodico come sia possibile individuare un file eseguibile nascosto nel traffico di rete, estrarlo e condurre una prima analisi per determinare il suo potenziale impatto. Tuttavia, questa è solo la fase iniziale di un'indagine forense più ampia. In un contesto reale, il file eseguibile estratto potrebbe essere caricato su piattaforme di **threat intelligence** come **VirusTotal** per verificare se sia già noto, oppure eseguito in un ambiente **sandbox** controllato per osservarne il comportamento.



Conclusioni

Questa esperienza ha messo in luce quanto sia fondamentale la **network forensics** nella cybersecurity moderna. La capacità di intercettare e analizzare il traffico di rete non è solo un esercizio tecnico, ma una competenza essenziale per la difesa delle infrastrutture informatiche. Un'organizzazione che non monitora il proprio traffico di rete è cieca di fronte agli attacchi, incapace di rilevare infezioni, esfiltrazioni di dati o attività sospette in corso. La cybersecurity non è solo questione di firewall e antivirus, ma di comprensione profonda del comportamento della rete e della capacità di leggere tra le righe del traffico per individuare anomalie che possono fare la differenza tra un sistema sicuro e un'infrastruttura compromessa.

Le conclusioni di questo lavoro non si limitano all'esercitazione tecnica, ma toccano il cuore stesso della sicurezza informatica. Ogni giorno, miliardi di pacchetti attraversano le reti globali, trasportando dati leciti ma anche minacce nascoste. Essere in grado di isolare, analizzare e comprendere questi pacchetti significa avere il potere di prevenire attacchi, di proteggere informazioni critiche e di garantire che le organizzazioni possano operare in un ambiente digitale sicuro. La capacità di risalire a un file malevolo partendo da un semplice file PCAP è la dimostrazione che, nella cybersecurity, ogni dettaglio conta, ogni pacchetto può raccontare una storia e ogni bit di informazione può essere la chiave per fermare una minaccia prima che sia troppo tardi.