Report su Wireshark e il Monitoraggio degli Indicatori di Compromissione

Data 31/01/24

Introduzione

Wireshark è uno strumento di analisi del traffico di rete, ampiamente utilizzato per la cattura e l'analisi dei pacchetti trasmessi attraverso una rete. Questo strumento fornisce una visione dettagliata del traffico di rete, consentendo agli amministratori di rete e agli analisti di sicurezza di identificare anomalie, problemi di performance e, in molti casi, anche attività malevole.

Uno degli aspetti fondamentali dell'utilizzo di Wireshark è la sua capacità di facilitare il monitoraggio passivo degli Indicatori di Compromissione (IOC). Gli IOC sono segnali o pattern di comportamento che possono indicare un potenziale attacco o una violazione della sicurezza.

Gli IOC sono utilizzati principalmente nelle attività di monitoraggio e rilevamento delle minacce per identificare comportamenti anomali o potenzialmente dannosi all'interno di un ambiente IT.

Gli IOC possono assumere diverse forme, e la loro identificazione può essere basata su vari tipi di dati e informazioni. Alcuni esempi comuni di IOC includono:

- Consumo eccessivo della banda di rete o delle schede di rete
- Traffico in entrata da sorgenti piuttosto sospette su porte critiche
- Multiple richieste TCP su ampi intervalli di porte, generalmente evidenza di una scansione in corso
- Numero molto elevato di richieste TCP, UDP provenienti contemporaneamente da diversi indirizzi IP, sintomo di un Ddos in corso
- Indirizzi IP Sospetti: Indirizzi IP noti per essere associati a attività malevole o server di comando e controllo.

Analizzando il traffico di rete con Wireshark, è possibile individuare questi indicatori e rispondere prontamente per prevenire o limitare danni.

Analisi della Scansione Wireshark

Dopo aver aperto e analizzato la scansione Wireshark, è emerso un pattern di comunicazione notevole che indica chiaramente un tentativo di scansione dell'host. La maggior parte dei pacchetti presentava un tipo di protocollo TCP, con il solo flag SYN attivato. Quando l'host riceveva questi pacchetti, rispondeva con il flag RST, ACK senza stabilire una connessione effettiva. Tuttavia, su alcune porte, veniva effettuato con successo il three-way handshake.

Solo su alcune porte viene completato il three-way handshake, indicando che l'attaccante ha individuato delle porte aperte.

Abbiamo notato la limitazione della scansione alle prime 1024 porte, questo suggerisce che l'attaccante potrebbe aver eseguito una scansione di tipo "Nmap", la quale di default scansiona le cosiddette "well-known ports" (porte ben conosciute) nella gamma 1-1024.

Metodologia di Identificazione delle Porte Aperte

Per individuare le porte che hanno stabilito una connessione, abbiamo impiegato una metodologia dettagliata utilizzando la sezione Statistiche di Wireshark e successivamente la visualizzazione delle Conversazioni. Il processo è stato il seguente:

Sezione Statistiche

Inizialmente, ci siamo diretti alla sezione Statistiche di Wireshark per ottenere una panoramica dettagliata del traffico catturato. Questa sezione fornisce informazioni chiave sulla distribuzione del traffico, inclusi i protocolli utilizzati e le porte coinvolte nelle connessioni.

Visualizzazione Conversazioni:

Successivamente, ci siamo concentrati sulla sezione Conversazioni, che consente di analizzare le connessioni tra indirizzi IP e porte. Abbiamo applicato un filtro per visualizzare solo i pacchetti di tipo TCP, concentrando l'analisi sul traffico di questo protocollo.

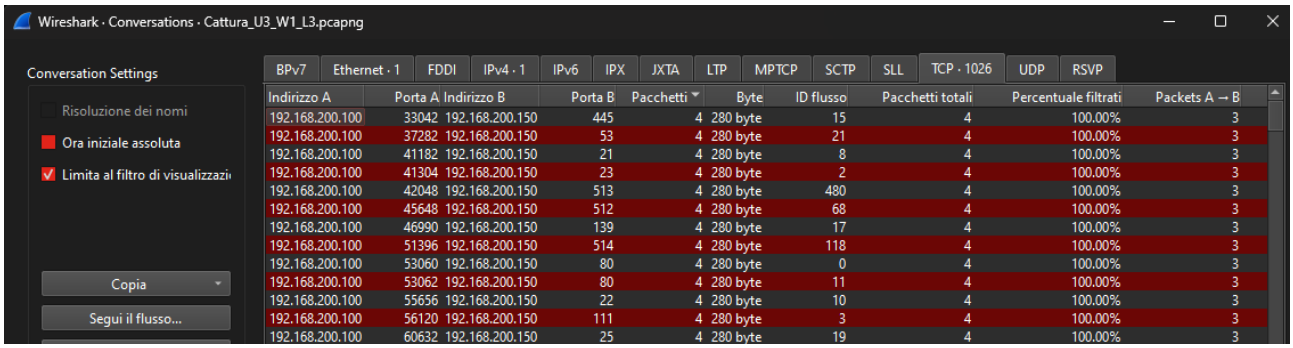
Ordinamento dei Pacchetti:

Abbiamo applicato un filtro specifico per i pacchetti TCP e successivamente li abbiamo ordinati in base al numero di pacchetti per ciascuna connessione, dal maggiore al minore. Questo ci ha permesso di identificare rapidamente le connessioni con un numero di pacchetti diverso dal solito.

Analisi delle Connessioni TCP:

Abbiamo osservato che la maggior parte delle connessioni TCP presentava solo due pacchetti, suggerendo che molte porte potrebbero essere chiuse. Tuttavia, abbiamo notato un pattern diverso per le porte aperte, dove il numero totale di pacchetti era di 4 per ciascuna connessione.

Questo approccio analitico ci ha permesso di distinguere chiaramente le porte aperte, evidenziando il fatto che le connessioni su tali porte comportavano un numero di pacchetti differente rispetto alle porte chiuse.



Analisi delle Porte Aperte

Durante l'analisi del traffico Wireshark, sono state identificate diverse porte che hanno stabilito connessioni, indicando la loro apertura. Di seguito sono elencate le porte aperte e i servizi associati:

Porta 21 (FTP):

Servizio: File Transfer Protocol (FTP)

Porta 22 (SSH):

Servizio: Secure Shell (SSH)

Porta 23 (Telnet):

Servizio: Telnet (gestione remota di sistemi)

Porta 25 (SMTP):

Servizio: Simple Mail Transfer Protocol (SMTP)

Porta 53 (DNS):

Servizio: Domain Name System (DNS)

Porta 80 (HTTP):

Servizio: Hypertext Transfer Protocol (HTTP)

Porta 111 (RPC):

Servizio: Remote Procedure Call (RPC)

Porta 139 (NetBIOS):

Servizio: NetBIOS (comunicazione su reti locali)

Porta 445 (SMB):

Servizio: Server Message Block (SMB) - utilizzato per la condivisione di file e stampanti

Porte 512, 513 e 514 (rexec, rlogin, rsh):

Servizi: Rexec, Rlogin, Rsh (Remote Execution Services)

Queste porte aperte rappresentano potenziali punti di accesso e devono essere attentamente valutate per garantire la sicurezza del sistema. L'identificazione precisa dei servizi in ascolto su queste porte fornisce una base essenziale per l'implementazione di misure di sicurezza mirate.

Mitigazione degli Impatti dell'Attacco: Raccomandazioni e Azioni Consigliate

Alla luce delle vulnerabilità identificate durante l'analisi della scansione Wireshark, è imperativo implementare azioni correttive mirate per ridurre gli impatti potenziali dell'attacco e migliorare la sicurezza complessiva del sistema. Di seguito sono fornite raccomandazioni e azioni consigliate:

Filtraggio del Traffico Ingressante:

Implementare filtri di traffico come un Firewall per consentire solo il traffico essenziale e bloccare pacchetti sospetti o non autorizzati. Questo può essere realizzato attraverso la configurazione di regole di firewall per limitare l'accesso a porte non necessarie.

Monitoraggio Continuo:

Implementare sistemi di monitoraggio continuo del traffico di rete e dei log di sicurezza. L'analisi costante dei pattern di comportamento anomalo può consentire una risposta tempestiva agli attacchi in corso.

Implementazione di Firme IDS/IPS:

Utilizzare sistemi di rilevamento delle intrusioni (IDS) o sistemi di prevenzione delle intrusioni (IPS) con firme aggiornate per rilevare e prevenire attività malevole.