Manuel Di Gangi

S9_L3

Threat Intelligence & IOC

20 marzo 2024

INDICE

Traccia

Durante la lezione teorica, abbiamo visto la Threat Intelligence e gli indicatori di compromissione. Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto. Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark.

Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco

1. Nozioni Teoriche

Wireshark è uno dei software più noti e potenti per l'analisi del traffico di rete. È un programma open-source utilizzato per catturare e analizzare i pacchetti di dati che passano attraverso una rete. Questo strumento è estremamente utile per gli amministratori di rete, gli ingegneri di sicurezza informatica e gli sviluppatori di software che hanno bisogno di comprendere e risolvere problemi di rete, analizzare il traffico di rete per motivi di sicurezza o sviluppare e testare applicazioni di rete.

Le caratteristiche principali di Wireshark includono:

- Cattura dei pacchetti: Wireshark è in grado di catturare e registrare i pacchetti di dati che transitano attraverso una rete.
- Analisi dettagliata dei pacchetti: consente agli utenti di analizzare dettagliatamente ciascun pacchetto.
- Filtri avanzati: offre potenti funzionalità di filtraggio che consentono agli utenti di concentrarsi solo sui pacchetti di interesse.
- Visualizzazione grafica: fornisce una varietà di visualizzazioni grafiche per aiutare gli utenti a interpretare i dati di traffico di rete in modo più intuitivo.

Gli IOCs (Indicatori di Compromissione) sono segnali o tracce che possono indicare la presenza di una possibile violazione della sicurezza informatica o di un'attività dannosa all'interno di un sistema o di una rete. Questi indicatori possono includere indizi come indirizzi IP sospetti, nomi di file malware, firme di virus, modelli di comportamento anomalo, attività di rete insolita e altro ancora. Gli IOCs sono utilizzati dagli esperti di sicurezza informatica per identificare, analizzare e rispondere a minacce alla sicurezza, permettendo loro di proteggere proattivamente i sistemi e le reti dalle attività dannose.

2. Analisi del traffico

Analizzando il traffico catturato notiamo subito la presenza di soli due host: 192.168.200.100 e 192.168.200.150

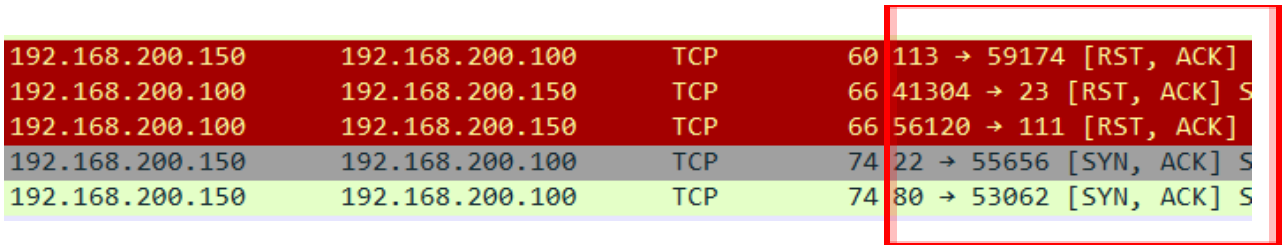
192.168.200.100	192.168.200.150
192.168.200.100	192.168.200.150
192.168.200.150	192.168.200.100
192.168.200.150	192.168.200.100

Proseguendo osserviamo una grande mole di richieste SYN dall'host 192.168.200.100 verso l'altro. L'aspetto particolare è che queste richieste vengono effettuate ogni volta su una porta differente, questo ci fa capire non si tratta di un normale tentativo di connessione, bensì è altamente probabile che questo host stia effettuando una scansione alla ricerca di vulnerabilità, servizi in ascolto o porte aperte da exploitare.

192.168.200.100	192.168.200.150	TCP	74 41304 → 23 [SYN] S
192.168.200.100	192.168.200.150	TCP	74 56120 → 111 [SYN]
192.168.200.100	192.168.200.150	TCP	74 33878 → 443 [SYN]
192.168.200.100	192.168.200.150	TCP	74 58636 → 554 [SYN]
192.168.200.100	192.168.200.150	TCP	74 52358 → 135 [SYN]
192.168.200.100	192.168.200.150	TCP	74 46138 → 993 [SYN]
192.168.200.100	192.168.200.150	TCP	74 41182 → 21 [SYN] S
192.168.200.150	192.168.200.100	TCP	74 23 → 41304 [SYN, A
192.168.200.150	192.168.200.100	TCP	74 111 → 56120 [SYN,

L'host 192.168.200.150 d'altro canto risponde alle richieste con una risposta di tipo:

- [RST, ACK] se la porta è chiusa;
- [SYN, ACK] se la port è apert;



192.168.200.150	192.168.200.100	TCP	60	113 → 59174 [RST, ACK]
192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [RST, ACK] S
192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [RST, ACK]
192.168.200.150	192.168.200.100	TCP	74	22 → 55656 [SYN, ACK] S
192.168.200.150	192.168.200.100	TCP	74	80 → 53062 [SYN, ACK] S

3. Azioni preventive

Per difendersi efficacemente da una scansione delle porte all'interno di una rete informatica, è fondamentale adottare misure preventive solide per proteggere l'integrità e la sicurezza della rete stessa.

Ecco alcune azioni preventive specifiche:

- **Segmentazione della rete**: Dividere la rete in segmenti per limitare il traffico tra i diversi segmenti. In questo modo, anche se un dispositivo all'interno della rete viene compromesso, la sua capacità di esplorare o danneggiare altri segmenti sarà limitata.
- **Monitoraggio del traffico interno**: Utilizzare strumenti di monitoraggio del traffico di rete per rilevare e analizzare le attività sospette o non autorizzate, comprese le scansioni delle porte. Come nel caso analizzato sopra il monitoraggio del traffico interno può aiutare a identificare rapidamente eventuali comportamenti anomali e a rispondere tempestivamente.
- **Implementazione di regole di sicurezza**: Configurare regole di sicurezza rigorose sui dispositivi di rete, come router, switch e **firewall**, per limitare l'accesso solo alle porte e ai servizi necessari. Utilizza ACL (Access Control Lists) e altre tecniche di filtraggio per consentire solo il traffico autorizzato.

- **Politiche di autenticazione forte**: Implementare politiche di autenticazione forte, ad esempio l'autenticazione a due fattori, per proteggere l'accesso ai dispositivi di rete e alle risorse sensibili.
- **Aggiornamenti regolari**: Assicurarsi che tutti i dispositivi di rete e il firmware siano aggiornati con le patch di sicurezza più recenti per correggere vulnerabilità note che potrebbero essere sfruttate durante una scansione delle porte o altri attacchi.

4. Conclusioni

Nel nostro caso, dopo aver rilevato un tale comportamento anomalo da parte di un host, sarebbe ideale installare un firewall sulla macchina scansionata (o installare un firewall esterno a difesa di questa) ed applicare una regola che blocca i tentativi di connessione dall'indirizzo 192.168.200.100.