Threat Intelligence & IOC

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**

Riferimenti teorici

Threat Intelligence

Come fanno i professionisti della security a conoscere e capire a fondo le minacce che possono impattare un asset di una compagnia? La risposta è la «**Threat Intelligence**» (TI)
La Threat Intelligence include le attività di raccolta di informazioni che provengono da fonti di diverso tipo in merito alle potenziali minacce che potrebbero impattare un sistema o una compagnia. I dati di potenziali nemici, le loro motivazioni, metodologie e strumenti a disposizione sono tutte informazioni fondamentali per capire da chi e come difendersi.

Come la TI supporta le Security Operations
La Threat intelligence (TI) è una forma particolare di information gathering. La TI si basa sull'analisi dei segnali, dei dati e delle evidenze raccolte per costruire un modello/una strategia di prevenzione e difesa da minacce esterna quanto più efficiente possibile. La TI, può essere categorizzata come segue:
Strategic intelligence: che ha come obiettivo primario quello di fornire informazioni sulle minacce e sui potenziali attori delle minacce per fornire alle compagnie una vista complessiva su come e da chi difendersi.
Tactical intelligence: che include dettagli tecnici e comportamentali da condividere con gli esperti di security per mettere in atto le azioni di risposta.
Operational intelligence: che include specificatamente i dettagli per prevenire e rispondere alla singola minaccia. Include anche dettagli precisi sugli attori della minaccia, la sua provenienza ed i potenziali vettori d'attacco.

Ci sono differenti sorgenti di informazioni dalle quali la TI può attingere e recuperare informazioni, come le sorgenti pubbliche o fonti a pagamento. Le prime vengono anche dette «open source intelligence», mentre le seconde vengono anche chiamate «closed source intelligence, oppure proprietary intelligence». Indipendentemente dalla sorgente, le informazioni sulle minacce, dette anche «**feed**» hanno lo scopo principale di fornire dettagli aggiornati alle compagnie circa le ultime minacce sul panorama nazionale / internazionale.

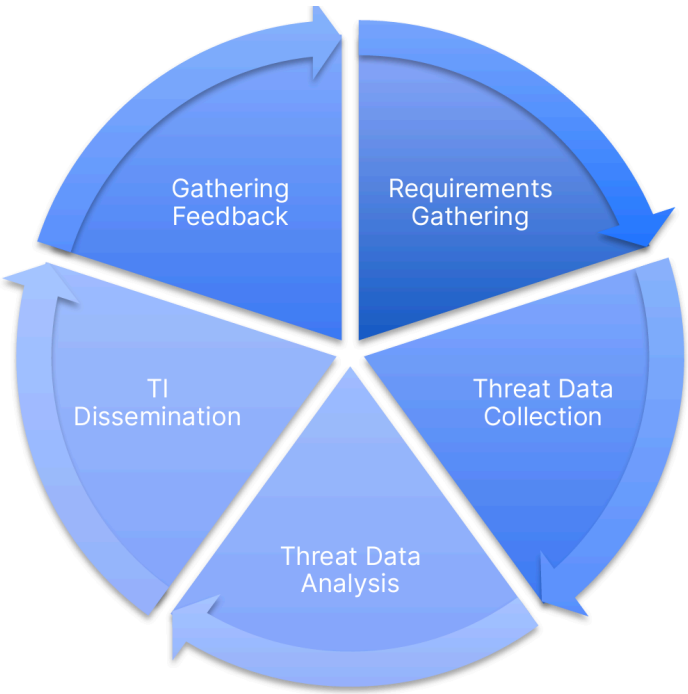
Generalmente, i «feed» includono informazioni come indirizzi IP, hostname, domini, indirizzi email, URLs e altri dettagli circa le potenziali minacce.
Tra le fonti di «feed» open source troviamo siti quali: Alienvault; Virus Total; Cisco Talos Intelligence; Senki; Virus Share.
La TI closed source include tutte quelle informazioni che si reperiscono tramite tool di terze parti. In questo caso è il vendor del tool o della piattaforma che provvede alla ricerca delle informazioni e le elabora prima di metterle a disposizione delle compagnie. Tra le ragioni per le quali molte compagnie scelgono la via della closed source TI c'è la volontà di mantenere private le informazioni raccolte da eventuali «nemici».

Per la valutazione delle informazioni si utilizzano alcuni fattori comuni, come:

- La tempestività: si valuta se l'informazione è attuale oppure datata. Nel secondo caso, l'informazione risulta non essere più rilevante.
- L'esattezza: si valuta se l'informazione è accurata, ovvero possiamo fidarci dell'informazione?
- La rilevanza: si valuta se l'informazione è rilevante per gli asset della compagnia. Se l'informazione descrive piattaforme, software diversi da quelli adottati dalla compagnia, allora risulta non essere rilevante.

Un modo per riassumere la valutazione delle informazioni è tramite il «**confidence factor**», ovvero il fattore di fiducia, che molte delle volte è espresso quantitativamente da un numero/intervallo di numeri e da un livello. Più alto il confidence factor, più sarà affidabile l'informazione. Tuttavia, non bisogna scartare a prescindere le info con un confidence factor basso, in quanto potrebbero essere informazioni in uno stato iniziale ancora da confermare.
ThreatConnect utilizza un sistema di valutazione delle informazioni basato su sei livelli:
Confermata (90-100): l'informazione risulta confermata da diverse sorgenti e la minaccia risulta reale dopo la valutazione.
Probabile (70-89): la minaccia non è stata ancora confermata, ma molti dei segnali indicano una probabilità alta che essa sia reale.
Possibile (50-69): alcune delle informazioni indicano un grado di veridicità concreto, ma non ci sono ancora evidenze per confermare la minaccia.
Incerta (30-49): la valutazione dell'informazione è possibile, ma sono necessarie più informazioni per identificare la minaccia.
Improbabile (2-29): la valutazione dell'informazione è possibile, ma non è la scelta più logica, data la presenza di informazioni discordanti.
Screditata (1): la valutazione ha confermato che la minaccia non è reale.

È richiesta una buona fase iniziale di pianificazione. Sempre più organizzazioni, utilizzano il «**Threat Intelligence life cycle**», ovvero il ciclo di vita della TI:



Requirements gathering: La prima fase del ciclo di vita della TI è la pianificazione dei requisiti. Essi possono essere creati in base allo storico degli attacchi subiti, alle minacce più probabili che impattano il mercato di appartenenza della compagnia o come risultato di un «risk assessment» precedentemente effettuato.
Threat data collection: Una volta che sono stati identificati i requisiti, si può iniziare la fase di raccolta dei «feed» dalle sorgenti di TI. Si ricorda che solo le info che sono in linea con i requisiti definiti sono da considerare rilevanti. Questa fase può essere anche ripetuta all'interno del ciclo di vita della TI, qualora si dovesse aggiungere un ulteriore requisito oppure si dovesse modificare uno degli esistenti.
Threat data analysis: Una volta recuperati i dati su eventuali minacce, esse devono essere processate dai tool e dai software disponibili. Alcune delle informazioni potrebbero già essere in un formato «leggibile» dai tool presenti, mentre altre potrebbero necessitare di modifiche alla formattazione. In questa fase ricadono tutte quelle attività che consentono alle informazioni di essere «consumate» dai tool disponibili, e analizzate automaticamente per creare report sulle minacce attuali per consulto da parte della dirigenza.
TI dissemination: Nella fase di TI dissemination, ovvero «diffusione delle informazioni», i dati appena lavorati ed i report appena costruiti dai tool automatici vengono condivisi alla dirigenza ed al personale operativo (responsabili delle security operations) che utilizzeranno il report per eventuali decisioni strategico-operative (ad esempio, come gestire eventuali minacce, quali misure preventive adottare).
Gathering feedback: L'ultima fase del ciclo di vita della TI è la fase di raccolta dei feedback circa i report creati. Il continuo miglioramento infatti è un elemento critico per l'intero processo e deve essere di conseguenza utilizzato per affinare le ricerche, limando e dettagliando i requisiti che verranno successivamente utilizzati per un «nuovo ciclo» al fine di migliorare l'output generale del programma di Threat intelligence.

Quando un'organizzazione decide di iniziare un programma di «**Threat assessment**», ovvero valutazione delle minacce, deve trovare un modo standard per descriverle. Generalmente le compagnie utilizzano due fattori:

- Gli attori delle minacce (threat actors) -> Nazioni o Stati; Crimine organizzato; Attivisti; Attori interni/impiegati.

- La classificazione delle minacce (threat classification) -> Uno dei modelli più utilizzati è il modello «**STRIDE**» di Microsoft per la **classificazione delle minacce**, dove ogni lettera rappresenta una categoria:

Spoofing of user identity, ovvero l'azione di impersonificare in maniera non autorizzata un utente valido di un sistema.
Tampering, ovvero l'azione non autorizzata di alterare un sistema causando danni ad esso o ad un suo componente.
Repudiation, che include tutte le minacce associate agli utenti che negano di eseguire un'azione senza che altre parti abbiano modo di provare il contrario, ad esempio, un utente esegue un'operazione illegale in un sistema che non ha la capacità di tracciare le operazioni vietate (tramite log per esempio).
Information disclosure, che si riferisce alla divulgazione di informazioni che implicano l'esposizione di dati e informazioni sensibili a persone che non dovrebbero avervi accesso, ad esempio la capacità degli utenti di leggere un file a cui non è stato concesso l'accesso.
Denial of Service, include tutte le minacce che volutamente causano indisponibilità di sistemi o servizi.
Elevation of privilege, che include tutte le minacce in cui un utente senza privilegi ottiene un accesso privilegiato ad un sistema così disponendo di privilegi sufficienti per distruggere o alterare/modificare l'intero sistema.

Le compagnie che vogliono capire a fondo la minaccia che potenzialmente potrebbero subire, possono inserire all'interno del loro piano annuale di sicurezza quello che viene chiamato «**threat modeling**», dove vengono presi in esame diversi fattori al fine di capire i veri rischi per l'organizzazione.
Il threat modeling prende in esame:

- La valutazione delle skills dei threat actors, le risorse che hanno a disposizione, l'intento e la loro motivazione.
- La totalità degli asset esposti a potenziali minacce esterne, come dispositivi network, applicazioni, ed altri target che potrebbero essere oggetto delle minacce.
- Lista dei potenziali vettori di attacco, ovvero il mezzo tramite il quale un potenziale attaccante potrebbe ottenere accesso ad un target.
- L'impatto dell'attacco nel caso andasse a segno.
- La probabilità che l'attacco vada a segno.

Ai fattori appena visti viene associato uno «**score**» per **quantificare il rischio** al quale una compagnia è esposta.

Indicatori di compromissione (IOC)

Cosa succede se un attacco va a buon fine? Le compagnie generalmente rispondono con un piano che viene appunto chiamato «piano di risposta agli incidenti», o «**incident response plan**».

Gli indicatori di compromissione (IOC) sono utilizzati dai responsabili delle security operations e sono degli indicatori, ovvero dei segnali/delle evidenze degli attacchi per

ricostruire uno storico e capire cosa è successo. Quindi comprendono lo studio di quei segnali che ci fanno capire che un evento potenzialmente dannoso si sta verificando o si è verificato su un sistema.
Vedremo i metodi utilizzati per identificare gli indicatori di compromissione che impattano:

- Le reti
- Gli end-point (e sistemi operativi)
- Le applicazioni e i servizi

Analisi degli eventi Network:
La maggior parte degli incidenti di sicurezza vengono identificati grazie all'**analisi del traffico di rete** che mostra flussi inaspettati o comunque sospetti. I responsabili delle security operations devono essere abili a capire i segnali e ad analizzarli per far fronte all'incidente e ridurre gli impatti dove possibile.
Ci sono principalmente tre metodi piuttosto comuni per ottenere visibilità sulla rete e sul traffico che sono:

- Router-based monitoring
- Active monitoring
- Passive monitoring

Router-based monitoring
È l'attività del monitoraggio delle rete basato sul traffico gestito dai router, in quanto essi processano tutto il traffico della rete e ne tengono spesso traccia nelle loro tabelle interne. Esistono diverse tecnologie per catturare il traffico di rete gestito dai router come:
-NetFlow: recuperano le informazioni sui flussi di rete gestiti dai router e inviano le informazioni centralmente ad un «flow collector» per successiva analisi.
-RMON (remote networking monitor): sviluppato inizialmente per monitorare il traffico sulle LAN, opera generalmente in architettura client-server ed utilizza delle «sonde» per recuperare informazioni dai dispositivi.
-SNMP (simple network management protocol): è un protocollo di management per le reti di calcolatori che è comunemente utilizzato per recuperare informazioni dai router e dagli altri dispositivi di rete. SNMP fornisce, tuttavia, più informazioni sul dispositivo che sul traffico gestito rispetto a quanto fanno invece RMON e NetFlow.

Active monitoring
Il monitoraggio attivo non avviene in modo centralizzato come per il router-based, ma piuttosto viene effettuato direttamente sui dispositivi al fine di recuperare i dati. Tale strategia potrebbe essere vincente per piccole compagnie, con numero di server/host limitato. Due esempi di monitoraggio attivo sono:

- **Ping**: informazioni a livello network possono essere acquisite attivamente utilizzando l'utility ping, come informazioni circa lo stato di una connessione, le rotte, la latenza, la banda ed il numero di pacchetti in ritardo o persi.
- **iPerf**: un tool che permette di misurare diversi fattori riguardanti la rete come ad esempio la massima larghezza di banda di una rete e la latenza. Il tool è comunemente utilizzato per valutare l'efficienza della rete.

Passive monitoring
Il monitoraggio passivo è un metodo per catturare informazioni circa i flussi di rete che passano un **determinato link**, come ad esempio una connessione cablata tra due macchine. Quindi mentre il monitoraggio attivo viene effettuato direttamente sul dispositivo, il monitoraggio passivo viene effettuato sul link.

Tra le tecniche di recupero flussi di rete ci sono infine i «**network monitoring tools**», ovvero i software utilizzati per lo sniffing delle comunicazioni su una rete come ad esempio **Wireshark.** Tra gli **indicatori di compromissione** che possono essere identificati con i tool appena visti al livello network troviamo:

- **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

Analisi degli eventi sugli host:
Così come per le reti, anche per gli host possiamo identificare una serie di tool e tecniche note per supportare le analisi delle evidenze di attacchi in corso o già accaduti.
Tra le tecniche più comuni troviamo:

- Il monitoraggio continuo delle risorse di sistema: una tecnica molto basilare è il controllo delle risorse di un sistema per identificare eventuali attacchi esterni a fronte di un incremento ingiustificato dell'utilizzo computazionale.
- Monitoraggio dei processi: Alcuni attacchi avanzati riescono a «nascondersi» nel sistema operativo mostrandosi come dei processi leciti, il che rende praticamente impossibile la loro identificazione. Il monitoraggio dei processi ha il compito di monitorare il comportamento e le risorse utilizzate da ogni processo attivo al fine identificare eventuali anomalie.

Analisi degli eventi applicativi o dei servizi:
Un prerequisito per l'analisi degli eventi su applicazioni e servizi è conoscere esattamente il loro scopo, qual è il loro comportamento atteso e le risorse che servono per il loro funzionamento. Tra la tecniche che permettono di identificare IOC su applicazioni e servizi troviamo:

- Log applicativi: i log applicativi forniscono informazioni critiche su eventi che si verificano sull'applicativo, includendo informazioni di dettaglio sull'evento come data e ora in cui l'evento si è verificato, se è coinvolto un utente e così via.
- L'analisi comportamentale: identifica se un applicativo inizia a «funzionare» diversamente da quanto dovrebbe. Ad esempio, pensate ad un attacco di tipo SQLi dove un'applicazione inizia a restituire nome utente e password degli utenti.

PROCEDIMENTO

Su UTM non è possibile creare una **cartella condivisa** tra il mio host e la macchina Kali. Dopo aver analizzato una cattura del traffico di rete effettuata con Wireshark dalla macchina Kali Linux, si procede nella ricerca di Indicatori di compromissione.

Identificare eventuali IOC (evidenze di attacchi in corso)

Indirizzo IP sospetto: 192.168.200.100
Macchina vittima: 192.168.200.150
Porte coinvolte: 1-1024

Notiamo numerose richieste SYN con protocollo TCP su porte diverse. Questo fa pensare ad una probabile scansione da parte dell'attaccante sul client con IP 192.168.200.150.
Osservando la cattura di Wireshark si è riscontrato quindi un numero di richieste TCP molto elevate, inviate dall'host sorgente (192.168.200.150), all'host di destinazione (192.168.200.150). **L'invio di multiple richieste TCP su ampi intervalli di porte è un Indicatore di compromissione, che evidenzia un attacco in corso.**
Le richieste TCP (Transmission Control Protocol) sono richieste di comunicazione inviate attraverso il protocollo TCP, che è uno dei principali protocolli di trasporto utilizzati nella suite di protocolli di Internet (TCP/IP). TCP offre una comunicazione affidabile e orientata alla connessione tra due dispositivi su una rete, il che vuol dire che prima di effettuare la connessione, invia pacchetti con il flag SYN per instaurare un canale comunicativo affidabile. Infatti, le richieste TCP sono spesso associate a connessioni in cui una parte, chiamata client, richiede o invia dati a un'altra parte, chiamata server.

Per analizzare le richieste TCP inviate, si è cliccato sul tab **Statistiche**, selezionando **Conversazioni**. Con il tab "**TCP-1206**" notiamo che l'host di destinazione ha inviato 1026 richieste TCP. Cliccando poi su "**Porta B**", notiamo che le richieste sono state effettuate su un ampio intervallo di porte dell'host di destinazione, il cui IP era identificabile nella colonna "Indirizzo B": 192.168.200.150. Il range di porte va dalla 1 alla 1024.

In base agli IOC trovati, ipotizza i potenziali vettori di attacco utilizzati

Scanning per la ricerca di vulnerabilità: L'attaccante potrebbe eseguire il port scanning per individuare porte aperte e identificare vulnerabilità potenziali nei servizi in esecuzione su tali porte.
Preparazione per un attacco futuro: Il port scanning può essere un passo preliminare per preparare un attacco più mirato. L'attaccante potrebbe cercare di mappare la topologia della rete per identificare obiettivi potenziali.
L'ipotesi è che il vettore di attacco utilizzato sia la scansione delle porte e dei servizi lanciata sull'host target 192.168.200.150 dall'attaccante 192.168.200.100.

Notiamo nella cattura di Wireshark che alla richiesta TCP dell'attaccante verso alcune porte, sono state inviate risposte positive dal target, evidenziate dal flag "SYN+ACK". In questo modo, l'attaccante ha potuto individuare le porte aperte e i servizi disponibili sull'host target. Ma allo stesso modo l'attaccante ha ricevuto anche risposte negative dal target, evidenziate dal flag "RST+ACK", indicando quindi anche le porte chiuse. Queste evidenze, sono deducibili anche nella schermata conversazioni, tab "**TCP-1206**". Selezionando il tab "**Pacchetti**" il tool ha ordinato le richieste TCP in base al numero di pacchetti inviati, dal maggior numero di pacchetti al minore numero di pacchetti. Possiamo osservare che per le porte 21-23, 25, 53, 80, 111, 139, 445, 512-514 il numero di pacchetti scambiati è di 4, il che fa presumere che si sia concluso il three way hand shake, con conseguente connessione dell'attaccante alle porte associate ai servizi di rete. Per le altre porte, invece, si notano soli due pacchetti scambiati in totale, presumibilmente una richiesta SYN dell'attaccante e una risposta di porta chiusa dall'host di destinazione. **La nostra ipotesi sembra essere quindi confermata dal fatto che oltre ad inviare richieste SYN+ACK, che mostrano le porte aperte alla comunicazione, abbiamo anche delle richieste RST+ACK che invece mostrano la comunicazione sulla porta chiusa.**

È utile ricordare che quando l'IP è visibile nell'alert di un SIEM -> Virus Total (feed open source) per verificare se c'è già l'IP nella lista delle minacce o se deve magari essere inserito nella lista nera di quella compagnia.

RST+ACK = Il server risponde con un pacchetto con i flag Reset e ACK abilitati. Questo comportamento è indicativo di una **porta chiusa**. Non completa il 3-way-handshake, ma chiude la comunicazione inviando un pacchetto RST (**reset**). Tuttavia, riesce a recuperare informazioni sullo stato della porta. Utile in quanto genera meno entropia e «rumore» a livello di rete.

Consiglia un'azione per ridurre gli impatti dell'attacco

Isolamento delle Porte: Isolare le porte coinvolte nell'attacco. Ciò può impedire che l'attaccante prosegua con ulteriori fasi dell'attacco.
Regole Firewall: Aggiornare le regole del firewall per limitare l'accesso non autorizzato e per rilevare attività di scanning ricorrente.
Monitoraggio Attivo: Implementare un monitoraggio attivo per rilevare e rispondere tempestivamente a ulteriori attività di scanning o tentativi di intrusione.
Aggiornamento dei Sistemi: Assicurarsi che tutti i sistemi siano aggiornati con le ultime patch di sicurezza per ridurre il rischio di sfruttamento di eventuali vulnerabilità scoperte.
Formazione e Sensibilizzazione: Fornire formazione al personale su pratiche di sicurezza informatica per ridurre la probabilità di cadere vittima di attacchi futuri.

Poiché, in questo caso, l'attacco proviene da una sola macchina, possiamo bloccare l'IP e le porte usando il firewall, in modo da bloccare tutte le comunicazioni dall'attaccante.

Potremmo quindi **mettere delle regole al nostro Firewall che andrà a bloccare le richieste di ping e l'indirizzo IP dell'attaccante, in questo caso 192.168.200.100.**
È buona norma utilizzare un SIEM o un SOAR.

Un SIEM (Security Information and Event Management) è un sistema che raccoglie e analizza i dati di sicurezza. Il SIEM può aiutare a identificare e rispondere agli attacchi in diversi modi, tra cui:

- **Identificazione di anomalie**: II SIEM può identificare anomalie nel traffico di rete o nei log di sistema, che potrebbero indicare un attacco.
- **Rilevamento di minacce conosciute**: Il SIEM può utilizzare liste di minacce conosciute per rilevare attacchi noti.
- **Analisi di correlazione**: II SIEM può correlare eventi di sicurezza diversi per identificare attacchi complessi.

Un SOAR può integrare un SIEM per automatizzare la risposta agli eventi di sicurezza. Questo può aiutare a migliorare la rapidità e l'efficacia della risposta agli attacchi.
Ecco alcuni esempi di come un SOAR può essere utilizzato per rispondere automaticamente agli attacchi:

- **Blocco dell'IP dell'attaccante**: Il SOAR può bloccare l'IP dell'attaccante utilizzando un firewall o un altro dispositivo di rete.
- **Avviso di un team di sicurezza**
- **Avvio di una procedura di risposta automatizzata**: II SOAR può avviare una procedura di risposta automatizzata che può includere azioni come la rimozione di malware o la modifica delle impostazioni di sicurezza.

Conclusioni

Nella cattura di rete fornita possiamo notare multiple richieste TCP su ampi intervalli di porte. Da ciò possiamo supporre sia stato effettuato un portscanning con un tool che potrebbe essere Nmap o qualcosa di simile.
Per ridurre gli impatti negativi che un attacco di port scanning ed enumeration service può provocare, si consiglia l'implementazione di una misura di sicurezza preventiva sul target per negare la possibilità di individuare vulnerabilità che possono essere successivamente sfruttate per ottenere accesso al sistema operativo e compiere operazioni non autorizzate.
La misura consigliata consiste nella corretta configurazione di un Firewall che, tramite policy, blocchi l'accesso alle porte per quel determinato attaccante, inibisca ulteriori attacchi e, in generale, prevenga la possibilità di ottenere la lista delle porte aperte e dei servizi disponibili.