S9-L5 **Threat Intelligence & IOC**

**Traccia**: Esercizio Threat Intelligence & IOC 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 lʼesercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

● Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso

● In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati

● Consigliate unʼazione per ridurre gli impatti dellʼattacco attuale ed eventualmente un simile attacco futuro

Introduzione alla Threat Intelligence

**Definizione**: La Threat Intelligence ( TI ) è la raccolta, l'analisi e la condivisione di informazioni su minacce attuali e potenziali alla sicurezza informatica. Queste informazioni provengono da diverse fonti e includono dettagli sui cyber attacchi, sulle vulnerabilità dei sistemi, sulle tattiche degli attaccanti e sugli indicatori di compromissione (IoC) .

**Scopo**: L'obiettivo della TI è di fornire una visione completa del panorama delle minacce, consentendo alle organizzazioni di:

● Comprendere: Riconoscere e valutare le minacce attuali e potenziali che possono colpire l'organizzazione.

● Prevenire: Implementare misure di sicurezza proattive per mitigare i rischi prima che si concretizzino.

● Rispondere: Reagire in modo rapido ed efficace agli incidenti di sicurezza, riducendo l'impatto e accelerando il recupero.

**Da cos'è composta la Threat Intelligence:**

● Dati Grezzi: Informazioni raccolte da varie fonti, come log di sistema, dati di rete, rapporti di incidenti e fonti OSINT ( Open Source Intelligence).

● Elaborazione dei Dati: Trasformazione dei dati grezzi in informazioni utili tramite filtraggio, normalizzazione e contestualizzazione.

● Analisi: Esame dettagliato delle informazioni per identificare pattern, tendenze e relazioni tra diverse minacce.

● Produzione di Rapporti: Creazione di rapporti strutturati che presentano i risultati dell'analisi in modo chiaro e utilizzabile.

● Disseminazione: Condivisione delle informazioni con le parti interessate tramite vari canali, come piattaforme di collaborazione, email, dashboard e report.

**Il Ciclo di Vita della Threat Intelligence**

Il ciclo di vita della Threat Intelligence è un processo continuo e iterativo che guida le attività di raccolta, analisi e utilizzo delle informazioni sulle minacce. Ogni fase del ciclo serve a migliorare la comprensione delle minacce e a informare le decisioni di sicurezza.

1. Pianificazione e Direzione: Determinare gli obiettivi e i requisiti di intelligence.

( Requirements Gathering )La prima fase del ciclo di vita della TI è la pianificazione dei requisiti. Questi possono essere definiti in base allo storico degli attacchi subiti, alle minacce più probabili che impattano il mercato di appartenenza della compagnia, o come risultato di una valutazione del rischio ("risk assessment") precedentemente effettuata.

1. Raccolta: Ottenere dati da fonti interne ed esterne.

( Threat Data Collection) Una volta identificati i requisiti, si può iniziare la fase di raccolta dei "feed" dalle sorgenti di TI. Solo le informazioni che sono in linea con i requisiti definiti devono essere considerate rilevanti. Questa fase può essere ripetuta all'interno del ciclo di vita della TI, qualora vengano aggiunti nuovi requisiti o modificati quelli esistenti.

1. Elaborazione: Pulizia, organizzazione e formattazione dei dati raccolti.
2. Analisi: Interpretazione dei dati per generare insights utili.

( Threat Data Analysis ) Una volta recuperati i dati su eventuali minacce, questi devono essere processati dai tool e dai software disponibili. Alcune informazioni potrebbero già essere in un formato "leggibile" dai tool, mentre altre potrebbero richiedere modifiche alla formattazione. In questa fase, tutte le attività necessarie per rendere le informazioni fruibili dai tool disponibili vengono eseguite, consentendo l'analisi automatica e la creazione di report sulle minacce attuali per la consultazione da parte della dirigenza.

1. Disseminazione: Distribuzione delle informazioni rilevanti agli stakeholder.

( TI Dissemination ) Nella fase di TI dissemination, ovvero la "diffusione delle informazioni", i dati appena elaborati e i report generati dagli strumenti automatici vengono condivisi con la dirigenza e il personale operativo (responsabile delle operazioni di sicurezza). Questi report saranno utilizzati per prendere decisioni strategico-operative, come la gestione delle minacce e l'adozione di misure preventive.

1. Feedback: Valutazione dell'efficacia e miglioramento continuo del processo.

( Gathering Feedback) L'ultima fase del ciclo di vita della TI è la raccolta dei feedback sui report precedentemente creati. Il continuo miglioramento è un elemento critico per l'intero processo e deve essere utilizzato per affinare le ricerche, perfezionando e dettagliando i requisiti che verranno utilizzati nel "nuovo ciclo" per migliorare l'output generale del programma di Threat Intelligence.

**Indicatori di Compromissione (IoC)**

Gli Indicatori di Compromissione ( IoC) sono segnali specifici che suggeriscono che un sistema o una rete è stata compromessa da un attacco informatico.

**Tipi di IoC:**

● Indirizzi IP Malevoli: IP noti per essere utilizzati in attività dannose.

● Hash di File: Impronte digitali uniche di file malevoli.

● URL e Domini Malevoli: Siti web utilizzati per phishing o distribuzione di malware.

● Processi Anomali: Programmi o attività in esecuzione non autorizzati o sospetti.

● Modifiche ai File: Alterazioni non autorizzate a file di sistema o applicazioni.

**Uso degli IoC:**

● Rilevamento: Identificare e monitorare attività sospette.

● Risposta agli Incidenti: Informare le azioni correttive durante un'indagine su un incidente.

● Prevenzione: Bloccare attacchi futuri utilizzando liste di controllo aggiornate.

**Relazione sulla Ricerca degli Indicatori di Compromissione (IoC)**

In questa analisi, abbiamo utilizzato Wireshark per esaminare il traffico di rete catturato.L'obiettivo è identificare Indicatori di Compromissione (IoC), segnali che suggeriscono attività sospette o malevole sulla rete. Gli IoC analizzati includono indirizzi IP, protocolli anomali, comportamenti di connessione sospetti e altre evidenze di potenziali attacchi.

1. **Indirizzi IP Malevoli**

Un IP malevolo è un indirizzo IP noto per essere coinvolto in attività dannose, come distribuzione di malware, phishing, attacchi DDoS, tentativi di accesso non autorizzati o scansioni di rete. Questi IP vengono spesso utilizzati da attori malevoli per compromettere sistemi e reti. Sono identificati tramite analisi delle minacce, segnalazioni di incidenti e database pubblici o privati, come liste di blocco (blacklist) mantenute da organizzazioni di sicurezza informatica.

* **192.168.200.150**: Questo indirizzo IP sembra essere coinvolto in diverse comunicazioni. Potrebbe essere il bersaglio o la fonte di traffico sospetto.
* **192.168.200.255**: Questo indirizzo rappresenta un broadcast, ma è utile verificarlo nel contesto di comunicazioni anomale.
*  **192.168.200.100** (Source): Questo indirizzo IP genera traffico diretto verso **192.168.200.150**, ed è quindi sospetto. Va analizzato se è l'attaccante o un nodo compromesso.
*  **192.168.200.150** (Destination): Questo IP sembra essere il bersaglio della maggior parte delle connessioni TCP. Potrebbe rappresentare una macchina vulnerabile sotto attacco.

1. **Porte e Protocolli Anomali**

Porte e protocolli anomali si riferiscono all'uso di porte di comunicazione o protocolli in modo inusuale o sospetto rispetto al comportamento normale di una rete. Ad esempio, un servizio che comunica su una porta non standard (come il protocollo HTTP sulla porta 12345 invece della porta 80 o 443) o l'uso di protocolli in modi non previsti può indicare un'attività malevola, come tunnel di dati nascosti, exploit o movimenti laterali da parte di un attaccante. Questi comportamenti sono spesso indizi di compromissione o tentativi di eludere i sistemi di sicurezza.

* **Porta 33876**: Utilizzata in un flusso TCP. Potrebbe essere una porta non standard per comunicazioni normali. Verificare se è associata a traffico sospetto o non autorizzato.
* **Porta 80 (HTTP)**: Questa è una porta standard, ma il traffico che la utilizza va analizzato per verificare se contiene payload malevoli.
* **Porta 53006**: Non comune. Utilizzata per traffico TCP in questo dump e va investigata come possibile segnale di compromissione.
* **55656, 53006, 49174**: Queste porte non standard sono utilizzate per le comunicazioni. È possibile che siano sfruttate per attività malevole o backdoor.
* **Porta 80 (HTTP)**: Sebbene sia una porta standard, va verificato se il traffico sulla porta HTTP contiene exploit o payload malevoli.
* **Porta 443**: Utilizzata per HTTPS, ma potrebbe essere sfruttata per connessioni criptate illecite

1. **Tentativi di Connessione e Errori**

Tentativi di connessione ed errori si riferiscono a eventi di rete in cui un sistema cerca di stabilire una comunicazione con un altro, ma la connessione non va a buon fine. Questi eventi possono indicare:

* Scansioni di rete: Gli attaccanti verificano quali porte sono aperte o quali servizi sono attivi su un sistema.
* Tentativi di brute force: Ripetute connessioni fallite su porte specifiche, spesso legate a credenziali errate, suggeriscono tentativi di accesso non autorizzati.
* Errori di configurazione: Possono derivare da impostazioni errate dei sistemi o servizi.
* Segnali di attacco: Errori come pacchetti respinti o risposte RST/ACK potrebbero indicare che un attaccante sta sondando la rete o cercando vulnerabilità.

Monitorare questi eventi aiuta a rilevare anomalie e mitigare potenziali minacce.

Sono visibili pacchetti con flag **RST (Reset)**, il che potrebbe indicare:

* + **Comunicazioni interrotte** intenzionalmente.
  + **Scanner di rete** o tentativi di ricognizione che terminano le connessioni dopo aver verificato se una porta è aperta.

1. **Nomi Host**

Nomi host sono identificatori univoci assegnati ai dispositivi di una rete per facilitarne l’identificazione e la comunicazione. Possono essere utilizzati per monitorare attività sospette, in quanto:

* Host malevoli: Un nome host che richiama server di comando e controllo (C2) o domini usati per phishing/malware può indicare compromissione.
* Nomi anomali: Host con nomi inconsueti o non conformi agli standard aziendali possono segnalare sistemi compromessi o configurati impropriamente.
* Risoluzioni DNS sospette: Se un nome host legittimo punta a un IP noto per attività malevole, può essere segno di un attacco (come DNS spoofing).

Analizzare i nomi host aiuta a individuare dispositivi compromessi o comunicazioni verso risorse pericolose.

* Il nome "METASPLOITABLE" suggerisce che la macchina è una configurazione vulnerabile utilizzata per test di penetrazione. Tuttavia, in un contesto reale, qualsiasi host con un nome simile potrebbe essere preso di mira da attacchi.

1. **Anomalie nei Pacchetti**

Anomalie nei pacchetti si riferiscono a irregolarità o comportamenti insoliti nei dati trasmessi attraverso la rete. Queste anomalie possono indicare attività sospette o malevole, come:

* Pacchetti con dimensioni insolite: Dati troppo grandi o troppo piccoli rispetto al normale traffico di rete.
* Sequenze TCP anomale: Problemi nei flag (come SYN senza risposta o RST inaspettati) possono segnalare scansioni o tentativi di exploit.
* Dati non attesi: Contenuti strani o codificati in protocolli standard (es. payload di malware nascosti in pacchetti HTTP o DNS).
* Comportamenti fuori standard: Uso improprio di protocolli o trasmissioni su porte non standard.

Queste anomalie possono derivare da errori di configurazione, attacchi (es. DDoS, spoofing) o tentativi di eludere i sistemi di sicurezza. Analizzarle aiuta a rilevare e mitigare potenziali minacce.

* Alcuni pacchetti TCP contengono dettagli di configurazione, come il **Window Size** e **ACK**, che potrebbero essere indicatori di scansioni o exploit attivi.
* **ARP Request/Reply**: Le richieste ARP possono essere normali, ma se ci sono molte richieste insolite, può trattarsi di un **attacco di spoofing ARP**.

1. **Flag TCP Anomali**

I flag TCP anomali sono segnali nel protocollo TCP che indicano comportamenti insoliti o sospetti durante la comunicazione tra dispositivi. Ogni pacchetto TCP include flag che definiscono lo stato della connessione, come SYN (richiesta di connessione), ACK (riconoscimento), o RST (reset della connessione). Flag anomali possono includere:

* SYN ripetuti senza risposta: Segnalano tentativi di connessione non completati, tipici di scansioni o attacchi SYN Flood.
* RST non attesi: Indicano connessioni interrotte in modo forzato, spesso per nascondere attività malevole.
* Combinazioni inusuali (es. SYN e FIN insieme): Usate in attacchi per testare le risposte di un sistema.

Queste anomalie possono rivelare scansioni, attacchi DoS, o tentativi di sfruttare vulnerabilità.

**RST, ACK**: I pacchetti che contengono questi flag possono indicare che:

* + Un attaccante sta effettuando scansioni di rete o testando connessioni.
  + Il traffico è interrotto deliberatamente dopo aver stabilito una connessione iniziale, il che è tipico di attività di ricognizione.

**SYN**: Molti pacchetti contengono flag SYN, suggerendo che ci sono numerosi tentativi di connessione. Questo potrebbe essere segno di una **scansione di rete** o un **tentativo di exploit**.

1. **Sequenza Temporale e Anomalie**

Una sequenza temporale anonima è un'analisi cronologica degli eventi di rete che rimuove informazioni sensibili, come nomi di utenti, indirizzi IP o dettagli specifici, per garantire la privacy dei dati. Questa tecnica è utile per condividere informazioni su incidenti di sicurezza senza rivelare dettagli che potrebbero compromettere la riservatezza.

Ad esempio, una sequenza temporale anonima potrebbe apparire così:

1. T=0: Tentativo di connessione alla porta X del sistema Y.
2. T+5 secondi: Rilevata risposta anomala con flag TCP RST.
3. T+10 secondi: Ripetizione del tentativo su una porta diversa.
4. T+20 secondi: Traffico sospetto interrotto bruscamente.

Questo tipo di analisi consente di evidenziare comportamenti sospetti o malevoli senza esporre informazioni critiche, favorendo la collaborazione tra team di sicurezza.

* I pacchetti hanno **sequenze rapide e ravvicinate**. Questo potrebbe indicare un attacco di tipo **flooding** o tentativi automatizzati di connessione da parte di uno script o malware.

1. **Lunghezza dei Pacchetti**

La lunghezza dei pacchetti si riferisce alla quantità di dati contenuti in un pacchetto di rete, espressa in byte. Analizzare questa caratteristica è importante perché:

* Pacchetti troppo grandi: Potrebbero indicare tentativi di attacchi DoS (come un Ping of Death) o l'uso improprio di protocolli per trasferire dati non autorizzati.
* Pacchetti troppo piccoli: Spesso associati a ricognizioni o scansioni di rete, poiché gli attaccanti inviano pacchetti ridotti per sondare porte o servizi.
* Lunghezza anomala rispetto al protocollo: Se un pacchetto HTTP o DNS è più lungo o più corto del previsto, potrebbe contenere dati malevoli o essere un tentativo di elusione dei controlli di sicurezza.

Monitorare e confrontare la lunghezza dei pacchetti con il traffico normale aiuta a identificare attività sospette o fuori standard.

* Molti pacchetti hanno **Length = 0**, suggerendo tentativi di connessione senza invio di dati reali. Questo è comune in:
  + **Ricognizioni di rete**.
  + **Tentativi di handshake TCP incompleti** (potenzialmente attacchi SYN flood).

**Rapporto di Analisi - Vettori di Attacco e Azioni di Mitigazione**

**Analisi dei Vettori di Attacco Potenziali in Base agli IoC Raccolti**

Dalle immagini fornite, sono emersi vari **Indicatori di Compromissione (IoC)** che suggeriscono la presenza di attività malevole all'interno della rete. Ecco le ipotesi sui possibili vettori di attacco in base agli IoC trovati:

1. **Tentativi di Connessione su Porte Non Standard**
   * **IoC:** La presenza di tentativi di connessione su porte diverse da quelle standard (80, 443) e il traffico anomalo su **porte elevate** (>1024) possono suggerire un attacco di tipo **port scanning** per identificare vulnerabilità o porte aperte da sfruttare.
   * **Vettore di attacco:** Un attaccante potrebbe utilizzare strumenti come **Nmap** o **Masscan** per mappare i servizi attivi e vulnerabili sulla macchina di destinazione.
2. **Anomalie nei Pacchetti TCP**
   * **IoC:** La ripetizione di pacchetti TCP con flag **SYN** senza completare l'handshake (indicando un possibile SYN Flood) e pacchetti **RST, ACK** che sembrano forzare la terminazione di connessioni.
   * **Vettore di attacco:** Questo tipo di traffico è tipico di un **attacco DDoS** (Distributed Denial of Service) volto a saturare le risorse del sistema o a mascherare attività malevole come l'iniezione di codice. Può anche indicare **ricognizioni** (scansioni di rete per determinare quali porte sono vulnerabili).
3. **Indirizzo IP Sospetto (192.168.200.150)**
   * **IoC:** L'indirizzo IP che ha generato il traffico anomalo potrebbe essere un punto di origine per un attacco **interno** o un **attaccante esterno** che sta cercando di compromettere i sistemi.
   * **Vettore di attacco:** Se l'indirizzo IP appartiene a un dispositivo interno compromesso, potrebbe essere usato come parte di un attacco più ampio, come un **escalation di privilegio** o un attacco di **movimento laterale** all'interno della rete.

**Azioni per Ridurre gli Impatti dell'Attacco Attuale**

1. **Bloccare l'IP sospetto (192.168.200.150)**
   * La prima azione immediata dovrebbe essere **isolare** l'indirizzo IP sospetto per impedire ulteriori tentativi di connessione o interazioni con il sistema compromesso. Questo può essere fatto a livello di **firewall** o tramite **Access Control Lists (ACL)**.
2. **Rafforzare le Regole del Firewall**
   * Implementare **filtri di rete** più rigorosi per limitare l'accesso alle **porte non standard** e bloccare tentativi di connessione su porte elevate non necessarie.
   * Bloccare connessioni in ingresso da IP esterni non autorizzati o **non affidabili**, basandosi su blacklist di IP malevoli noti.
3. **Monitoraggio Attivo e Rilevamento Intrusioni**
   * Configurare e abilitare **sistemi di rilevamento delle intrusioni (IDS)** o **sistemi di prevenzione delle intrusioni (IPS)** per monitorare e bloccare automaticamente comportamenti sospetti come scansioni di porte o attacchi DoS.
   * Analizzare i **log di rete** per identificare altre attività sospette provenienti da fonti simili.
4. **Verifica e Correzione di Vulnerabilità nei Servizi**
   * Effettuare una **revisione della configurazione di rete** e dei servizi esposti sulla macchina vulnerabile, in particolare per i servizi HTTP, HTTPS e altre porte che potrebbero essere sfruttate.
   * Assicurarsi che **tutti i servizi siano aggiornati** con le ultime patch di sicurezza.

**Prevenzione di Attacchi Simili in Futuro**

1. **Rafforzare le Misure di Autenticazione**
   * Abilitare l'**autenticazione multifattore (MFA)** su tutte le interfacce sensibili per prevenire accessi non autorizzati, in particolare su applicazioni o interfacce di amministrazione remota.
   * Rivedere e **limitare l'accesso alle porte di amministrazione**, come quelle utilizzate per SSH, RDP, e altri servizi critici, configurandole per essere accessibili solo da indirizzi IP interni.
2. **Implementare Monitoraggio Continuo del Traffico di Rete**
   * Utilizzare strumenti avanzati di **analisi del traffico di rete** come **Wireshark** o **Zeek** per identificare traffico sospetto e attacchi in tempo reale.
   * Implementare soluzioni di **Security Information and Event Management (SIEM)** per correlare eventi da più fonti (firewall, IDS, antivirus) e rilevare pattern anomali.
3. **Segmentazione della Rete**
   * Suddividere la rete in segmenti più piccoli e sicuri per limitare l'impatto di un attacco che comprometta un segmento. Ad esempio, separare la rete aziendale dalla rete di amministrazione e dalla rete degli utenti.
   * **Isolare i dispositivi sensibili**, come server di produzione o database, per ridurre la possibilità che un attaccante possa muoversi lateralmente attraverso la rete.
4. **Educazione e Formazione per il Personale**
   * Condurre regolarmente corsi di formazione per sensibilizzare gli utenti su **buone pratiche di sicurezza**, come evitare di cliccare su link sospetti o scaricare allegati da fonti non verificate.

**Conclusioni**

L'analisi del traffico di rete ha rivelato segni di attacchi mirati attraverso la scansione di porte e possibili tentativi di denial-of-service. Gli IoC identificati, come l'indirizzo IP sospetto e il traffico TCP anomalo, suggeriscono un attacco che mira a ottenere accesso non autorizzato o a compromettere la disponibilità dei servizi. Le azioni di mitigazione immediata includono il blocco dell'IP sospetto, il rafforzamento della sicurezza del firewall e il monitoraggio attivo del traffico di rete. Implementando queste contromisure, si potrà ridurre il rischio di danni attuali e prevenire attacchi simili in futuro.