

Pratica S9-L3

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

Sommario

Pratica S9-L3	1
Threat Intelligence & IOC	1
Introduzione	3
Threat Intelligence (TI)	3
Definizione	3
Information Gathering	4
Fonti delle informazioni	4
Valutazione delle informazioni	5
Fasi del Threat Intelligence	6
Requirements gathering	6
Threat data collection	6
Threat data analysis	7
TI dissemination	7
Gathering feedback	7
Threat Assessment	8
Fattori di descrizione delle minacce	8
Threat actors	8
Threat classification	9
Threat modeling	9
Indicatori di compromissione – IoC	10
Metodi per identificare gli indicatori di compromissioni	10
Analisi degli eventi Network	10
Analisi degli eventi sugli host	12
Analisi degli eventi applicativi o dei servizi	12
Esercitazione sull'identificazione di IoC analizzando una cattura del traffico di rete con Wireshark	13
Identificazione di IoC, ovvero evidenze di attacchi in corso	13
Ipotesi sui potenziali vettori di attacco utilizzati	15
Consiglio per ridurre gli impatti dell'attacco	16

Introduzione

Threat Intelligence (TI)

Definizione

Si tratta di un processo di ***raccolta, analisi e diffusione di informazioni sulle minacce informatiche per costruire una strategia di prevenzione o difesa da minacce esterne che sia il più efficiente possibile.***

In sostanza, è un processo di identificazione e analisi delle cyberminacce.

Esistono tre categorie di Threat Intelligence:

- **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, ma anche dettagli precisi sugli attori della minaccia, la sua provenienza ed i potenziali vettori d'attacco. Quindi, è un Intelligence orientato all'azione e che mira a supportare le attività operative in tempo reale.

La Threat Intelligence (TI) è un elemento cruciale per le **Security Operations**, cioè per l'insieme di processi e attività mirate a garantire la sicurezza informatica e la gestione degli incidenti in un'organizzazione.

Le Security Operations comprendono monitoraggio, analisi degli eventi, risposta agli incidenti e miglioramento continuo delle difese.

La TI supporta le Security Operations fornendo informazioni dettagliate sulle minacce cibernetiche, come modelli di attacco, indicatori di compromissione e comportamenti degli attori delle minacce.

Queste informazioni consentono alle Security Operations di anticipare attività sospette, migliorare l'analisi degli eventi di sicurezza e guidare una risposta mirata.

La TI potenzia la capacità di adattamento delle Security Operations, permettendo una gestione più efficiente delle minacce e una difesa più solida contro gli attacchi informatici.

Infatti, la Threat intelligence fornisce la conoscenza relativa alle cyberminacce che potrebbero colpire o che hanno colpito un'organizzazione al fine di approntare azioni di prevenzione o difesa appropriata.

In particolare, La Threat intelligence, tramite le informazioni sulle minacce, consente alle organizzazioni di intraprendere azioni efficaci per prevenire gli attacchi informatici, prima che si verifichino, oppure di rispondere meglio agli attacchi in corso.

In tal senso, la TI è fondamentale per consentire di pianificare con anticipo i Piani di Business Continuity e Disaster Recovery, consentendo alle organizzazioni di comprendere meglio le minacce potenziali e di sviluppare strategie per garantire la continuità operativa in caso di eventi avversi.

Si comprende, quindi, la definizione della Threat Intelligence data dalla società di consulenza americana Gartner: “[E’] *La conoscenza basata su prove, compresi contesto, meccanismi, indicatori, implicazioni e suggerimenti pratici, di una minaccia o di un pericolo esistente o emergente per le risorse.*

Tale conoscenza può essere utilizzata per indirizzare il processo decisionale di risposta alla minaccia o al pericolo in questione”. (Gartner Inc. – Società di consulenza americana).

Information Gathering

La Threat Intelligence può essere considerata, dal punto di vista di un PT, una forma particolare di Information gathering, in quanto include le **attività di raccolta di informazioni in merito alle potenziali minacce che potrebbero impattare un sistema o una compagnia.**

Le informazioni fondamentali per capire da chi e come difendersi sono i dati di potenziali nemici, le loro motivazioni, metodologie e strumenti a disposizione.

Fonti delle informazioni

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.

• **Open Source Intelligence**

Open source Threat intelligence si riferisce a quelle informazioni sulle minacce ricavate da **sorgenti pubbliche**. Sono spesso le stesse compagnie a condividere le informazioni circa le nuove minacce. Ad oggi la difficoltà maggiore quando si parla di Open source TI è quella di individuare una fonte che sia attendibile.

Tra le fonti di «feed» open source troviamo siti quali:

Alienvault

Virus Total

Cisco Talos Intelligence

Senki

Virus share

• **Closed Source Intelligence**

A differenza della TI open source, 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».

Valutazione delle informazioni

A prescindere dalla fonte, è necessario effettuare la valutazione e l'accertamento delle informazioni reperite utilizzando alcuni fattori comuni, come:

- La **tempestività**: per cui si valuta se un'informazione è attuale o datata in modo da scartare quell'informazione che, essendo datata, non è più rilevante.
- L'**esattezza**: per cui si valuta se l'informazione è accurata.
- La **rilevanza**: per cui 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.

La valutazione delle informazioni può essere rappresentata dal “**confidence factor**” (il fattore di Fiducia), che è parametro espresso da un numero/intervallo di numeri e da un livello. Questo fattore rappresenta il grado di attualità, accuratezza e rilevanza di una determinata informazione.

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.

Fasi del Threat Intelligence

Il «Threat Intelligence life cycle» (ciclo di vita della TI) è il modello più utilizzato per descrivere le fasi o step della Threat intelligence.



Requirements gathering

La prima fase del ciclo di vita della TI è **fase di pianificazione dei requisiti di informazione**.

Scopo principale di questa fase è definire e identificare chiaramente i criteri e le esigenze specifiche dell'organizzazione in termini di informazioni sulle minacce.

In particolare, questa fase mira a **stabilire quali tipi di minacce sono rilevanti, i settori di interesse, i metodi di attacco di maggiore preoccupazione, gli indicatori di compromissione desiderati e altre specifiche pertinenti**.

Infatti, i requisiti 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.

In sintesi, l'obiettivo è fornire una guida chiara per la successiva acquisizione e analisi delle informazioni sulle minacce, in modo che possano essere allineate alle esigenze specifiche e alle priorità dell'organizzazione.

Threat data collection

Una volta che sono stati identificati i requisiti, si può iniziare la **fase di raccolta dei «feed», cioè dei dati/informazioni sulle minacce, dalle sorgenti di TI (sorgenti pubbliche o private)**.

Le informazioni, provenienti da queste fonti eterogenee, vengono, di norma, aggregate in un dashboard centralizzato, come un SIEM o una piattaforma di Threat Intelligence, per una gestione più facile.

Solo le info che sono in linea con i requisiti definiti in precedenza vengono considerate rilevanti e raccolte.

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

La terza fase del ciclo di vita della TI è **fase di elaborazione e analisi approfondita dei dati sulle minacce raccolti**. Una volta recuperati i dati su eventuali minacce, questi devono essere processati dai tool e dai software disponibili.

- Per quanto riguarda l'**elaborazione**, i dati raccolti devono essere trattati, il che comporta:
 - la filtrazione di dati non pertinenti raccolti incidentalmente
 - la strutturazione dei dati per facilitare la fase di analisi: si tratta del processo di organizzazione e formattazione dei dati raccolti.Essendo variegate le fonti dalle quali i dati sono raccolti, alcune delle informazioni potrebbero già essere in un formato «leggibile» dai tool presenti, mentre altre potrebbero necessitare di modifiche alla formattazione.
L'organizzazione dei dati in modo coerente può consistere nel raggruppamento di dati simili o nel collegamento di elementi di dati eterogenei per fornire un contesto specifico a eventi e risorse.
- Una volta completato il trattamento dei dati, si passa alla fase di **analisi**, che è di vitale importanza per tradurre i dati grezzi raccolti in informazioni sulle cyberminacce utili e attuabili: i dati raccolti ed elaborati vengono analizzati per rilevare le minacce e comprendere il loro impatto.
Il risultato del processo di analisi è la trasformazione di informazioni in una vera e propria conoscenza (intelligence), approfondita e contestualizzata, delle minacce alla sicurezza.
L'analisi automatizzata dei dati viene effettuata dai tool e dai software per creare report sulle minacce attuali che siano consultabili da parte dell'organizzazione.

In sintesi, nella fase di Threat data analysis ricadono tutte quelle attività che consentono alle informazioni di essere «consumate» dai tool disponibili, e analizzate automaticamente per creare report sulle minacce attuali che siano consultabili da parte della dirigenza e del personale operativo.

TI dissemination

Nella fase di TI dissemination, ovvero la **fase di «diffusione delle informazioni»**, i dati appena lavorati ed i report appena costruiti dai tool automatici vengono condivisi alla **dirigenza** e al **personale operativo**, responsabile delle security operations.

In tal modo, queste parti (dirigenza/personale operativo) utilizzeranno i report per eventuali decisioni strategico-operative di sicurezza e risposta alle minacce (ad esempio, come gestire eventuali minacce o 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 precedentemente** dall'organizzazione per determinare se l'analisi di intelligence è stata tempestiva, rilevante e attuabile.

Di seguito si riportano alcune buone domande guida che è possibile porre per ricevere feedback che possono essere utilizzati **per migliorare la raccolta e l'analisi di future Threat intelligence**:

- Il prodotto di threat intelligence finito ha portato ad azioni che hanno ridotto il rischio per una o più unità aziendali?
- L'intelligence finita era al giusto livello di dettaglio tecnico per consentire ai vari team di comprenderla facilmente e di agire?
- Ci sono state unità aziendali che avrebbero potuto trarre beneficio dal lavoro ma non l'hanno ricevuto?

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.**

Threat Assessment

Il "Threat assessment" è il processo di **valutazione** e analisi sistematica **delle minacce** che possono influenzare un'organizzazione, un sistema o un ambiente specifico.

Questo processo coinvolge l'identificazione delle potenziali minacce, la valutazione della loro gravità e delle possibili conseguenze, nonché la formulazione di strategie per mitigare o gestire i rischi associati a tali minacce.

Scopo principale del Threat Assessment è **comprendere e valutare il contesto delle minacce per l'adozione di misure preventive o reattive mirate a proteggere gli interessi dell'organizzazione.**

Fattori di descrizione delle minacce

Per la valutazione delle minacce, le aziende utilizzano un modello standardizzato di descrizione. In particolare vengo utilizzati due **fattori descrittivi delle minacce**:

- Gli attori delle minacce (threat actors)
- La classificazione delle minacce (threat classification)

Threat actors

Ci sono diversi **schemi per identificare gli attori delle minacce**, quello proposto di seguito adotta una divisione in **quattro** macro-categorie:

- **Nazioni / Stati**: gli attori delle minacce che ricadono all'interno di questa categoria hanno generalmente accessi a risorse di gran lunga superiore a qualsiasi singolo individuo o compagnia. Infatti, essi hanno a disposizione le risorse di intere nazioni o sono generalmente attori privati sponsorizzati dalle nazioni stesse.
- **Crimine organizzato**: il crimine organizzato ha acquisito un ruolo centrale come threat actor soprattutto negli ultimi anni. Infatti, con l'avvento dei ransomware le organizzazioni criminali sfruttano gli attacchi informatici per generare guadagno finanziario.
- **Attivisti**: sono gruppi organizzati che generalmente utilizzano l'hacking a scopo politico, di ribellione, o protesta verso determinate leggi / idee.
Gli attivisti possono essere singoli individui oppure gruppi organizzati, come per esempio Anonymous o altri gruppi che nel corso degli anni si sono resi famosi allo stesso modo.

Nel caso degli attivisti, le risorse a loro disposizione variano sensibilmente, a seconda che si tratti di individui o gruppi organizzati.

- **Attori interni:** infine, da non sottovalutare, sono le minacce che vengono portate alle compagnie dagli impiegati, ovvero dagli attori interni. Generalmente non casuali, alcune delle minacce possono anche essere frutto di disattenzioni sul lavoro. Le minacce interne sono considerate molto pericolose in quanto non direttamente e preventivamente identificabili.

Threat classification

Come per l'identificazione degli attori delle minacce, anche per quanto riguarda la classificazione delle minacce esistono schemi diversi, ed alcune delle compagnie potrebbero creare degli schemi su misura in base ai propri asset.

Tuttavia, 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 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. Un esempio è quello di un utente che 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. Un esempio è 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.

Threat modeling

Il threat modeling è un **processo attraverso il quale è possibile indentificare ed enumerare potenziali minacce, impatti potenziali sugli asset e proporre adeguati meccanismi di mitigazione.**

Questo rappresenta, nel contesto IT, un approccio strutturato alla sicurezza di una risorsa o di un insieme di risorse che possiedono un certo valore.

Le compagnie che hanno intenzione di capire a fondo la minaccia che potenzialmente potrebbero subire, possono inserire il threat modeling all'interno del loro piano annuale di sicurezza.

Questo modello prende in esame diversi fattori al **fine di capire i veri rischi per l'organizzazione:**

- **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.

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

Indicatori di compromissione – IoC

Si è detto in precedenza che La Threat Intelligence è un processo relativo alla conoscenza delle minacce informatiche che supporta le operazioni di sicurezza delle organizzazioni, al fine di consentire l'adozione di più efficaci strategie di prevenzione e difesa dalle minacce.

Nel caso in cui, invece, un attacco vada a buon fine, le compagnie rispondono con un Incident Response Plan, cioè un piano di risposta agli incidenti.

Nel contesto dell'avvenuta esecuzione di un attacco informatico, sono fondamentali gli Indicatori di Compromissione, ovvero **segnali e traccia che indicano la presenza di una compromissione delle reti, degli end-point, dei sistemi operativi, delle applicazioni e dei servizi.**

Gli IoC sono evidenze di attacchi avvenuti e sono utilizzati, dai responsabili delle security operations, durante le fasi di incident response per ricostruire uno storico degli attacchi e determinarne l'entità, le conseguenze e le modalità.

In sintesi, gli IoC sono utilizzati dopo che un attacco è stato contenuto, quando l'organizzazione colpita necessita di scoprire il come, il quando e il perché è avvenuto l'attacco.

Metodi per identificare gli indicatori di compromissioni

Si procede ad elencare i metodi utilizzati per identificare gli indicatori di compromissione che riguardano:

Le reti

Gli end-point e sistemi operativi

Le applicazioni e 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 di **monitoraggio** delle reti basata sul **traffico di rete gestito dai router**, in quanto essi processano tutto il traffico delle reti e ne tengono spesso traccia nelle loro tabelle interne. Questo tipo di monitoraggio avviene, quindi, **in modo centralizzato**.

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 network 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): SNMP 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'utilità 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 la differenza con il monitoraggio attivo è che mentre questo viene effettuato direttamente sui dispositivi, il monitoraggio passivo viene **effettuato sul link**.

Network monitoring tools

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/già accaduti.

Tra le **tecniche** più comuni per identificare loc sugli host 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** di 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.
Un esempio, è il caso di un attacco di tipo SQLi dove un'applicazione inizia a funzionare diversamente da quanto dovrebbe, restituendo nome, utente e password degli utenti.

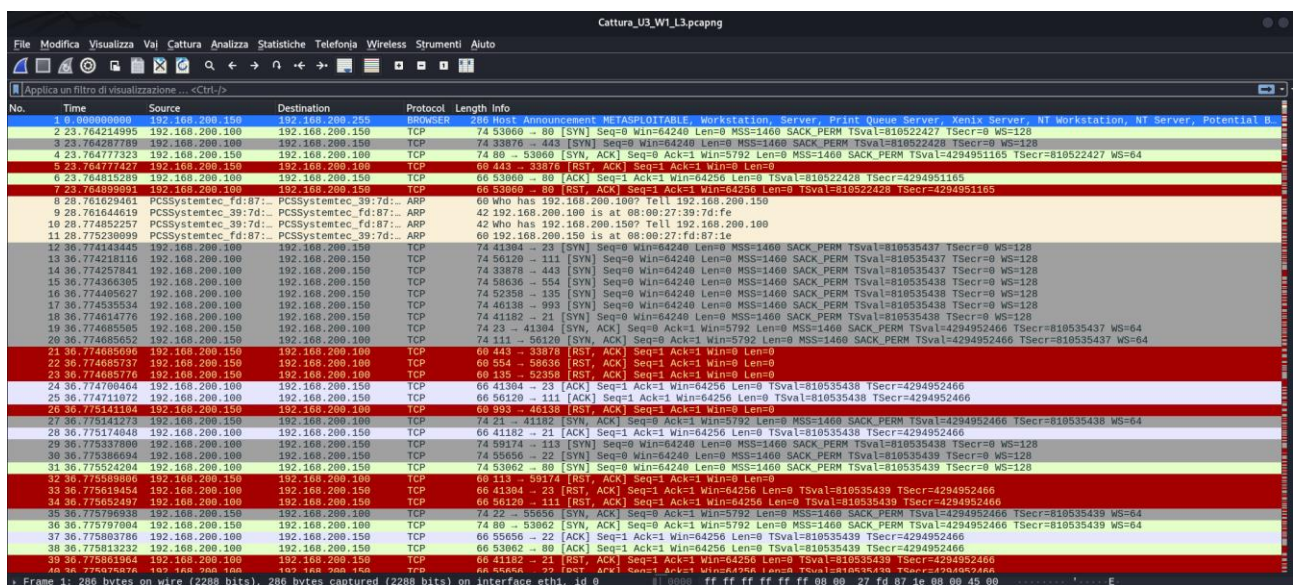
Esercitazione sull'identificazione di IoC analizzando una cattura del traffico di rete con Wireshark

L'esercitazione svolta nel presente report consiste nella ricerca di Indicatori di compromissione attraverso l'analisi del traffico di rete catturato da Wireshark, operando dalla macchina Kali Linux .

In particolare, le richieste della traccia erano di:

- identificare eventuali IoC, evidenze di attacchi in corso
- Sulla base degli IoC trovati, fare delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliare un'azione per ridurre gli impatti negativi dell'attacco

Identificazione di IoC, ovvero evidenze di attacchi in corso



The screenshot shows a Wireshark capture titled 'Cattura_U3_W1_L3.pcapng'. The packet list pane displays a series of TCP packets. The first packet is a SYN from 192.168.200.150 to 192.168.200.150. Subsequent packets show a high frequency of SYN requests from the same source to the same destination, indicating a potential SYN flood attack. The packet details pane shows the TCP header fields, including the SYN flag being set.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	288	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential B...
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951105 TSecr=810522427 WS=64
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	60	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951105
7	23.764839502	192.168.200.100	192.168.200.150	TCP	60	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 TSval=810522428 TSecr=4294951105
8	28.761629401	PCSSystemtec_fd:87...	PCSSystemtec_39:7d...	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d...	PCSSystemtec_fd:87...	ARP	42	192.168.200.100 is at 08:00:27:fd:87:1e
10	28.774952257	PCSSystemtec_39:7d...	PCSSystemtec_fd:87...	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PCSSystemtec_fd:87...	PCSSystemtec_39:7d...	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
12	36.774134445	192.168.200.100	192.168.200.150	TCP	74	41384 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15	36.774366395	192.168.200.100	192.168.200.150	TCP	74	58036 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16	36.774409527	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	40138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
19	36.774685595	192.168.200.150	192.168.200.100	TCP	74	23 → 41384 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
21	36.774685698	192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 58036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774709464	192.168.200.100	192.168.200.150	TCP	60	41384 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774741072	192.168.200.100	192.168.200.150	TCP	60	56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60	993 → 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775143273	192.168.200.150	192.168.200.100	TCP	74	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
28	36.775174848	192.168.200.100	192.168.200.150	TCP	60	41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775378998	192.168.200.100	192.168.200.150	TCP	74	59174 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74	55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53862 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
32	36.775609906	192.168.200.150	192.168.200.100	TCP	60	111 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66	41384 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35	36.775709338	192.168.200.150	192.168.200.100	TCP	74	22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
36	36.775737094	192.168.200.150	192.168.200.100	TCP	74	80 → 53862 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66	53862 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.775861964	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40	36.776004876	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

Osservando la cattura di Wireshark si è riscontrato un **numero di richieste TCP molto elevate**, inviate dall' host sorgente, identificato dall'indirizzo IP 192.168.200.150, all' host di destinazione, identificato dall'indirizzo IP 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.

File Modifica Visualizza Vai Cattura Analizza Statistiche Telefono Wireless Strumenti Aiuto

Proprietà file di cattura Ctrl+Alt+Shift+C

Indirizzi risolti

Gerarchia di protocolli

Appllica un filtro di visualizzazione...

No.	Time	Source	Destination
1	0.009080090	192.168.200.150	Conversioni
2	23.764214995	192.168.200.150	Terminatori
3	23.764207788	192.168.200.150	Lunghezza dei pacchetti
4	23.764777323	192.168.200.150	Gerarchia I/O
5	23.764777427	192.168.200.150	
6	23.764310260	192.168.200.150	
7	23.764939091	192.168.200.150	Tempo di risposta del servizio
8	8.761629461	PC\$Systematic.fid.8	DHCP (BOOTP) Statistics
9	28.761644619	PC\$Systematic.39.7	NetPerfMetric Statistics
10	28.74852257	PC\$Systematic.39.7	QNC-RPC Programs
11	28.775230999	PC\$Systematic.fid.8	
12	28.77434445	192.168.200.150	29Wsc
13	28.774231115	192.168.200.150	ANCP
14	28.774257841	192.168.200.150	BCA.net
15	28.774306395	192.168.200.150	Collectd
16	28.774408762	192.168.200.150	
17	28.774355534	192.168.200.150	
18	28.774614776	192.168.200.150	DNS
19	28.774855905	192.168.200.150	Gratco di flusso
20	28.774865652	192.168.200.150	HART-IP
21	28.774859596	192.168.200.150	HFPEEDS
22	28.774808737	192.168.200.150	
23	28.774808776	192.168.200.150	HTTP
24	24.774700464	192.168.200.150	
25	26.774711072	192.168.200.150	

announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xerox Server, Potential B

== 80 [SYN] Seq=> Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128

== 443 [SYN] Seq=> Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128

== 3660 [SYN, ACK] Seq=> Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64

== 33876 [RST, ACK] Seq=> Ack=1 Win=0 Len=0

== 650 [ACK] Seq=> Ack=1 Win=64240 Len=0 TSval=810522428 TSecr=4294951165

== 80 [RST, ACK] Seq=> Ack=1 Win=64240 Len=0 TSval=810522428 TSecr=4294951165

== 192.168.200.1097 Tell 192.168.200.150

== 8.200.168.101 at 08:00:27:39:7d:7f

== 192.168.200.1507 Tell 192.168.200.100

== 8.200.150 at 08:00:27:7d:7f:81e

== 23 [SYN] Seq=> Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128

== 111 [SYN] Seq=> Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128

== 443 [SYN] Seq=> Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128

== 554 [SYN] Seq=> Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128

== 125 [SYN] Seq=> Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128

== 993 [SYN] Seq=> Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128

== 21 [SYN] Seq=> Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128

== 3304 [SYN, ACK] Seq=> Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64

== 56129 [SYN, ACK] Seq=> Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64

== 33878 [RST, ACK] Seq=> Ack=1 Win=0 Len=0

== 58836 [RST, ACK] Seq=> Ack=1 Win=0 Len=0

== 23836 [RST, ACK] Seq=> Ack=1 Win=0 Len=0

== 23 [ACK] Seq=> Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466

== 111 [ACK] Seq=> Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466

Cattura_U3_W1_L3.pcapng

Wireshark · Conversations · Cattura_U3_W1_L3.pcapng

Conversation Settings		Ethernet · 2	IPv4 · 2	IPv6	TCP · 1026	UDP · 1							
	Risoluzione dei nomi	Indirizzo A	Indirizzo B	Pacchetti	Byte	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Inizio Rel	Durata	Bits/s A → B	Bits/s B → A
	Ora iniziale assoluta	08:00:27:39:7d:fe	08:00:27:fd:87:1e	2,082	140 kB	1,054	78 kB	1,028	62 kB	23.764215	13.1147	47 kbps	37 kbps
		08:00:27:fd:87:1e	ff:ff:ff:ff:ff:ff	1	286 byte	1	286 byte	0	0 byte	0.000000	0.0000		

Wireshark - Conversations - Cattura_03_Wi_L3.pcapng															
Conversation Settings		Ethernet - 2	IPv4 - 2	IPv6	TCP: 1026	UDP: 1									
	Indirizzo A	Porta A	Indirizzo B	Porta B	Pacchetti	Byte	ID flusso	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Inizio Rel.	Durata	Bits/s A → B	Bits/s B → A
Risoluzione dei nomi	192.168.200.100	37365	192.168.200.150	2	2	134 byte	876	1	74 byte	1	60 byte	36.864770	0.0002		
	192.168.200.100	34748	192.168.200.150	2	2	134 byte	292	1	74 byte	1	60 byte	36.806880	0.0002		
	192.168.200.100	58938	192.168.200.150	3	2	134 byte	966	1	74 byte	1	60 byte	36.873582	0.0003		
On iniziale assoluta	192.168.200.100	43056	192.168.200.150	4	2	134 byte	557	1	74 byte	1	60 byte	36.832248	0.0003		
	192.168.200.100	54283	192.168.200.150	5	2	134 byte	661	1	74 byte	1	60 byte	36.841442	0.0003		
	192.168.200.100	40874	192.168.200.150	6	2	134 byte	712	1	74 byte	1	60 byte	36.798733	0.0002		
Copia	192.168.200.100	52702	192.168.200.150	7	2	134 byte	505	1	74 byte	1	60 byte	36.827912	0.0002		
	192.168.200.100	47720	192.168.200.150	8	2	134 byte	124	1	74 byte	1	60 byte	36.790063	0.0001		
	192.168.200.100	41343	192.168.200.150	9	2	134 byte	429	1	74 byte	1	60 byte	36.820242	0.0001		
Segui il flusso...	192.168.200.100	46014	192.168.200.150	10	2	134 byte	216	1	74 byte	1	60 byte	36.795081	0.0001		
	192.168.200.100	37252	192.168.200.150	11	2	134 byte	54	1	74 byte	1	60 byte	36.780326	0.0001		
	192.168.200.100	41700	192.168.200.150	12	2	134 byte	793	1	74 byte	1	60 byte	36.854291	0.0002		
Grafico...	192.168.200.100	58918	192.168.200.150	13	2	134 byte	235	1	74 byte	1	60 byte	36.801644	0.0002		
	192.168.200.100	53648	192.168.200.150	14	2	134 byte	382	1	74 byte	1	60 byte	36.815493	0.0002		
	192.168.200.100	42454	192.168.200.150	15	2	134 byte	233	1	74 byte	1	60 byte	36.801319	0.0002		
Protocollo Bluetooth	192.168.200.100	36316	192.168.200.150	16	2	134 byte	748	1	74 byte	1	60 byte	36.849675	0.0003		
	192.168.200.100	39713	192.168.200.150	17	2	134 byte	93	1	74 byte	1	60 byte	36.817253	0.0001		
	192.168.200.100	57066	192.168.200.150	18	2	134 byte	743	1	74 byte	1	60 byte	36.849341	0.0002		
✓ Ethernet	192.168.200.100	49988	192.168.200.150	19	2	134 byte	102	1	74 byte	1	60 byte	36.787546	0.0002		
	192.168.200.100	48812	192.168.200.150	20	2	134 byte	285	1	74 byte	1	60 byte	36.806168	0.0003		
	192.168.200.100	41162	192.168.200.150	21	4	280 byte	8	1	74 byte	1	74 byte	36.774615	0.0002		
IEEE 802.11	192.168.200.100	55656	192.168.200.150	22	4	280 byte	10	3	206 byte	1	74 byte	36.775387	0.0006		
	192.168.200.100	41304	192.168.200.150	23	4	280 byte	2	3	206 byte	1	74 byte	36.774143	0.00		

192.168.200.100	38352	192.168.200.150	1022	2	134 byte	594	1	74 byte	1	60 byte	36.835363	0.0026
192.168.200.100	59292	192.168.200.150	1023	2	134 byte	463	1	74 byte	1	60 byte	36.823536	0.0003
192.168.200.100	37738	192.168.200.150	1024	2	134 byte	404	1	74 byte	1	60 byte	36.817332	0.0003

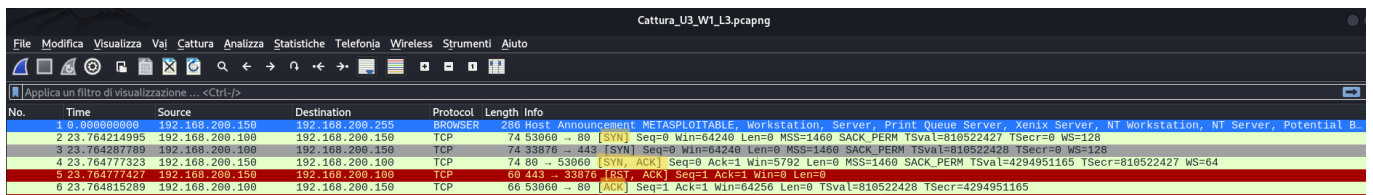
Ipotesi sui potenziali vettori di attacco utilizzati

L'ipotesi è che il vettore di attacco utilizzato sia una **scansione delle porte e servizi** lanciato sull'host target 192.168.200.150 dall'attaccante 192.168.200.100.

Questa ipotesi è sostenuta da due evidenze:

- le molteplici richieste TCP, evidenziate dal flag SYN, sono state inviate ad un numero elevato di porte diverse (che è esattamente ciò che fa un tool come Nmap)
- Tornando ad osservare la schermata principale della cattura di Wireshark, si può notare 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.



Cattura_U3_W1_L3.pcapng

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.100	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential B...
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53668 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
4	23.76477323	192.168.200.100	192.168.200.150	TCP	74	89 → 53668 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
5	23.764774724	192.168.200.100	192.168.200.150	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53668 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899994	192.168.200.100	192.168.200.150	TCP	66	53668 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165

Allo stesso modo l'attaccante ha ricevuto anche risposte negative dal target, evidenziate dal flag "RST+ACK", ad indicare che le porte chiuse.

21	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774700464	192.168.200.150	192.168.200.150	TCP	66	41394 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711872	192.168.200.150	192.168.200.150	TCP	66	56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775141104	192.168.200.150	192.168.200.150	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	192.168.200.150	192.168.200.150	TCP	74	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
28	36.775174048	192.168.200.150	192.168.200.150	TCP	66	41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775337880	192.168.200.150	192.168.200.150	TCP	74	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
30	36.775386994	192.168.200.150	192.168.200.150	TCP	74	55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31	36.775524204	192.168.200.150	192.168.200.150	TCP	74	53662 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
32	36.775589886	192.168.200.150	192.168.200.150	TCP	60	113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.150	192.168.200.150	TCP	66	41394 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775652497	192.168.200.150	192.168.200.150	TCP	66	56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

Queste evidenze, sono deducibili anche nella schermata conversazioni, tab "TCP-1206".

Selezionando stavolta 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.

In questo modo si è potuto 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, che le porte siano aperte, con conseguente connessione dell'attaccante alle porte associate ad alcuni 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.

Ethernet - 2	IPv4 - 2	IPv6	TCP - 1026	UDP - 1													
Indirizzo A	Porta A	Indirizzo B	Porta B	Pacchetti	Byte	ID flusso	Packets A + B	Bytes A + B	Packets B + A	Bytes B + A	Inizio Ret	Durata	Bits/s A + B	Bits/s B + A			
192.168.200.100	41182	192.168.200.150	21	4	280 byte	8	3	206 byte	1	74 byte	36.774615	0.0012					
192.168.200.100	55656	192.168.200.150	22	4	280 byte	10	3	206 byte	1	74 byte	36.775387	0.0006					
192.168.200.100	41304	192.168.200.150	23	4	280 byte	2	3	206 byte	1	74 byte	36.774143	0.0015					
192.168.200.100	60632	192.168.200.150	25	4	280 byte	19	3	206 byte	1	74 byte	36.776512	0.0015					
192.168.200.100	37282	192.168.200.150	53	4	280 byte	21	3	206 byte	1	74 byte	36.776671	0.0014					
192.168.200.100	53060	192.168.200.150	80	4	280 byte	0	3	206 byte	1	74 byte	23.764215	0.0007					
192.168.200.100	53062	192.168.200.150	80	4	280 byte	11	3	206 byte	1	74 byte	36.775524	0.0005					
192.168.200.100	56120	192.168.200.150	111	4	280 byte	3	3	206 byte	1	74 byte	36.774218	0.0014					
192.168.200.100	46990	192.168.200.150	139	4	280 byte	17	3	206 byte	1	74 byte	36.776478	0.0014					
192.168.200.100	33042	192.168.200.150	445	4	280 byte	15	3	206 byte	1	74 byte	36.776386	0.0015					
192.168.200.100	45648	192.168.200.150	512	4	280 byte	68	3	206 byte	1	74 byte	36.781357	0.0006					
192.168.200.100	42048	192.168.200.150	513	4	280 byte	480	3	206 byte	1	74 byte	36.825388	0.0039					
192.168.200.100	51396	192.168.200.150	514	4	280 byte	118	3	206 byte	1	74 byte	36.788600	0.0011					
192.168.200.100	37296	192.168.200.150	1	2	134 byte	674	1	74 byte	1	60 byte	36.854770	0.0002					
192.168.200.100	34748	192.168.200.150	2	2	134 byte	292	1	74 byte	1	60 byte	36.806880	0.0002					
192.168.200.100	58538	192.168.200.150	3	2	134 byte	966	1	74 byte	1	60 byte	36.873582	0.0003					
192.168.200.100	43056	192.168.200.150	4	2	134 byte	357	1	74 byte	1	60 byte	36.832248	0.0003					
192.168.200.100	54282	192.168.200.150	5	2	134 byte	661	1	74 byte	1	60 byte	36.841442	0.0003					
192.168.200.100	40874	192.168.200.150	6	2	134 byte	212	1	74 byte	1	60 byte	36.798733	0.0003					
192.168.200.100	52102	192.168.200.150	7	2	134 byte	505	1	74 byte	1	60 byte	36.827912	0.0002					
192.168.200.100	47720	192.168.200.150	8	2	134 byte	124	1	74 byte	1	60 byte	36.790063	0.0001					
192.168.200.100	41448	192.168.200.150	9	2	134 byte	429	1	74 byte	1	60 byte	36.820242	0.0002					
192.168.200.100	46014	192.168.200.150	10	2	134 byte	716	1	74 byte	1	60 byte	36.795061	0.0002					
192.168.200.100	37252	192.168.200.150	11	2	134 byte	54	1	74 byte	1	60 byte	36.780326	0.0003					
192.168.200.100	41700	192.168.200.150	12	2	134 byte	793	1	74 byte	1	60 byte	36.854291	0.0002					
192.168.200.100	58814	192.168.200.150	13	2	134 byte	235	1	74 byte	1	60 byte	36.801464	0.0002					
192.168.200.100	53648	192.168.200.150	14	2	134 byte	382	1	74 byte	1	60 byte	36.815493	0.0003					
192.168.200.100	42454	192.168.200.150	15	2	134 byte	233	1	74 byte	1	60 byte	36.801319	0.0002					
192.168.200.100	58792	192.168.200.150	16	2	134 byte	229	1	74 byte	1	60 byte	36.814676	0.0002					

Consiglio per ridurre gli impatti dell'attacco

Per ridurre gli impatti negativi che un simile attacco di port scanning e enumeration service può provocare, si consiglia, sul target, l'implementazione di una misura di sicurezza preventiva, che però, nel caso in esame, aiuta a limitare il raggio di azione dell'attacco stesso.

Infatti, con una scansione generale del target, si possono individuare molteplici 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, la quale, tramite policy che blocchi l'accesso alle porte per quel determinato attaccante, inibisca eventuali attacchi più marcati e, in generale, che l'elenco delle porte aperte e dei servizi disponibili non sia individuato.