TEAM

Cyber Secure TECH

INDICE GENERALE

S9_L1-L5

Cyber Secure TECH

INDICE
GIORNO 1

S9_L1

Giorno 1 – Security Operation

Cyber Secure TECH

TRACCIA
GIORNO 1

Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato.

La macchina Windows XP che abbiamo utilizzato ha di default il Firewall disabilitato.

L'esercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno. Per questo motivo:

1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP
2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch –sV, per la service detection e -o nomefilereport per salvare in un file l'output)
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.
5. Trovare le eventuali differenze e motivarle.

Che differenze notate? E quale può essere la causa del risultato diverso?

Requisiti: Configurate l'indirizzo di Windows XP come di seguito: 192.168.240.150 Configurate l'indirizzo della macchina Kali come di seguito: 192.168.240.100

Cyber Secure TECH

C.I.A.

Uno degli scopi principali della sicurezza informatica è mettere al sicuro le informazioni ed i dati. La sicurezza di un ambiente informatico viene parametrata sulla base di «principi fondamentali».

Uno dei principi cardine e più importanti per valutare lo stato della sicurezza delle informazioni di un dato ambiente è il «CIA principle», dove:

- C, staper Confidentiality, ovvero la riservatezza del dato
- I, staper Integrity, ovvero l'integrità del dato
- A, staper Availability, ovvero la disponibilità del dato Generalmente, i controlli di sicurezza sono valutati in base al loro impatto sulle componenti del «CIA principle» (detto anche CIA triad) e da li si parte per effettuare opportune azioni di remediation

LA POSSIBILITÀ CHE UN EVENTO POSSA ACCADERE CAUSANDO DANNI PARZIALI O TOTALI A DATI, INFORMAZIONI OPPURE ASSET PRENDE IL NOME DI «RISCHIO».

COME ABBIAMO VISTO NELLE UNITÀ PRECEDENTI, IL RISCHIO PUÒ ESSERE GESTITO IN DIVERSI MODI, TRA I QUALI:

- RIDUZIONE DEL RISCHIO: INTRODUCENDO DELLE «SECURITY REMEDIATION ACTION», OVVERO DELLE AZIONI DI RIMEDIO PER RIDURRE / ELIMINARE IL RISCHIO
- ACCETTAZIONE DEL RISCHIO: ACCETTANDO IL RISCHIO RESIDUO
- RIMOZIONEDEL RISCHIO: RIMUOVENDO L'ASSET (LADDOVE NON CRITICA) SOGGETTA AL RISCHIO
- TRASFERIMENTO DEL RISCHIO: TRASFERENDO IL RISCHIO AD UN'ALTRA ENTITÀ, AD ESEMPIO UN'ASSICURAZIONE O AD UN'AZIENDA DI SICUREZZA ESTERNA

Cyber Secure TECH

SECURITY OPERATION

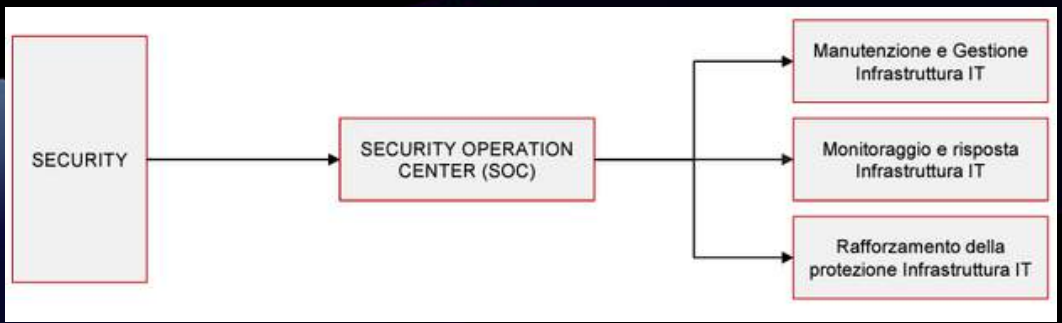
Il Security Operation Center (SOC), è un sotto-dipartimento all'interno del dipartimento di Sicurezza che eroga servizi finalizzati alla protezione dei sistemi informatici, quali:

1) Servizi di gestione: in questa categoria ricadono tutte quelle attività di gestione e manutenzione dell'infrastruttura IT delle compagnie, come ad esempio, la manutenzione dei server, degli switch e router di rete, degli applicativi e così via.

2) Servizi di monitoraggio e risposta: questa sezione comprende tutte quelle attività erogate al fine di monitorare in tempo reale tutte le componenti dell'infrastruttura IT della compagnia. Il monitoraggio ha lo scopo di individuare tempestivamente eventuali «minacce» (anche chiamate «security threats») ed in caso di attacco andato a buon fine, ha il compito di rispondere prontamente per limitare i danni. Al fine di settare gli strumenti e le configurazioni, è importante capire da quali tipi di minacce bisogna difendersi. Questa fase prende il nome di «threat identification»

I servizi di «Security Operation» possono anche essere definiti secondo una logica temporale in relazione al verificarsi di una situazione particolare che viene detta «incidente di sicurezza».

Sebbene possa sembrare scontato, un «incidente di sicurezza» si riferisce ad un impatto negativo sulla riservatezza, integrità o disponibilità un evento che ha un attacco esterno di una data risorsa, come risultato di oppure di un azione volutamente dannosa proveniente dall'interno (ad esempio da un impiegato).
Mentre con il termine generico «incidente», si includono all'interno delle casistiche considerate poc'anzi anche gli eventi ambientali e accidentali.



Cyber Secure TECH

1.1 Presentazione Azienda

Cyber Secure TECH

About Us

Info

Azienda leader nel settore della sicurezza informatica, specializzata nella fornitura di soluzioni avanzate per la protezione dei dati e delle infrastrutture aziendali.
Offre servizi di consulenza, implementazione e gestione della sicurezza informatica per clienti in diversi settori, tra cui finanza, sanità, pubblica amministrazione e telecomunicazioni.

Mission statement

Protezione delle informazioni critiche e a mitigare i rischi associati alle minacce informatiche.
Ci impegniamo a fornire soluzioni personalizzate e all'avanguardia che assicurino la continuità operativa e la resilienza delle infrastrutture IT dei nostri clienti.

Vision

Garantire un futuro sicuro e affidabile per aziende e individui attraverso soluzioni di cybersecurity innovative, efficaci e accessibili.

Our values

Innovazione - Affidabilità - Integrità - Collaborazione - Formazione continua

Cyber Secure TECH

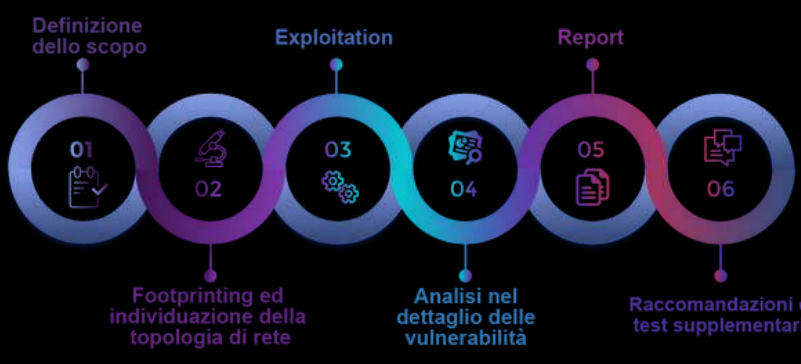
1.1 – Ingaggio

1.1 - INGAGGIO

I dettagli che riguardano un Penetration Test vengono stabiliti durante una fase preliminare detta fase di ingaggio.

Nella fase di ingaggio si definiscono:

- I costi di un'attività di Penetration Testing.
- Il perimetro dell'attività, ovvero l'insieme degli asset aziendali che saranno oggetto delle analisi.
- La finestra temporale necessaria per completare le analisi: (2 mesi), e la finestra temporale in cui verranno eseguiti i test (dalle 18:00 alle 22:00).
- Gli aspetti legali, come ad esempio la gestione di eventuali dati personali / dati sensibili da parte dell'entità che effettua i test. In questa fase di definiscono anche le regole di ingaggio: un documento dove è evidenziato cosa può fare e cosa non può fare il Pentester (il Pentester è colui che effettua il Test).
- Il tipo di Penetration Testing necessario.



Cyber Secure TECH

1.1 - INGAGGIO
COSTI

I costi di un'attività di Penetration Testing sono spalmati su un arco temporale di 8 settimane nella fascia oraria che va dalle ore 18:00 fino alle ore 22:00 da Lunedì a Venerdì.

COSTI ATTIVITÀ

Security Operation (5 giorni)	**€ 16.000**
Business Continuity Plan (4 giorni)	**€ 12.800**
Monitoring Event (3 giorni)	**€ 16.000**
Incident Response (5 giorni)	**€ 16.000**
Analisi dei Log (5 giorni)	**€ 16.000**
TOTALE	**€ 76.800**

Tariffa oraria 100 euro/h + IVA esclusa
conteggiata per ogni singolo operatore del Team

Cyber Secure TECH

1.1 - INGAGGIO

PERIMETRO ATTIVITÀ

Il perimetro dell'attività, ovvero l'insieme degli asset aziendali che saranno oggetto delle analisi.

Con il panorama delle minacce odierno in continua evoluzione, la maggior parte delle organizzazioni sa che deve adottare misure di sicurezza offensive come i test di penetrazione per rimanere un passo avanti rispetto agli aggressori.

Sulla base della nostra esperienza pluriennale nell'aiutare le organizzazioni a gestire i rischi per la sicurezza in tutta l'azienda, abbiamo compilato una raccolta di strumenti e risorse per i test di penetrazione per prepararti al successo.

In base alle informazioni e i metodi necessari per progettare e gestire un programma efficace di Pen Test, agiremo nel seguente modo:

- Firma dell'NDA (Non Disclosure Agreement) inteso come Accordo di riservatezza
- Autorizzazione ad operare in WHite Box

1.1 - INGAGGIO

ASPETTI LEGALI

Gli aspetti legali, come ad esempio la gestione di eventuali dati personali / dati sensibili da parte dell'entità che effettua i test. In questa fase di definiscono anche le regole di ingaggio: un documento dove è evidenziato cosa può fare e cosa non può fare il Pentester (il Pentester è colui che effettua il Test).

Così come la ISO 9001 detta gli standard per la certificazione di qualità, la 27001 è concepita appositamente per fornire le best-practice per un sistema di gestione della sicurezza delle informazioni sulle piattaforme utilizzate dal business. Similmente, il NIST Cybersecurity Framework comprende una serie di linee guida studiate per mitigare i rischi in tal senso.

A questi si aggiungono i **regolamenti comunitari e le leggi nazionali**. Il Regolamento Dora – entrato in vigore il 16 gennaio 2023 e vincolante a partire dal 17 gennaio 2025 – è incentrato **sull'individuazione e sulla gestione ex ante dei rischi informatici** e di cyber sicurezza al fine di raggiungere un elevato livello di resilienza operativa digitale, attraverso la **definizione dei presidi di gestione del rischio cyber** e con un approccio end-to-end.

"A differenza del **GDPR (General Data Protection Regulation)**, che non impone l'adozione di pratiche di controllo specifiche, lasciando ai Data Protection Officer ampio margine d'azione per scegliere gli strumenti che ritengono più idonei, il Regolamento Dora prevede in modo puntuale attività di vulnerability assessment e penetration test.

Allo stesso modo, la Direttiva NIS 2 **(Network and Information Systems)**, entrata in vigore il 17 gennaio 2023, **introduce una serie di obblighi che le aziende dovranno rispettare** nell'ottica di analizzare e valutare i rischi di sicurezza dei sistemi informativi tramite procedure certificate.

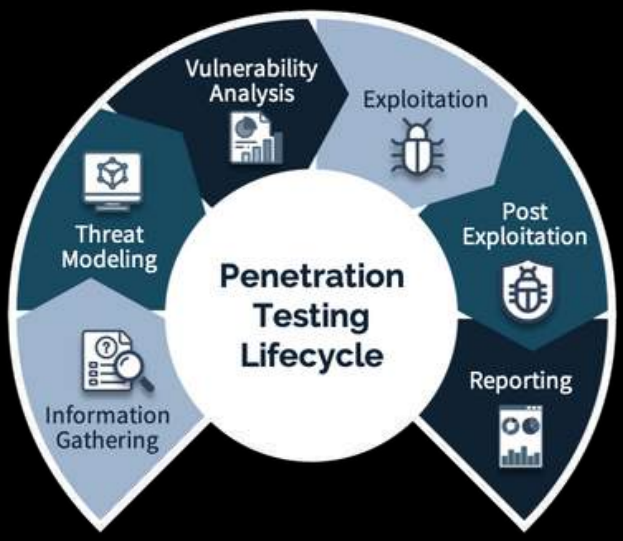
Ma non bisogna dimenticare che in Italia **AgID e ACN** hanno introdotto misure minime per le imprese che vogliono **accedere alle forniture verso la Pubblica Amministrazione**", continua Montrasi. "Per iscriversi al marketplace cloud della PA, per esempio, bisogna superare i test previsti dalle metodologie **OWASP (Open Worldwide Application Security Project)**".

Cyber Secure TECH

1.1 - INGAGGIO
TIPO DI PENTEST

Tipologie di PenTest

Si può definire il Penetration test come una vera e propria simulazione delle stesse strategie d'attacco che un hacker andrebbe a compiere.
In questo modo è possibile individuare per tempo i punti di vulnerabilità del sistema e dimostrare il rischio derivante da una potenziale sottrazione di dati, nonché, quali e quanti danni possano essere inflitti all'infrastruttura in caso di attacco informatico.



Si tratta di vulnerabilità e problematiche che possono derivare:

- dalla progettazione,
- dall'implementazione
- dalla scorretta gestione del sistema

e che è essenziale individuare per evitare che siano sfruttate per compromettere gli obiettivi di sicurezza del sistema e quindi del business. Ci piace chiamarlo più brevemente Pen Test e, come possiamo a questo punto dedurre, questa tipologia di valutazione mirata della sicurezza è dedicata a tutti i software e sistemi informatici che si interfacciano alla rete.

Nel nostro caso utilizzeremo la tipologia White Box Testing

Il White Box Penetration Testing, come si può dedurre, al contrario del Black Box Testing consiste in un'analisi a "scatola aperta". Per l'esecuzione del test, infatti, i tester avranno a disposizione informazioni complete sulla rete e sul sistema, compresi i codici sergente e le credenziali.
In questo modo il test sarà molto più preciso, poiché nella fase di attacco simulato l'operatore potrà concentrarsi meglio sul target specificato, utilizzando il maggior numero possibile di vettori di attacco.

I White Box Testing hanno però i loro svantaggi. Ad esempio, dato il livello di accesso di cui dispone il pentester, può essere necessario del tempo per decidere su quali aree è preferibile concentrarsi. Inoltre questa tipologia di test richiede spesso strumenti sofisticati come debugger e analizzatori di codice, che sono piuttosto costosi.

1.2 - Nozioni Teoriche

1.2 - NOZIONI TEORICHE

FIREWALL

Un firewall è un sistema di sicurezza della rete che monitora e controlla il traffico di rete in base a regole predefinite. Funziona come una barriera tra una rete interna sicura e reti esterne non affidabili, come Internet.

Tipi di Firewall

1. Firewall a filtro di pacchetti: Analizza i pacchetti basandosi su indirizzi IP e numeri di porta.
2. Firewall a ispezione dello stato: Monitora lo stato delle connessioni attive.
3. Firewall di applicazione: Esamina il contenuto dei pacchetti per applicazioni specifiche.
4. Firewall di nuova generazione (NGFW): Combina funzionalità avanzate come ispezione approfondita dei pacchetti e prevenzione delle intrusioni.

Funzionalità Principali

- Filtraggio dei Pacchetti: Blocca o permette il traffico basato su regole.
- NAT (Network Address Translation): Nasconde gli indirizzi IP interni.
- VPN (Virtual Private Network): Crea connessioni sicure tra reti o dispositivi remoti.
- Controllo delle Applicazioni: Regola l'uso delle applicazioni sulla rete.

Vantaggi

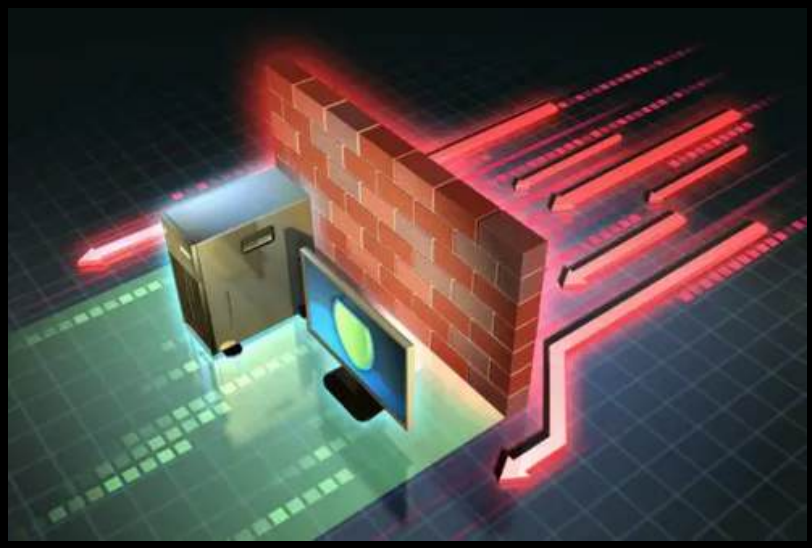
- Protezione da accessi non autorizzati
- Monitoraggio del traffico
- Gestione delle minacce
- Implementazione di politiche di sicurezza

Limitazioni

- Non proteggono da minacce interne
- Richiedono configurazione e manutenzione costante
- Non proteggono da tutte le tipologie di attacchi

Conclusione

I firewall sono essenziali per la sicurezza di rete, ma devono essere parte di una strategia di sicurezza più ampia che include altre misure come antivirus e crittografia.



Cyber Secure TECH

1.2 - NOZIONI TEORICHE

NMAP

Nmap (Network Mapper) è uno strumento di scansione delle reti utilizzato per la sicurezza informatica e l'amministrazione di rete. Permette di scoprire host e servizi su una rete, creando una mappa della rete.

Funzionalità Principali

1. Scansione degli Host: Identifica dispositivi attivi.
2. Rilevamento dei Servizi: Identifica servizi e versioni dei software in esecuzione.
3. Rilevamento del Sistema Operativo: Determina il sistema operativo degli host.
4. Scansione delle Porte: Verifica lo stato delle porte (aperte, chiuse, filtrate).
5. Nmap Scripting Engine (NSE): Esegue script per scansioni avanzate e rilevamento vulnerabilità.

Modalità di Scansione

1. TCP SYN Scan: Scansione stealth che non stabilisce una connessione completa.
2. TCP Connect Scan: Stabilisce una connessione completa, più facile da rilevare.
3. UDP Scan: Scansione delle porte UDP, più lenta.
4. ACK Scan: Determina se le porte sono filtrate o non filtrate.

Vantaggi

- Versatilità: Ampia gamma di funzionalità.
- Facilità d'Uso: Molte opzioni configurabili.
- Supporto Comunitario: Aggiornamenti regolari dalla comunità open source.

Limitazioni

- Rilevabilità: Alcune scansioni possono essere rilevate.
- Tempo di Scansione: Scansioni approfondite possono richiedere molto tempo.
- Autorizzazioni: Alcune scansioni richiedono privilegi elevati.

Conclusione

Nmap è uno strumento essenziale per la mappatura delle reti e la sicurezza informatica, utilizzato per identificare dispositivi, servizi e vulnerabilità. Deve essere utilizzato in modo etico e legale.

Cyber Secure TECH

1.2 - NOZIONI TEORICHE
LA VULNERABILITA'

Una vulnerabilità è una debolezza o falla in un sistema informatico, software, hardware, o rete che può essere sfruttata da un attaccante per ottenere accesso non autorizzato, compromettere il sistema, o causare danni. Le vulnerabilità possono derivare da errori di progettazione, implementazione, configurazione o aggiornamento del sistema.

Tipi Comuni di Vulnerabilità

1. Vulnerabilità Software:
   - Buffer Overflow: Eccesso di dati che supera la capacità di memoria riservata, permettendo l'esecuzione di codice arbitrario.
   - SQL Injection: Inserimento di codice SQL malevolo attraverso input utente non validato, che può manipolare il database.
2. Vulnerabilità di Configurazione:
   - Configurazioni Predefinite Insecure: Utilizzo di impostazioni di default che non sono sicure.
   - Permessi Impropri: Assegnazione inadeguata di permessi di accesso agli utenti.
3. Vulnerabilità di Rete:
   - Man-in-the-Middle (MitM): Intercettazione e alterazione del traffico tra due parti comunicanti.
   - Denial of Service (DoS): Sovraccarico di un sistema con traffico eccessivo, rendendolo inaccessibile agli utenti legittimi.

Impatto delle Vulnerabilità

- Accesso Non Autorizzato: Gli attaccanti possono ottenere accesso a dati sensibili o sistemi interni.
- Compromissione del Sistema: Esecuzione di codice malevolo, installazione di malware.
- Perdita di Dati: Furto, alterazione o cancellazione di dati importanti.
- Interruzione dei Servizi: Rendere i servizi indisponibili o degradare le loro prestazioni.

Gestione delle Vulnerabilità

- Scansione e Monitoraggio: Utilizzo di strumenti per rilevare vulnerabilità note.
- Patch e Aggiornamenti: Applicazione regolare di patch e aggiornamenti di sicurezza.
- Configurazione Sicura: Implementazione di best practice per configurazioni sicure.
- Formazione: Educazione degli utenti e degli amministratori sulla sicurezza informatica.

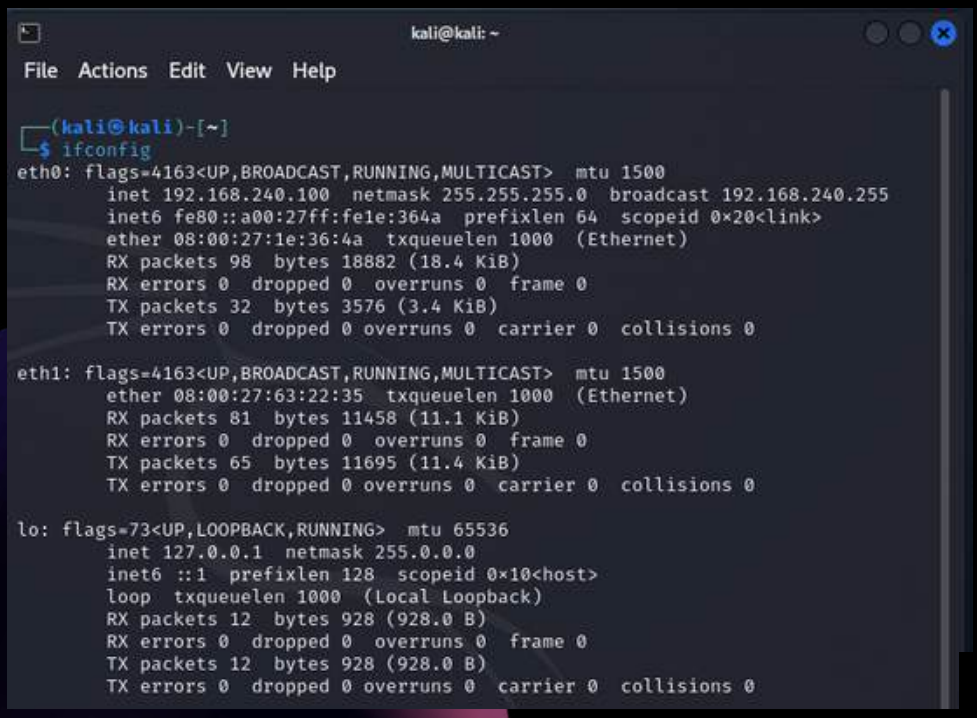
Conclusione

Le vulnerabilità sono punti deboli che possono essere sfruttati per attaccare sistemi informatici. La gestione proattiva delle vulnerabilità è essenziale per mantenere la sicurezza e l'integrità dei sistemi.

1.3 - Configurazione VM

CONFIGURAZIONE IP-KALI LINUX

- **Aprire un terminale di comando**: Avviamo Kali Linux e apriamo un terminale di comando.
- **Accedere al file di configurazione di rete**: Digitiamo sudo nano /etc/network/interfaces e premiamo Invio. Questo comando ci permetterà di accedere al file che contiene la configurazione di rete della nostra macchina.
- **Modificare l'indirizzo IP**: Nel file che si aprirà, cerchiamo la riga che contiene l'indirizzo IP attuale. Modifichiamolo con l'indirizzo IP richiesto.
- **Salvare le modifiche**: Per salvare le modifiche, premiamo i tasti Control + O, poi premiamo Invio e per chiudere l'editor nano, premiamo i tasti Control + X.
- **Riavviare la macchina**: Digitiamo reboot nel terminale e premiamo Invio per riavviare la macchina.
- **Verificare la modifica dell'indirizzo IP**: Dopo il riavvio, riapriamo un terminale di comando e digitiamo ifconfig. Questo comando ci mostrerà la configurazione della rete attuale. Verifichiamo che l'indirizzo IP sia stato modificato correttamente.



Cyber Secure TECH

CONFIGURAZIONE IP-WINDOWS XP

- **Aprire il Pannello di Controllo:** Clicchiamo su "Start" nell'angolo in basso a sinistra del desktop e selezioniamo “Pannello di Controllo”.

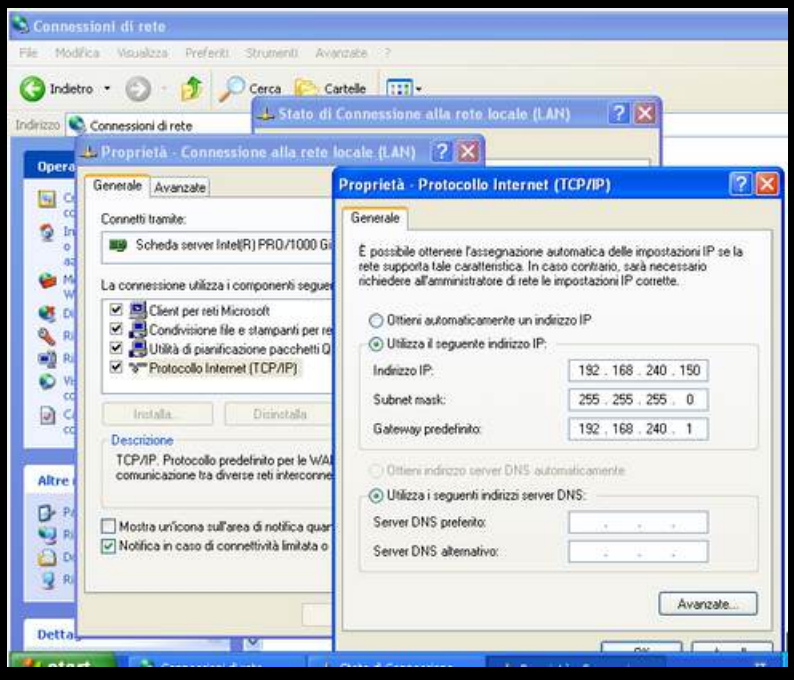
- **Accedere alle Connessioni di Rete:** Nel Pannello di Controllo, doppio clic su "Connessioni di rete e Internet" e quindi su “Connessioni di rete”

- **Selezionare la Connessione di Rete:** clicchiamo su "Connessione alla rete locale (LAN)" e con il tasto destro selezioniamo "Proprietà" dal menu contestuale.

- **Accedere alle Proprietà del Protocollo Internet (TCP/IP):** Nella scheda "Generale" della finestra Proprietà della connessione, scorriamo l'elenco e troviamo "Protocollo Internet (TCP/IP)", lo selezioniamo e clicchiamo su “Proprietà”.

- **Modificare l'Indirizzo IP:** Nella finestra Proprietà del Protocollo Internet (TCP/IP), selezioniamo “Utilizza il seguente indirizzo IP”. Questa opzione consente di inserire manualmente un indirizzo IP, una Subnet mask e un Gateway predefinito.
- I**nserire i seguenti dettagli**:
- Indirizzo IP: Inserisci l'indirizzo IP desiderato. Assicurati che l'indirizzo sia univoco e non sia già in uso nella rete.
- Subnet mask: Di solito è "255.255.255.0" per le reti locali standard, ma potrebbe variare in base alla configurazione della rete.
- Gateway predefinito: Inserisci l'indirizzo IP del router o del gateway della rete.

- **Salva le Modifiche**: Dopo aver inserito le informazioni necessarie, fai clic su "OK" per chiudere la finestra Proprietà del Protocollo Internet (TCP/IP). Fai clic su "Chiudi" nella finestra delle Proprietà della connessione di rete.

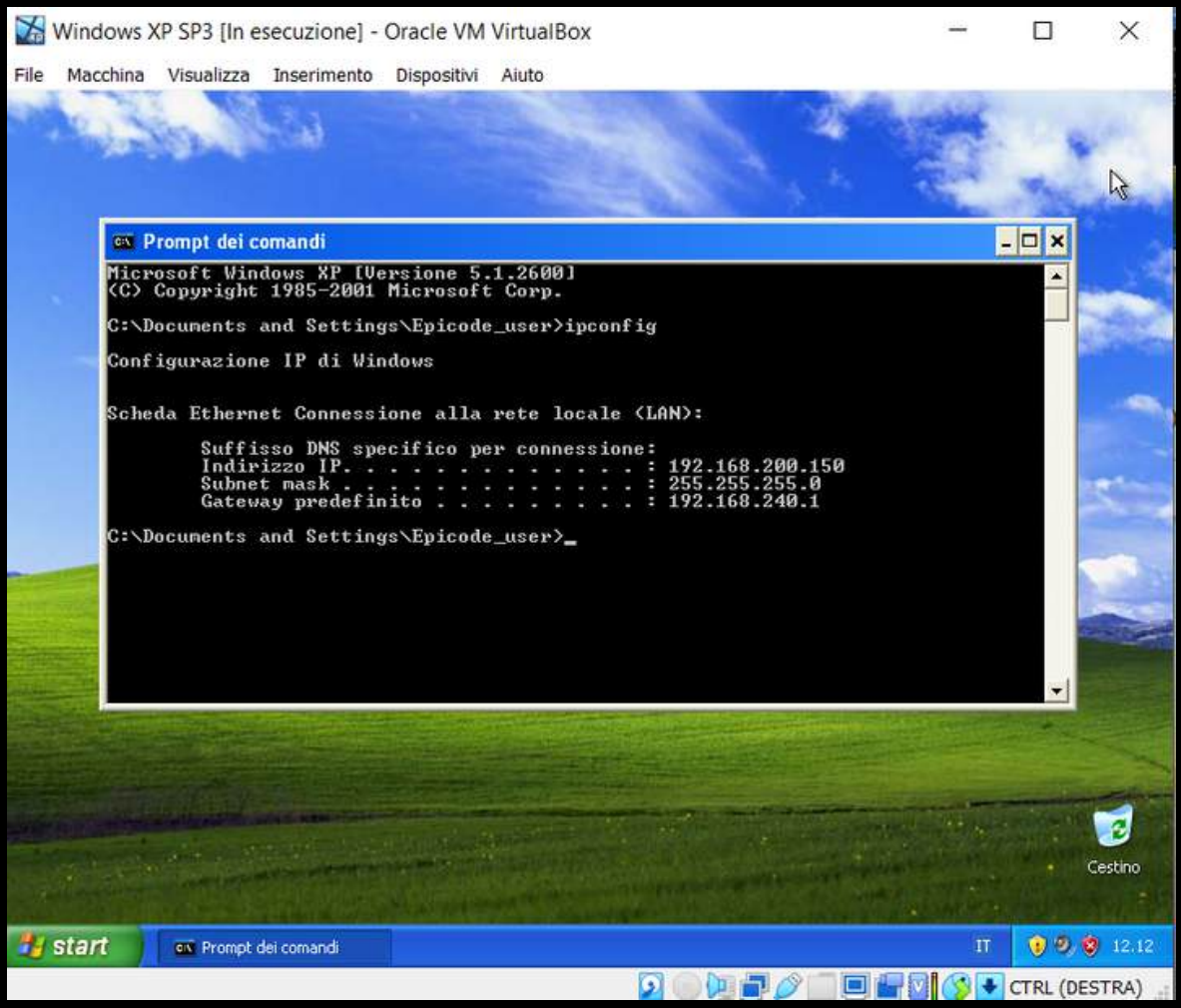


Cyber Secure TECH

VERIFICA IP-WINDOWS XP

- **Riavviare**: Riavvia la connessione di rete o il computer per applicare le modifiche.

- **Verificare la modifica dell'indirizzo IP**: Puoi verificare l'indirizzo IP configurato aprendo il Prompt dei comandi (Start > Esegui > digita "cmd" e premi Invio) e digitando "ipconfig" seguito da Invio.



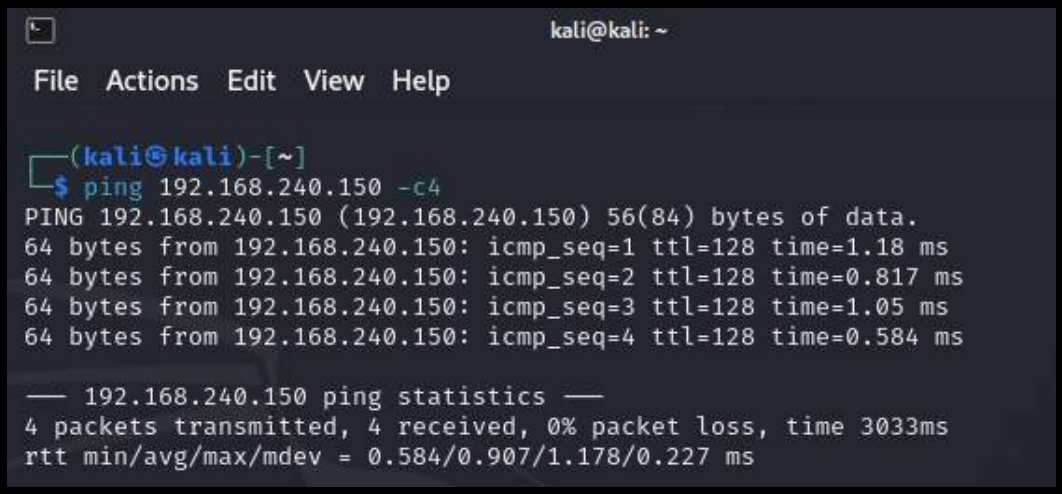
Cyber Secure TECH

VERIFICA COMUNICAZIONE

- **Assicurarsi che entrambe le macchine siano avviate**: Avviamo sia la macchina virtuale Kali Linux che Windows XP.

- **Eseguire il comando ping**: Apriamo un terminale su Kali Linux e digitiamo il comando ping seguito dall'indirizzo IP della macchina Metasploitable e lo switch -c4 per specificare il numero di pacchetti da inviare e premiamo invio.

- **Interpretare i risultati del ping**: Se la configurazione è corretta, vedremo una serie di righe che indicano il tempo impiegato per l'invio di ogni pacchetto, il numero di pacchetti inviati, ricevuti e persi. Se vediamo una risposta simile alla figura a destra, con il 100% dei pacchetti inviati e 0 pacchetti persi, significa che le due macchine possono comunicare correttamente tra loro.



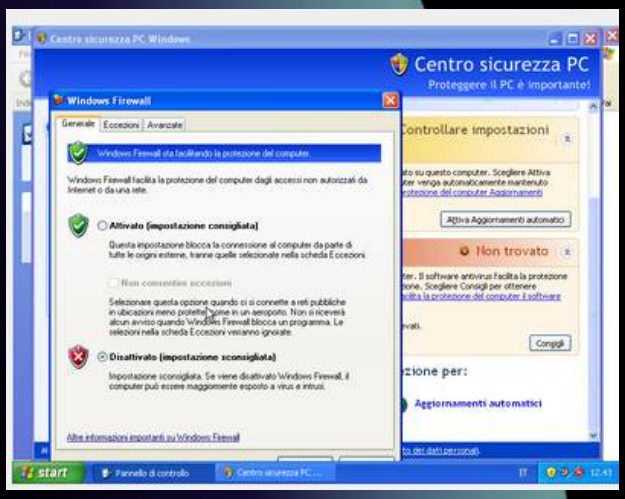
Cyber Secure TECH

1.4 - Nmap & Nessus scan

SCANSIONE DI WINDOWS

FIREWALL DISATTIVATO

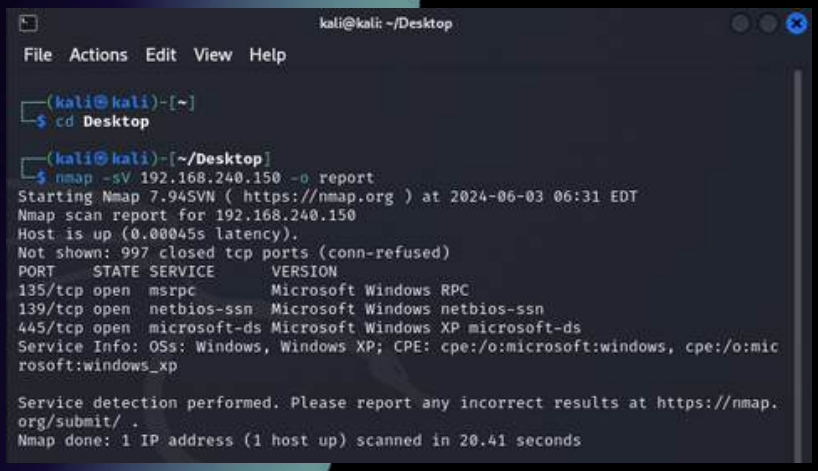
Prima di eseguire la scansione, disattiviamo il firewall su Windows XP.



Successivamente, sulla macchina Kali, utilizziamo il comando:

nmap -sV "indirizzo IP target" -o "nome del file output"

Questo comando permette di verificare lo stato e la versione delle porte, salvando i risultati in un file di testo.

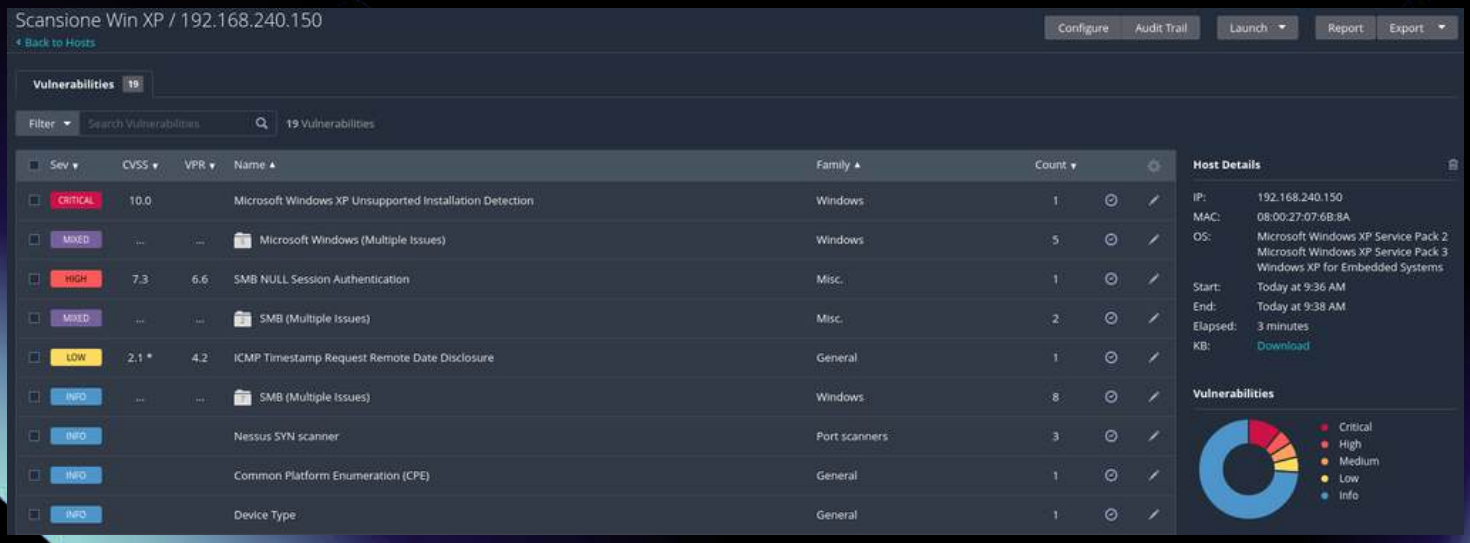


Dopo la scansione, osserviamo che le porte 135, 139 e 445 sono aperte.
Il servizio MSRPC (Microsoft Remote Procedure Call) è un protocollo di comunicazione utilizzato per permettere ai programmi di eseguire procedure su macchine remote come se fossero locali. È una implementazione dei protocolli RPC (Remote Procedure Call) di Microsoft, che consente la comunicazione tra diverse applicazioni su una rete.

Cyber Secure TECH

SCANSIONE NESSUS

Abbiamo effettuato una scansione basic con il tool di Vulnerability Scanning Nessus, in modo da avere una panoramica generale ed abbiamo riscontrato che i servizi attivi sulla porta 135 e 139 , quindi rispettivamente quello di Microsoft RPC e NetBios sono stati catalogati come CRITICAL; mentre sulla porta 445 il servizio Microsoft DS è catalogato come HIGH.



Cyber Secure TECH

PORTA 135 - MSRPC

Il servizio **MSRPC** (Microsoft Remote Procedure Call) è un **protocollo di comunicazione** utilizzato per permettere ai programmi di eseguire procedure su macchine remote come se fossero locali. È una implementazione dei protocolli RPC (Remote Procedure Call) di Microsoft, che consente la comunicazione tra diverse applicazioni su una rete.

Vulnerabilità e Sicurezza

MSRPC **può essere un vettore di attacco** se non è adeguatamente protetto. Alcuni attacchi noti includono:

- Exploits di Buffer Overflow: Vulnerabilità che consentono a un attaccante di eseguire codice arbitrario.
- Attacchi DoS (Denial of Service): Attacchi che possono rendere il servizio non disponibile.
- Rilevamento delle Porte: Gli attaccanti possono rilevare le porte aperte e tentare di sfruttare i servizi esposti.

Protezione del Servizio MSRPC

- Firewall: Configurare correttamente i firewall per bloccare l'accesso non autorizzato.
- Aggiornamenti di Sicurezza: Applicare regolarmente patch e aggiornamenti di sicurezza.
- Autenticazione e Autorizzazione: Utilizzare meccanismi di autenticazione robusti e controllare l'accesso ai servizi.

PORTA 139 - NETBIOS-SSN

NetBIOS-SSN (NetBIOS Session Service) è una delle tre componenti del protocollo NetBIOS (Network Basic Input/Output System), utilizzato per la comunicazione tra applicazioni su diverse macchine in una rete locale (LAN). NetBIOS-SSN è specificamente responsabile della gestione delle sessioni di comunicazione tra computer.

Vulnerabilità e Sicurezza

NetBIOS-SSN, come altri servizi di rete, **può essere soggetto a vari tipi di attacchi** se non adeguatamente protetto:

- Enumerazione di Rete: Gli attaccanti possono utilizzare strumenti per enumerare (scoprire) le risorse di rete, gli utenti e i gruppi su una rete locale.
- Accesso Non Autorizzato: Configurazioni deboli o mancanti possono permettere l'accesso non autorizzato a risorse condivise.
- Attacchi DoS (Denial of Service): Gli attaccanti possono tentare di interrompere il servizio saturando la rete con richieste.

Misure di Protezione

- Firewall: Configurare il firewall per limitare l'accesso alla porta 139, consentendo solo il traffico necessario.
- Disabilitare NetBIOS su TCP/IP: Su reti moderne, può essere utile disabilitare NetBIOS su TCP/IP se non è necessario.
- Aggiornamenti di Sicurezza: Assicurarsi che tutti i sistemi siano aggiornati con le ultime patch di sicurezza.
- Configurazioni di Sicurezza: Implementare politiche di sicurezza robuste, come l'utilizzo di password complesse e l'accesso limitato alle risorse condivise.

Cyber Secure TECH

PORTA 445 - MICROSOFT DS

Microsoft DS (Directory Services) è un **protocollo di rete** utilizzato principalmente per la condivisione di file, stampanti e servizi di directory su reti basate su Windows. Si basa sul protocollo SMB (Server Message Block), che è stato sviluppato da Microsoft per facilitare la condivisione di risorse in una rete.

Vulnerabilità Comuni

- Attacchi SMB: Exploit come EternalBlue, che è stato utilizzato nel ransomware WannaCry, sfruttano vulnerabilità nel protocollo SMB.
- Accesso Non Autorizzato: Configurazioni errate possono permettere accessi non autorizzati a file e risorse di rete.
- Attacchi di Forza Bruta: Gli attaccanti possono tentare di indovinare le credenziali di accesso utilizzando attacchi di forza bruta.

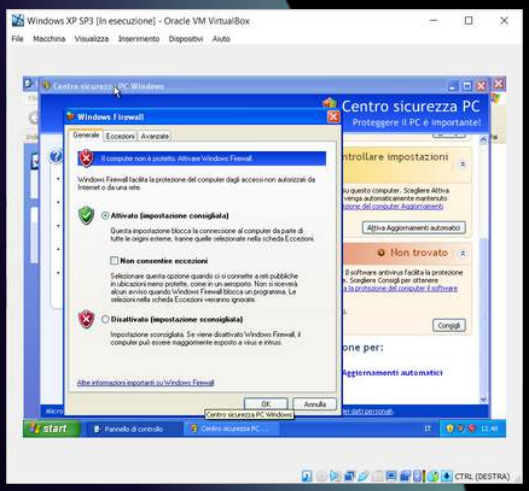
Misure di Protezione

- Autenticazione: Utilizza meccanismi di autenticazione per verificare l'identità degli utenti che accedono alle risorse condivise.
- Crittografia: Può utilizzare la crittografia per proteggere i dati durante il transito.
- Firewall: È importante configurare correttamente i firewall per proteggere i servizi esposti sulle porte 139 e 445.
- Patch e Aggiornamenti: Applicare regolarmente patch di sicurezza e aggiornamenti per correggere vulnerabilità note.

Cyber Secure TECH

SCANSIONE DI WINDOWS FIREWALL ATTIVATO

Prima di eseguire la scansione, attiviamo il firewall su Windows XP.



Il risultato della scansione ci riporta che la macchina o non è accesa, oppure se è accesa sta bloccando l'host discovery di nmap. Ci consiglia quindi di provare con il parametro –Pn. La situazione è piuttosto chiara, il Firewall sta bloccando il traffico in entrata con protocollo ICMP (il ping). Proviamo a sfruttare lo switch –Pn per evitare il ping e passare direttamente alla scansione dei servizi

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.92 ( https://nmap.org )
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.51 seconds
```

Successivamente, avviamo un'altra scansione sulla macchina Kali utilizzando il comando:

nmap -sV "indirizzo IP target" -Pn

Nel report, notiamo che la macchina Kali non ha ricevuto nessuna risposta dalle porte scansionate, poiché sono filtrate dal firewall che blocca le richieste esterne.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.240.150 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 09:15 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00053s latency).
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:07:6B:8A (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.68 seconds
```

- -sV: Effettua il rilevamento della versione dei servizi in esecuzione sulle porte aperte.
- 192.168.240.150: Specifica l'indirizzo IP del bersaglio da scansionare.
- -Pn: Disabilita il ping al bersaglio. Questo è utile quando si sospetta che il ping ICMP sia bloccato dal firewall.

Cyber Secure TECH

1.5 Conclusioni

DIFFERENZE TRA LE DUE SCANSIONI EFFETTUATE

Nella prima scansione effettuata con il **firewall disattivato** sulla macchina Windows XP, è possibile eseguire liberamente una scansione dei servizi attivi sulle porte dell'IP di destinazione.

Tuttavia in una seconda scansione, **attivando il firewall**, si notano due principali differenze:

1. Il firewall blocca la scansione esterna verso i servizi disponibili, mostrando principalmente porte filtrate. Di conseguenza, non è possibile determinare quali porte siano effettivamente aperte e quali chiuse né identificare i servizi attivi su di esse.
2. È necessario aggiungere l'opzione “-Pn” per bypassare il blocco del ping ICMP, probabilmente imposto da una regola del firewall. Questo permette di proseguire con la scansione senza che il ping iniziale venga bloccato e di visualizzare lo stato dell’host attivo.

Questi cambiamenti evidenziano l'efficacia del firewall nel limitare le informazioni accessibili ai tentativi di scansione dall'esterno, migliorando la sicurezza della rete.

Cyber Secure TECH


Giorno2
Business continuity &
disaster recovery

INDICE
GIORNO 2

S9_L2

Giorno 2 – Business Continuity & Disaster Recovery

Cyber Secure TECH

TRACCIA
GIORNO 2

Durante la lezione teorica, abbiamo affrontato gli argomenti riguardanti la business continuity e disaster recovery. Nell' esempio pratico di oggi, ipotizziamo di essere stati assunti per valutare quantitativamente l'impatto di un determinato disastro su un asset di una compagnia.
Con il supporto dei dati presenti nelle tabelle che seguono, calcolare la perdita annuale che s ubirebbe la compagnia nel caso di:

1. Inondazione sull'asset «edificio secondario»
2. Terremoto sull'asset «datacenter»
3. Incendio sull'asset «edificio primario»
4. Inondazione sull'asset «edificio primario e secondario»
5. Terremoto sull'asset «edificio primario»

Cyber Secure TECH

2.1 - Business Continuity Plan

2.1 - BUSINESS CONTINUITY & DISASTER RECOVERY

Durante la lezione teorica, abbiamo affrontato gli argomenti riguardanti la business continuity e disaster recovery.

ASSET	VALORE
Edificio primario	350.000€
Edificio secondario	150.000€
Datacenter	100.000€

EVENTO	ARO
Terremoto	1 volta ogni 30 anni
Incendio	1 volta ogni 20 anni
Inondazione	1 volta ogni 50 anni

EXPOSURE FACTOR	Terremoto	Incendio	Inondazione
Edificio primario	80%	60%	55%
Edificio secondario	80%	50%	40%
Datacenter	95%	60%	35%

Nell'esempio pratico di oggi, ipotizziamo di essere stati assunti per valutare quantitativamente l'impatto di un determinato disastro su un asset di una compagnia. Con il supporto dei dati presenti nelle tabelle che seguono, calcolare la perdita annuale che s ubirebbe la compagnia nel caso di:

- Inondazione sull'asset «edificio secondario»
- Terremoto sull'asset «datacenter»
- Incendio sull'asset «edificio primario»
- Incendio sull'asset «edificio secondario»
- Inondazione sull'asset «edificio primario»
- Terremoto sull'asset «edificio primario»

Cyber Secure TECH

2.1 - BUSINESS CONTINUITY & DISASTER RECOVERY

Pianificazione e scopo: Fase 1.1

Analisi strutturata dell'organizzazione e del suo business

Un'analisi strutturata dell'organizzazione e del business dell'organizzazione: un'analisi strutturata dell'organizzazione e del business è il primo passo nella stesura di un piano di continuità.

In questa fase, lo scopo è quello di dettagliare e «mappare» i dipartimenti interni di una compagnia e gli individui con i servizi critici erogati dalla compagnia stessa. Infatti, in ottica di evento catastrofico, un piano di continuità ben strutturato dovrà, come prima priorità, ridurre gli impatti su quelli che sono i «servizi core», ovvero i servizi principali erogati dalla compagnia.

Come abbiamo visto nelle unità precedenti per l'implementazione delle «remediation action», si riprende anche in questo contesto il concetto di «priorità»: gli asset critici, relativi al business hanno sempre la priorità.

Pianificazione e scopo: Fase 1.2

Creazione di un Team

La creazione di un team / gruppo di lavoro responsabile del BCP che deve essere approvato dai dirigenti della compagnia stessa: il secondo step nello sviluppo di un piano d'azione per la continuità del business è l'identificazione delle persone responsabili del business continuity plan (BCP).

Questa fase è molto importante, in quanto bisogna assicurare che tutti i dipartimenti di una compagnia siano consapevoli dell'esistenza di un piano di continuità. Pertanto, nella pianificazione del team di lavoro bisognerà includere:

- Un rappresentante di ogni dipartimento dell'organizzazione che si occupa di erogare servizi critici;
- Un esperto di servizi IT (information technology) con competenze tecniche nelle aree coperte dal BCP;
- Un membrodel team di Cyber Security, che abbia competenze del processo BCP;
- Un membrodel team della sicurezza fisica; Cyber Security & Ethical Hacking Business continuity plan Dei membri del team legale, che abbiano competenze sulle regolamentazioni, leggi e contratti in essere;
- Dei membri del team delle risorse umane (HR– human resources), per la gestione di eventuali impatti sullo staff, o su impiegati;
- Un rappresentante dei dirigenti che abbia potere decisionale, al fine di definire le priorità ed allocare eventualmente risorse.

Pianificazione e scopo: Fase 1.3

Valutazione delle risorse ed asset disponibili

Una valutazione delle risorse ed asset disponibili che saranno incluse nelle attività di business continuity: una volta che il team responsabile del BCP è stato definito, è il momento di definire le risorse richieste dal BCP.
Si possono definire le risorse definite per le tre fasi di seguito del BCP:

1) Sviluppo del BCP: (ovvero il costo) è perlopiù imputabile a capitale umano quale il team coinvolto nel processo di BCP ed eventualmente il costo dello staff esterno richiesto a supporto (se necessario).

2) Test, manutenzione e training per gli impiegati: il BCP deve essere testato, manutenuto, ma soprattutto bisogna organizzare delle sessioni di training / lezioni per gli impiegati al fine di mostrare il funzionamento del BCP.

3) Implementazione del BCP: infine, in caso di disastro, il BCP deve essere attuato il che richiede non solo capitale umano, ma anche un uso di risorse e mezzi. In questa fase, è molto probabile che per un periodo limitato una buona porzione della compagnia sia impegnata nell'implementazione del piano di continuità.

Pianificazione e scopo: Fase 1.4

Analisi delle leggi e regolamentazioni

Un'analisi delle leggi e regolamentazioni che la compagnia deve rispettare. Ad esempio, potrebbero essere in vigore delle leggi che stabiliscono quali servizi devono essere sempre erogati anche in situazioni critiche da una data compagnia: capita piuttosto frequentemente, che le compagnie sono in qualche modo legate a leggi statali o regolamentazioni che governano l'implementazione dei piani di continuità.

Questo succede spesso nel mercato dei «Financial Services», ovvero il mercato di quelle compagnie che erogano servizi finanziari come banche ed assicurazioni. In questi casi, le regolamentazioni pongono dei limiti o degli obblighi nello sviluppo dei piani di continuità operativa, ed è di conseguenza fondamentale capire il contesto giuridico nel quale si posiziona la compagnia al fine di sviluppare un piano che sia in linea con le leggi e le regolamentazioni in vigore.

Business Impact Assessment: Fase 2.0

Business Impact Analysis (BIA)

Una volta completato il primo step della pianificazione, è tempo di affrontare il Business impact analysis (BIA), ovvero l'analisi degli impatti sul business.

Il BIA ha lo scopo principale di identificare le risorse critiche di una compagnia e le potenziali minacce alle quali esse sono esposte. Inoltre, il BIA ha lo scopo di misurare la probabilità che tali minacce possano verificarsi e l'impatto che esse potrebbero avere sul business.

Il BIA e conseguentemente la sua «misurazione» può seguire due approcci:

1) Qualitativo: per il calcolo degli impatti di determinate minacce sul business NON si prendono in considerazione parametri misurabili, o numerici, ma bensì l'analisi è guidata da fattori non numerici.

2) Quantitativo: il calcolo degli impatti sul business prende in considerazione solamente parametri numerici o quantificabili

Cyber Secure TECH

Business Impact Assessment: Fase 2.1
Identificazione delle priorità

Il primo task da eseguire quando ci si prepara ad affrontare un **BIA** è l'identificazione delle priorità del business. Questo fattore dipende ovviamente da quello che è lo scopo principale, o il business principale della compagnia.

Da un punto di vista qualitativo, si potrebbero, di fatto, identificare le priorità in base alla loro criticità relativamente al business– dove agli asset a supporto del business viene assegnata una priorità superiore.

Da un punto di vista quantitativo, si potrebbe invece creare una lista contenente tutti gli asset della compagnia ed assegnare ad ognuno di essi un valore monetario, chiamato «asset value» (AV) e successivamente assegnare una priorità in base al valore.

Cyber Secure TECH

Business Impact Assessment: Fase 2.2
Identificazione dei rischi

Identificazione dei rischi: una volta completata la fase di identificazione delle priorità, bisogna stimare il rischio che impatterebbe l'organizzazione in caso di disastro.
Possiamo dividere i rischi in due grosse categorie:

1) Disastri naturali: ricadono all'interno di questa categoria tutti quei fenomeni che non sono causati direttamente dall'uomo in prima persona, come ad esempio terremoti, maremoti, valanghe, eruzioni vulcaniche.

2) Disastri causati dall'uomo: in maniera complementare sono inclusi nei disastri causati dall'uomo tutti quei fenomeni che vedono l'uomo commettere un'azione in prima persona come atti terroristici, esplosioni etc.

Cyber Secure TECH

Business Impact Assessment: Fase 2.3
Valutazione della probabilità

Una volta identificati i rischi che possono impattare sull'organizzazione, ad ognuno di essi si associa la probabilità che l'evento si verifichi. Se la probabilità è stimata in numero di volte che l'evento si è verificato nel corso di un anno, si parla di «Annualized Rate of Occurrence» (ARO), ovvero tasso annuale di occorrenza.

I dati storici e le statistiche messe a disposizione degli enti pubblici possono sicuramente supportare la valutazione delle probabilità per quanto riguarda i disastri naturali.

Business Impact Assessment: Fase 2.4
Valutazione degli impatti

A valle dell'identificazione dei rischi e della probabilità che essi si verifichino, si può procedere con la fase di valutazione degli impatti.

Il risultato della fase di valutazione degli impatti è una misura qualitativa (basso, medio, alto) o quantitativa (e quindi espressa in forma monetaria) degli impatti sul business legati ad un determinato evento.

Business planning: Fase 3

Le prime due fasi del BCP si focalizzano sulla pianificazione del BCP esull'identificazione delle priorità e dei rischi per il business. La fase del continuity planning ha invece lo scopo di sviluppare ed implementare una strategia per la riduzione dell'impatto dei rischi sugli asset protetti. Possiamo identificare all'interno della fase di continuity planning, le seguenti sottofasi:

1) Sviluppo della strategia: lo sviluppo della strategia è un'attività complementare all'identificazione delle priorità, discussa nella fase di BIA. Infatti, se nella BIA si identificano rischi ed asset prioritari, nella fase di sviluppo strategia si decidono i rischi che verranno gestiti all'interno del BCP. In questa fase il management deciderà quali rischi potrebbero essere accettabili, e quali invece no, quali rischi sono da evitare e quali invece inserire all'interno del BCP.

2) Stesura dei processi: all'interno di questa fase vengono dettagliati i processi e le procedure da seguire per la salvaguardia degli asset critici: personale, edifici ed infrastrutture. È bene ricordare che le persone sono sempre «l'asset» più significativo di una compagnia e pertanto devono essere dettagliati i processi per assicurare l'incolumità durante un'emergenza.

Approvazione ed implementazione: Fase 4

Una volta completate le fasi precedenti, è il momento di sottoporre il piano all'attenzione della dirigenza per revisione ed approvazione, prima di passare alla fase di implementazione, dove il team responsabile del BCP deve assicurarsi che tutte le risorse necessarie siano disponibili e che è stato organizzato, o erogato un piano di training per tutti gli impiegati che prendono attivamente parte al BCP.

Infine, tutte le fasi precedenti devono essere ampiamente documentate e rese disponibili per eventuale consultazione da parte degli impiegati.

2.2 - CASI STUDIO 1-5

2.2 - CASO STUDIO 1

INONDAZIONE SULL'ASSET «EDIFICIO SECONDARIO»

ASSET	VALORE
Edificio primario	350.000€
Edificio secondario	150.000€
Datacenter	100.000€

EVENTO	ARO
Terremoto	1 volta ogni 30 anni
Incendio	1 volta ogni 20 anni
Inondazione	1 volta ogni 50 anni

EXPOSURE FACTOR	Terremoto	Incendio	Inondazione
Edificio primario	80%	60%	55%
Edificio secondario	80%	50%	40%
Datacenter	95%	60%	35%

FORMULARIO CALCOLI

ARO: 1 / anni

PERDITA MONETARIA: **SLE = AV x EF**

PERDITA ARCO TEMPORALE: ALE = SLE x ARO

AV: ASSET VALUE, CHE PER L'ASSET EDIFICIO SECONDARIO È PARI A 150.000€

EF: EXPOSURE FACTOR, CHE PER LA COPPIA EDIFICIO SECONDARIO/INONDAZIONE È PARI AL 40%

SLE = 150.000€ X 0,40 = 60.000€

ARO PER L'EVENTO «INONDAZIONE» È 1 VOLTA OGNI 50 ANNI, CHE EQUIVALE A 0,02 VOLTE / ANNO.

ALE = SLE X ARO = 60.000€ X 0,02 = 1200€

LEGENDA

AV - Valore Asset

EF - Exposure Factor (Fattore di Esposizione)

SLE - Single Loss Expectancy (Aspettativa perdita singola)

ARO - N°volte evento in un anno

ALE - Annualized Loss Expectancy (Aspettativa perdita annualizzata)

Cyber Secure TECH

2.3 - CASO STUDIO 2

TERREMOTO SULL'ASSET «DATACENTER»

ASSET	VALORE
Edificio primario	350.000€
Edificio secondario	150.000€
Datacenter	100.000€

EVENTO	ARO
Terremoto	1 volta ogni 30 anni
Incendio	1 volta ogni 20 anni
Inondazione	1 volta ogni 50 anni

EXPOSURE FACTOR	Terremoto	Incendio	Inondazione
Edificio primario	80%	60%	55%
Edificio secondario	80%	50%	40%
Datacenter	95%	60%	35%

FORMULARIO CALCOLI

ARO: 1 / anni

PERDITA MONETARIA: **SLE = AV x EF**

PERDITA ARCO TEMPORALE: ALE = SLE x ARO

AV: 100.000€

EF: 95%

SLE = 100.000€ X 0,95 = 95.000€

ARO: 1/30=0.033

ALE = SLE X ARO = 95.000€ X 0,033 = 3135€

LEGENDA

AV - Valore Asset

EF - Exposure Factor (Fattore di Esposizione)

SLE - Single Loss Expectancy (Aspettativa perdita singola)

ARO - N°volte evento in un anno

ALE - Annualized Loss Expectancy (Aspettativa perdita annualizzata)

Cyber Secure TECH

2.4 - CASO STUDIO 3
INCENDIO SULL'ASSET «EDIFICIO PRIMARIO»

ASSET	VALORE
Edificio primario	350.000€
Edificio secondario	150.000€
Datacenter	100.000€

EVENTO	ARO
Terremoto	1 volta ogni 30 anni
Incendio	1 volta ogni 20 anni
Inondazione	1 volta ogni 50 anni

EXPOSURE FACTOR	Terremoto	Incendio	Inondazione
Edificio primario	80%	60%	55%
Edificio secondario	80%	50%	40%
Datacenter	95%	60%	35%

FORMULARIO CALCOLI

ARO: 1 / anni

PERDITA MONETARIA: **SLE = AV x EF**

PERDITA ARCO TEMPORALE: ALE = SLE x ARO

AV: 350.000€

EF: 60%

SLE = 350.000€ X 0,60 = 210.000€

ARO: 1/20= 0.05

ALE = SLE X ARO = 210.000€ X 0,05 = 10.500€

LEGENDA

AV - Valore Asset

EF - Exposure Factor (Fattore di Esposizione)

SLE - Single Loss Expectancy (Aspettativa perdita singola)

ARO - N°volte evento in un anno

ALE - Annualized Loss Expectancy (Aspettativa perdita annualizzata)

Cyber Secure TECH

2.5 - CASO STUDIO 3

INCENDIO SULL'ASSET «EDIFICIO SECONDARIO»

ASSET	VALORE
Edificio primario	350.000€
Edificio secondario	150.000€
Datacenter	100.000€

EVENTO	ARO
Terremoto	1 volta ogni 30 anni
Incendio	1 volta ogni 20 anni
Inondazione	1 volta ogni 50 anni

EXPOSURE FACTOR	Terremoto	Incendio	Inondazione
Edificio primario	80%	60%	55%
Edificio secondario	80%	50%	40%
Datacenter	95%	60%	35%

FORMULARIO CALCOLI

ARO: 1 / anni

PERDITA MONETARIA: **SLE = AV x EF**

PERDITA ARCO TEMPORALE: ALE = SLE x ARO

AV: 100.000€

EF: 50%

SLE = 150.000€ X 0,50 = 75.000€

ARO:1/20 = 0.05

ALE = SLE X ARO = 75.000€ X 0,05 = 3.750€

LEGENDA

AV - Valore Asset

EF - Exposure Factor (Fattore di Esposizione)

SLE - Single Loss Expectancy (Aspettativa perdita singola)

ARO - N°volte evento in un anno

ALE - Annualized Loss Expectancy (Aspettativa perdita annualizzata)

Cyber Secure TECH

2.6 - CASO STUDIO 4

INONDAZIONE SULL'ASSET «EDIFICIO PRIMARIO»

ASSET	VALORE
Edificio primario	350.000€
Edificio secondario	150.000€
Datacenter	100.000€

EVENTO	ARO
Terremoto	1 volta ogni 30 anni
Incendio	1 volta ogni 20 anni
Inondazione	1 volta ogni 50 anni

EXPOSURE FACTOR	Terremoto	Incendio	Inondazione
Edificio primario	80%	60%	55%
Edificio secondario	80%	50%	40%
Datacenter	95%	60%	35%

FORMULARIO CALCOLI

ARO: 1 / anni

PERDITA MONETARIA: **SLE = AV x EF**

PERDITA ARCO TEMPORALE: ALE = SLE x ARO

AV: 350.000€

EF: 55%

ARO: 1/50 = 0.02

SLE = 350.000€ X 0,55 = 192.500€

ALE = SLE X ARO = 192.500€ X 0,02 = 3.850€

LEGENDA

AV - Valore Asset

EF - Exposure Factor (Fattore di Esposizione)

SLE - Single Loss Expectancy (Aspettativa perdita singola)

ARO - N°volte evento in un anno

ALE - Annualized Loss Expectancy (Aspettativa perdita annualizzata)

Cyber Secure TECH

2.7 - CASO STUDIO 5
TERREMOTO SULL'ASSET «EDIFICIO PRIMARIO»

ASSET	VALORE
Edificio primario	350.000€
Edificio secondario	150.000€
Datacenter	100.000€

EVENTO	ARO
Terremoto	1 volta ogni 30 anni
Incendio	1 volta ogni 20 anni
Inondazione	1 volta ogni 50 anni

EXPOSURE FACTOR	Terremoto	Incendio	Inondazione
Edificio primario	80%	60%	55%
Edificio secondario	80%	50%	40%
Datacenter	95%	60%	35%

FORMULARIO CALCOLI

ARO: 1 / anni

PERDITA MONETARIA: **SLE = AV x EF**

PERDITA ARCO TEMPORALE: ALE = SLE x ARO

AV: 350.000€

EF: 80%

SLE = 350.000€ X 0,80 = 280.000€

ARO: 1/30 = 0.033

ALE = SLE X ARO = 280.000€ X 0,033 = 9.240€

LEGENDA

AV - Valore Asset

EF - Exposure Factor (Fattore di Esposizione)

SLE - Single Loss Expectancy (Aspettativa perdita singola)

ARO - N°volte evento in un anno

ALE - Annualized Loss Expectancy (Aspettativa perdita annualizzata)

Cyber Secure TECH

4.CONCLUSIONI

4 - CONCLUSIONI

Il Business Continuity Plan e il Disaster Recovery Plan sono essenziali per garantire la resilienza e la capacità di ripresa delle aziende di fronte a eventi catastrofici come terremoti, inondazioni o incendi. Implementando piani solidi, le aziende possono minimizzare l'interruzione delle operazioni, proteggere i dati cruciali e ridurre i tempi di inattività.

Una preparazione adeguata consente non solo di salvaguardare le risorse fisiche e digitali, ma anche di mantenere la fiducia dei clienti e delle parti interessate.

In definitiva, la capacità di rispondere efficacemente a emergenze garantisce la continuità delle attività aziendali e la stabilità a lungo termine.

Cyber Secure TECH


GIORNO 3
MONITORING EVENT
FROM SIEM

INDICE
GIORNO 3

S9_L3

Giorno 3 - Monitoring from SIEM

Cyber Secure TECH

TRACCIA
GIORNO 3

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.

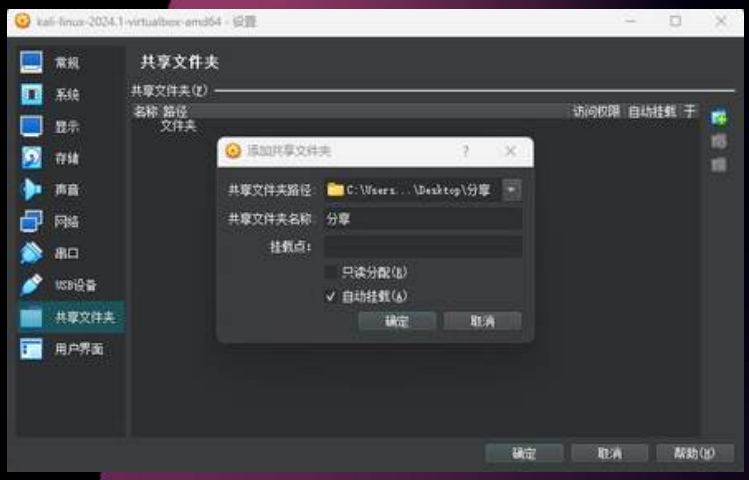
Cyber Secure TECH

3.1 - CREAZIONE CARTELLA CONDIVISA

3.1 - CREAZIONE CARTELLA CONDIVISA

Abbiamo creato una cartella sul localhost dandogli un nome; successivamente abbiamo scaricato uno zip contenente un file di cattura del tool di Kali chiamato Wireshark e lo abbiamo inserito nella medesima.

Aprendo il S.O. Kali riusciamo a visualizzare la cartella condivisa che abbiamo creato attraverso il percorso del FileSystem



Cyber Secure TECH

3.2. - IDENTIFICAZIONE IOC

3.2 - IDENTIFICAZIONE IOC

In figura 1 aprendo il file zip Cattura_U3_W1_L3 nel S.O. Kali, si può notare
la lettura del file in Wireshark e riuscire a visualizzare i pacchetti inviati (con il Flag SYN) e i pacchetti ricevuti (con il Flag ACK).

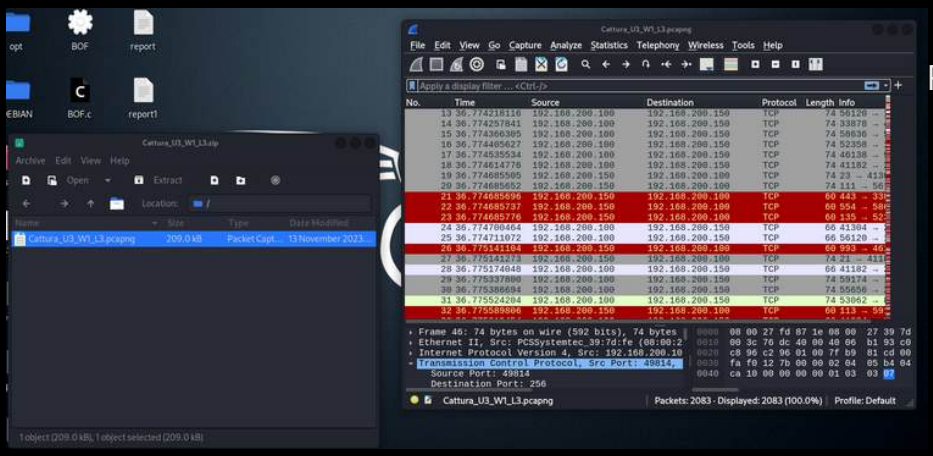


Fig. 1

In figura 2 analizzando il traffico catturato, rileviamo subito la presenza di soli due host: 192.168.200.100 e 192.168.200.150. Continuando l'analisi, osserviamo una grande quantità di richieste SYN provenienti dall'host 192.168.200.100 verso 192.168.200.150. È interessante notare che queste richieste vengono inviate ogni volta su una porta diversa, il che indica chiaramente che non si tratta di un normale tentativo di connessione, ma è molto probabile che questo host stia eseguendo una scansione per individuare vulnerabilità, servizi attivi o porte aperte da sfruttare. L'host 192.168.200.150, invece, risponde alle richieste con un messaggio di tipo: [RST, ACK] se la porta è chiusa; [SYN, ACK] se la porta è aperta.

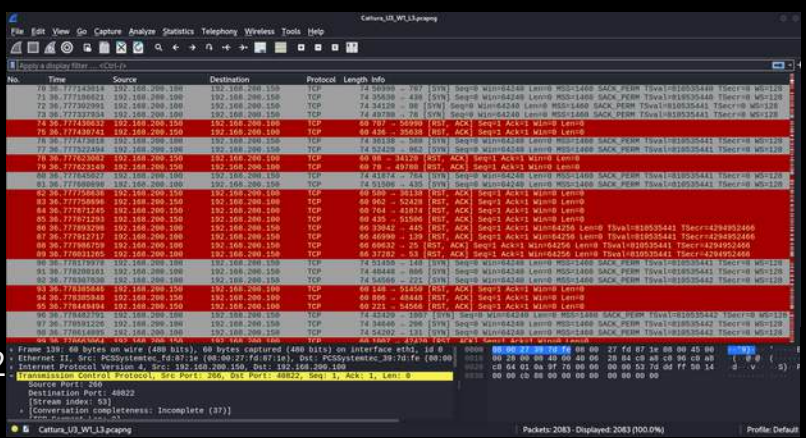


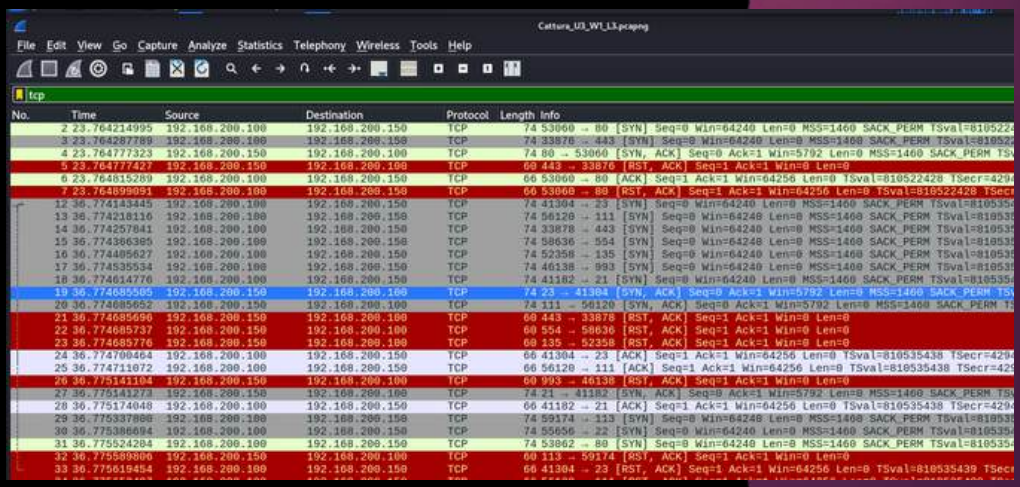
Fig. 2

Cyber Secure TECH

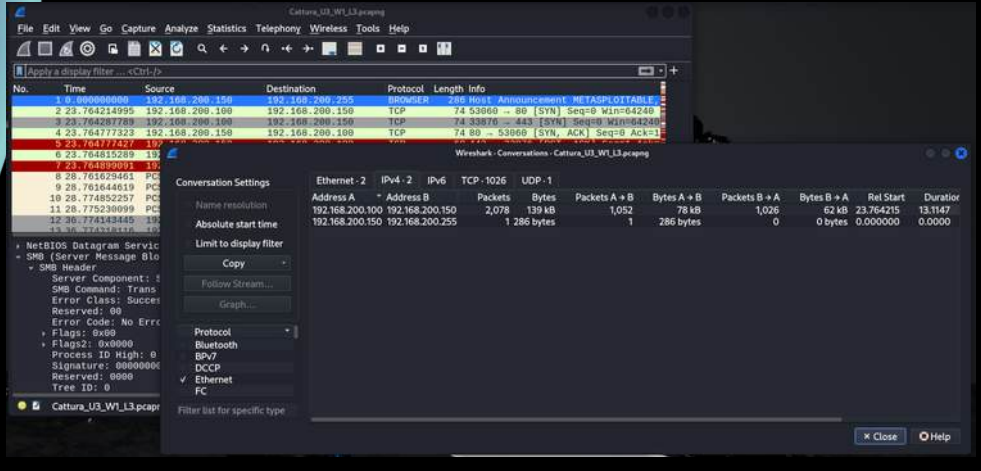
3.3 - IPOTESI ATTACCO

3.3 - IPOTESI ATTACCO

Nella figura sottostante riusciamo a dedurre in modo più specifico il contenuto dei pacchetti ed in parte riusciamo a visualizzare
gli indirizzi IP rispettivamente sulle colonne Source e Destination. Notiamo come i pacchetti **SYN** che sono i pacchetti inviati per instaurare una connessione, vengono inviati dall'indirizzo IP **192.168.200.100**, mentre i pacchetti di risposta **SYN, ACK** (risposta positiva, quindi porta aperta) o **RST, ACK** (risposta negativa, porta chiusa) sono inviati dall'IP **192.168.200.150**. Da questo possiamo dedurre che il primo IP sia quello dell'**attaccante** e il secondo della macchina **vittima**.



Per ottenere una panoramica dettagliata degli indirizzi IP coinvolti nello scambio di pacchetti registrato in un file **.pcapngI (file .pcapng (Packet Capture Next Generation) sono un formato di file utilizzato per la cattura e la memorizzazione dei pacchetti di rete.)** basta cliccare su "Statistics" > "Conversations" e selezionare IPv4 per vedere gli indirizzi IP coinvolti nella conversazione, il numero totale di pacchetti scambiati, il numero di pacchetti inviati da un IP all'altro e viceversa ed anche la loro dimensione.



Cyber Secure TECH

3.4 - TCPDUMP

3.4 - TCPDUMP

Un altro tool molto pratico per analizzare i file **.pcapng** è **tcpdump**, uno strumento già presente nella nostra VM Kali Linux e utilizzabile da riga di comando. Per questa analisi, abbiamo utilizzato i seguenti comandi:

Chiediamo a tcpdump di contare **quanti pacchetti con protocollo tcp** sono contenuti nel file

```
┌──(kali㉿kali)-[~/Desktop]
└─$ tcpdump -r Cattura_U3_W1_L3.pcapng 'tcp' --count

reading from file Cattura_U3_W1_L3.pcapng, link-type EN10MB (Ethernet), snapshot length 262144
2078 packets
```

Questo comando è stato eseguito per vedere effettivamente **chi sta inviando più pacchetti TCP con flag SYN** e quindi possa essere ritenuto esecutore(192.168.200.100) di questa ipotetica scansione ai danni dell'altro indirizzo IP rilevato (192.168.200.150).

- tcpdump -r file.pcapng 'tcp[tcpflags] & tcp-syn != 0' -nn: Questo comando legge il file .pcapng e filtra i pacchetti TCP con il flag SYN impostato, mostrando gli indirizzi IP e le porte senza risolvere i nomi (opzione -nn).
- awk '{print $3}': Estrae il terzo campo dell'output di tcpdump, che contiene l'indirizzo IP sorgente e la porta.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ tcpdump -r Cattura_U3_W1_L3.pcapng 'tcp[tcpflags] & tcp-syn != 0' -nn | awk '{print $3}'

reading from file Cattura_U3_W1_L3.pcapng, link-type EN10MB (Ethernet), snapshot length 262144
192.168.200.100.53060
192.168.200.100.33876
192.168.200.150.80
192.168.200.100.41304
192.168.200.100.56120
192.168.200.100.33878
192.168.200.100.58636
192.168.200.100.52358
192.168.200.100.46138
192.168.200.100.41182
192.168.200.150.23
```

Per **contare i pacchetti inviati con i flag SYN-ACK e RST-ACK** e determinare quanti corrispondono a porte aperte e chiuse, possiamo utilizzare tcpdump e analizzare i flag dei pacchetti TCP.
Ricordiamo che i pacchetti SYN-ACK indicano una porta aperta, mentre RTS-ACK una porta chiusa.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ tcpdump -r Cattura_U3_W1_L3.pcapng 'tcp[tcpflags] == (tcp-rst|tcp-ack)' --count

reading from file Cattura_U3_W1_L3.pcapng, link-type EN10MB (Ethernet), snapshot length 262144
1026 packets

┌──(kali㉿kali)-[~/Desktop]
└─$ tcpdump -r Cattura_U3_W1_L3.pcapng 'tcp[tcpflags] == (tcp-syn|tcp-ack)' --count

reading from file Cattura_U3_W1_L3.pcapng, link-type EN10MB (Ethernet), snapshot length 262144
13 packets
```

3.5 - REMEDATION ACTION

3.5 - REMEDIATION ACTION

Per proteggersi efficacemente dalle scansioni delle porte in una rete informatica, è essenziale adottare misure preventive robuste per mantenere l'integrità e la sicurezza della rete. Di seguito sono elencate alcune azioni preventive specifiche:

1. **Configurazione di regole di sicurezza**: Impostare regole di sicurezza stringenti sui dispositivi di rete come router, switch e **firewall** per limitare l'accesso solo alle porte e ai servizi necessari. L'uso di ACL (Access Control Lists) e altre tecniche di filtraggio consente di permettere solo il traffico autorizzato.Possiamo configurare delle **firewall statico** per bloccare l'accesso a tutte le porte da parte di un determinato attaccante, in modo da evitare che informazioni su porte e servizi in ascolto finiscano nelle sue mani.
2. **Monitoraggio del traffico interno**: Utilizzare strumenti di monitoraggio per analizzare il traffico di rete e rilevare attività sospette o non autorizzate, incluse le scansioni delle porte. Il monitoraggio interno aiuta a identificare rapidamente comportamenti anomali e a rispondere prontamente.
3. **Segmentazione della rete**: Suddividere la rete in segmenti distinti per ridurre il traffico tra le diverse sezioni. Questo approccio limita la capacità di un dispositivo compromesso di esplorare o danneggiare altri segmenti della rete.
4. **Politiche di autenticazione avanzate**: Implementare politiche di autenticazione robuste, come l'autenticazione a due fattori, per proteggere l'accesso ai dispositivi di rete e alle risorse sensibili.
5. **Aggiornamenti frequenti**: Garantire che tutti i dispositivi di rete e il firmware siano regolarmente aggiornati con le ultime patch di sicurezza, per correggere le vulnerabilità note che potrebbero essere sfruttate durante una scansione delle porte o altri tipi di attacchi.

3.6 - CONCLUSIONE SU THREAT INTELLIGENCE E INDICATORI DI COMPROMISSIONE (IOC)

3.6 - CONCLUSIONE SU THREAT INTELLIGENCE E INDICATORI DI COMPROMISSIONE (IOC)

La **Threat Intelligence** e gli Indicatori di Compromissione (**IOC**) sono componenti fondamentali della strategia di sicurezza informatica moderna. La Threat Intelligence fornisce informazioni preziose sulle minacce attuali e potenziali, permettendo alle organizzazioni di anticipare, identificare e rispondere efficacemente agli attacchi.

Gli IOC, d'altra parte, sono strumenti critici per rilevare e mitigare compromissioni, fornendo segnali specifici che indicano attività dannose all'interno della rete.
L'integrazione di Threat Intelligence e IOC nel framework di sicurezza consente una difesa proattiva e reattiva. La Threat Intelligence aiuta a comprendere il contesto delle minacce e a prendere decisioni informate, mentre gli IOC permettono una risposta rapida e precisa agli incidenti, limitando i danni e prevenendo future violazioni.
In un panorama di minacce in continua evoluzione, l'adozione di un approccio basato su Threat Intelligence e IOC è indispensabile.

Questi strumenti non solo migliorano la visibilità e la consapevolezza delle minacce, ma rafforzano anche la capacità di difesa delle organizzazioni, proteggendo le risorse critiche e mantenendo la fiducia delle parti interessate.

GIORNO 4
Incident Response

INDICE
GIORNO 4

S9_L4

Giorno 4 - Incident Response

Cyber Secure TECH

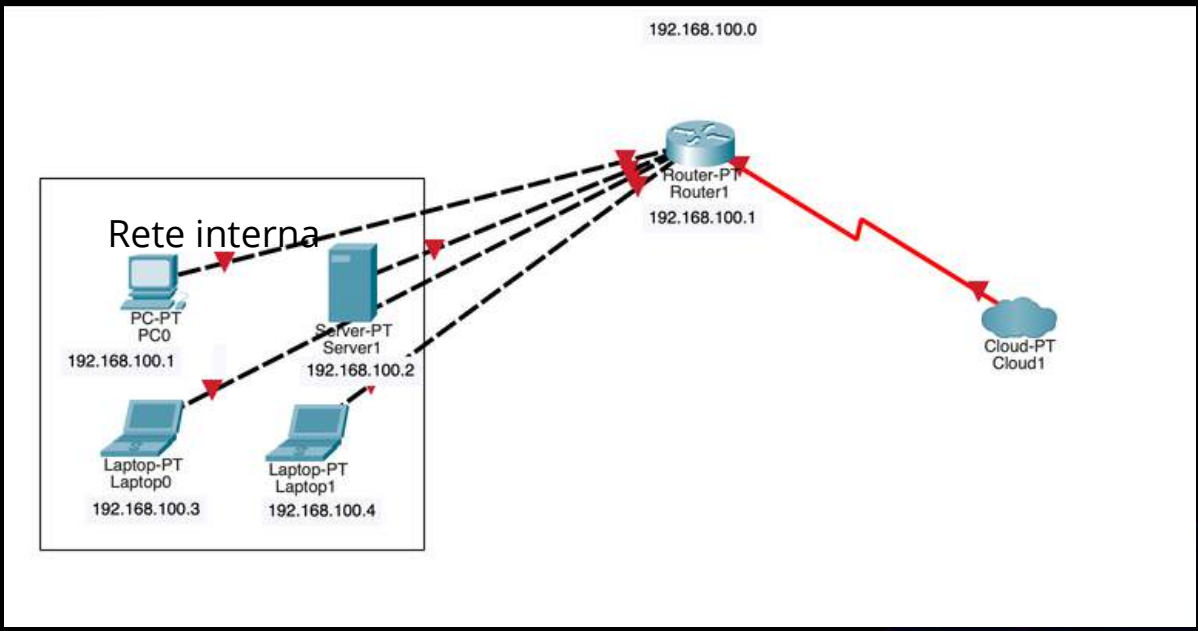
TRACCIA
GIORNO 4

Incident response Con riferimento alla figura, il database con diversi dischi per lo storage è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite Internet.

L'attacco è attualmente in corso e siete parte del team di CSIRT. Rispondere ai seguenti quesiti.

Mostrate le tecniche di:

1) Isolamento
2) Rimozione del sistema infetto
3) Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. Indicare anche Clear



Cyber Secure TECH

4.1 - RILEVAMENTO ANALISI

4.1 - RILEVAMENTO ANALISI

La fase di rilevamento ed analisi è una delle più complicate da gestire come un processo automatizzato e continuativo di routine. Infatti, sebbene ci siano diversi mezzi messi a disposizione per la fase di monitoraggio ed analisi, alcuni degli incidenti sono rilevabili solamente da personale con forte esperienza sul campo.

Tra gli indicatori di attacchi in corso troviamo:

- Gli alert che hanno origine da un sistema di prevenzione e rilevamento intrusioni (IPS/IDS) o da un SIEM o da un sistema antivirus. Gli alert automatici «scattano» quando un evento sospetto si manifesta.
- I Log generati da un sistema operativo, da un servizio o da un'applicazione, un dispositivo di rete e tutti i dispositivi hardware e software che sono in grado di produrre log.
- Informazioni pubbliche circa nuove vulnerabilità ed exploit appena scoperti (0-day), o scoperti in ambienti controllati.
- Persone interne o esterne alla compagnia che riportano attività sospette che potrebbero indicare un incidente di sicurezza in corso.

L'analisi è un processo piuttosto complesso che può essere supportato da alcune azioni per migliorare l'efficacia:

- Profilazione delle rete e dei sistemi
- Implementazione di tool UEBA (User and Entity Behavior Analytics)
- Creazione di policy di logging efficaci
- Correlazione degli eventi
- Cattura del traffico

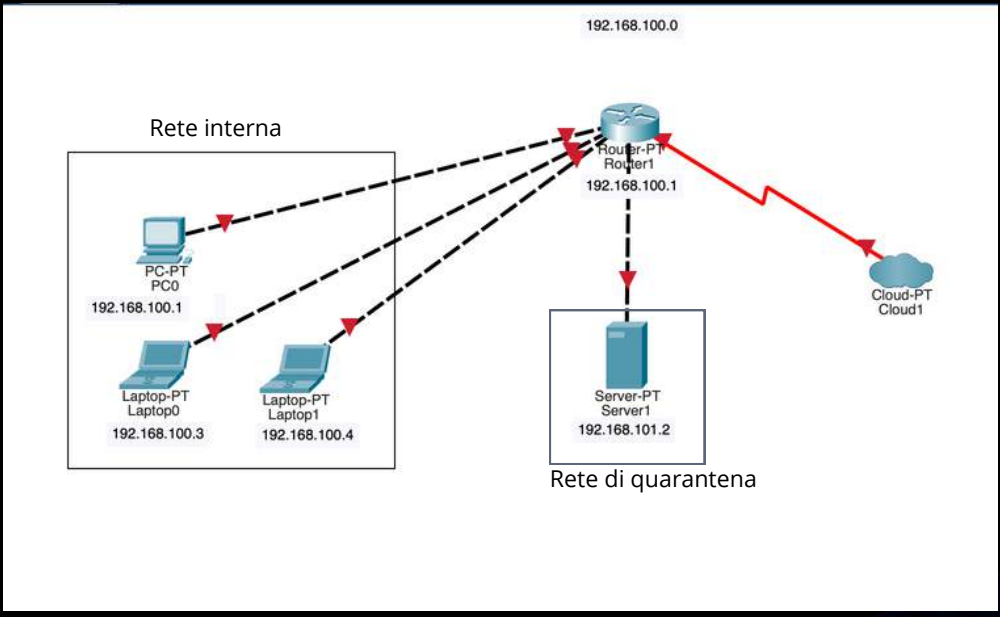
4.2 - FASE DI CONTENIMENTO

4.2 - CONTENIMENTO

SEGMENTAZIONE DELLA RETE

Segmentando la rete, spostiamo il server infetto in un'altra subnet, comunemente chiamata "rete di quarantena". Questo consente di limitare l'accesso dell'attaccante ad altri dispositivi presenti nella rete interna e, in caso di malware, ne impedisce la diffusione verso altri sistemi. Tuttavia, il server rimane accessibile tramite Internet, il che può rappresentare un rischio residuo.

Per garantire una maggiore sicurezza, è essenziale implementare politiche di controllo degli accessi rigorose all'interno della rete di quarantena. Questo include l'uso di firewall avanzati e sistemi di rilevamento delle intrusioni (IDS) per monitorare e bloccare attività sospette. Inoltre, è consigliabile limitare il traffico in entrata e in uscita dal server infetto solo ai servizi strettamente necessari per le attività di analisi e risoluzione del problema. Nel caso in cui la segmentazione non sia sufficientemente efficace, si procede con l'isolamento del server.



4.2 - CONTENIMENTO

Tecniche di Segmentazione

La segmentazione è una tecnica di sicurezza informatica utilizzata per dividere una rete in subnet più piccole e gestibili, chiamate segmenti, ciascuno con i propri controlli di sicurezza. Questo approccio migliora la sicurezza riducendo la superficie d'attacco e limitando il movimento laterale di eventuali intrusi all'interno della rete. Ecco alcune caratteristiche principali della segmentazione:

1. **Isolamento delle Risorse:** Le risorse critiche vengono isolate dagli altri segmenti della rete, riducendo il rischio di accesso non autorizzato.
2. Controllo degli Accessi: Politiche di accesso più restrittive possono essere applicate a ciascun segmento, basate sul principio del minimo privilegio.
3. **Miglior Monitoraggio e Risposta:** La segmentazione facilita il monitoraggio delle attività e la risposta agli incidenti, permettendo una rapida identificazione e contenimento delle minacce all'interno di un segmento specifico.
4. **Performance Migliorata:** Riducendo il traffico di rete attraverso una segmentazione intelligente, si possono migliorare le performance della rete.

Tecniche di Contenimento

Il contenimento è una strategia di risposta agli incidenti che mira a limitare l'impatto di una minaccia identificata e impedire la sua diffusione. Le tecniche di contenimento includono:

1. Isolamento del Sistema: Disconnettere i sistemi compromessi dalla rete per impedire ulteriori danni.
2. Blocco degli Account: Disabilitare gli account utente compromessi per prevenire ulteriori accessi non autorizzati.
3. Limitazione del Traffico di Rete: Utilizzare firewall e altri dispositivi di rete per bloccare il traffico sospetto o malevolo.
4. Patch e Aggiornamenti: Applicare patch e aggiornamenti di sicurezza per correggere le vulnerabilità sfruttate dall'attacco.
5. Backup e Ripristino: Utilizzare backup recenti per ripristinare i sistemi compromessi a uno stato sicuro.

Differenze Chiave

- Proattività vs Reattività: La segmentazione è una misura proattiva, progettata per prevenire attacchi futuri attraverso la strutturazione della rete. Il contenimento, invece, è una misura reattiva, applicata in risposta a un incidente in corso.
- Scope: La segmentazione riguarda la configurazione della rete a lungo termine, mentre il contenimento si concentra sull'immediata limitazione dei danni durante un incidente di sicurezza.

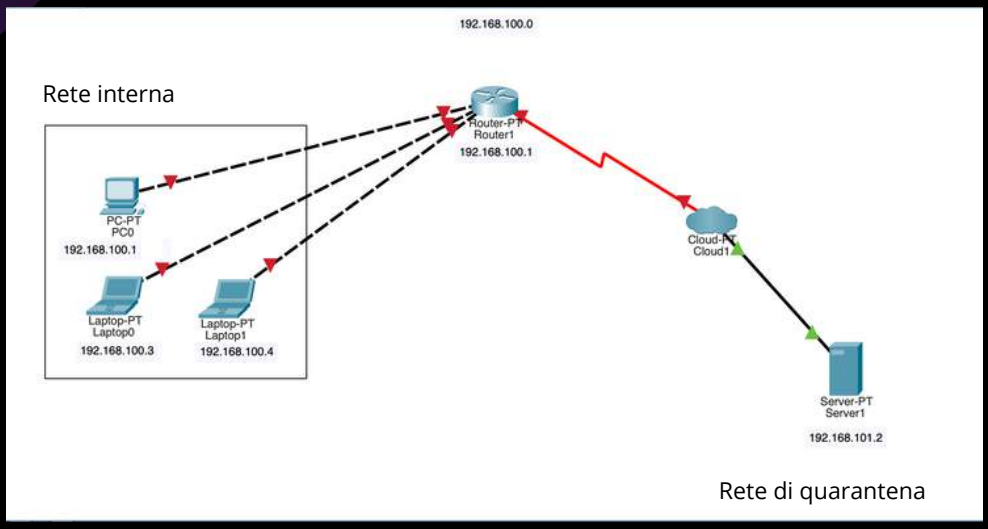
In sintesi, entrambe le tecniche sono fondamentali per una strategia di sicurezza informatica completa, con la segmentazione che funge da misura preventiva e il contenimento che fornisce una risposta efficace agli incidenti.

4.2 - CONTENIMENTO

ISOLAMENTO

L'isolamento è una tecnica impiegata quando è necessario un contenimento più rigoroso del sistema infetto. In questo scenario, il sistema viene completamente disconnesso dalla rete interna, riducendo ulteriormente le possibilità dell'attaccante di accedere ad altri dispositivi all'interno della rete aziendale.

Tuttavia, anche in questo caso, il dispositivo infetto potrebbe rimanere accessibile tramite Internet, il che rappresenta ancora un potenziale rischio di sicurezza.



Isolamento nelle Tecniche di Contenimento

L'isolamento è una tecnica di contenimento fondamentale utilizzata nella risposta agli incidenti di sicurezza informatica per limitare l'impatto di una minaccia identificata e impedirne la diffusione. L'isolamento prevede la separazione dei sistemi compromessi dal resto della rete per prevenire ulteriori danni e contenere l'attacco.
Caratteristiche Principali dell'Isolamento

- Isolamento del Sistema:
  - **Disconnessione Fisica o Logica**: Il sistema compromesso viene scollegato fisicamente dalla rete o isolato logicamente tramite configurazioni di rete, come la disabilitazione delle interfacce di rete.
  - **Mantenimento della Funzionalità Limitata**: In alcuni casi, il sistema può rimanere operativo ma con accesso limitato, permettendo ulteriori analisi senza rischiare la propagazione della minaccia.

- Isolamento del Segmento di Rete:
  - **Segmentazione Temporanea**: Segmentare temporaneamente parti della rete per contenere l'incidente all'interno di un'area specifica.
  - **Controllo del Traffico**: Utilizzare firewall e altre soluzioni di sicurezza per bloccare il traffico tra segmenti della rete.

- Isolamento degli Utenti:
  - **Blocco degli Account**: Disabilitare gli account utente compromessi per prevenire ulteriori accessi non autorizzati.
  - **Restrizione dei Privilegi**: Ridurre i privilegi degli utenti sospetti per limitare le loro capacità all'interno del sistema.

- Isolamento delle Applicazioni:
  - **Containerizzazione**: Eseguire applicazioni in contenitori separati per limitare l'impatto di un compromesso a livello applicativo.
  - **Virtualizzazione**: Utilizzare macchine virtuali per isolare applicazioni e servizi critici, rendendo più facile il contenimento in caso di attacco.

Benefici dell'Isolamento

- Limitazione della Propagazione: L'isolamento impedisce alla minaccia di diffondersi ad altri sistemi e segmenti della rete.
- Facilitazione dell'Analisi: Separare il sistema compromesso consente una migliore analisi forense senza il rischio di ulteriori contaminazioni.
- Riduzione dell'Impatto: Minimizza i danni operativi e finanziari limitando l'incidente a una parte controllata dell'infrastruttura.

Tecniche di Isolamento Comune

- Network Quarantine: Isolamento della macchina compromessa in una rete di quarantena per ulteriori indagini.
- Virtual LANs (VLANs): Utilizzo di VLAN per separare il traffico di rete e limitare l'accesso tra segmenti.
- Endpoint Isolation: Utilizzo di software di sicurezza per isolare endpoint compromessi.

Esempi di Applicazione

- Ransomware Attack: In caso di attacco ransomware, isolare i sistemi infetti per prevenire la crittografia di ulteriori dati.
- Phishing Compromise: Disabilitare l'account email compromesso e isolare i sistemi coinvolti per prevenire l'ulteriore diffusione di email malevoli.

In sintesi, l'isolamento è una tecnica di contenimento critica per gestire e limitare gli effetti degli incidenti di sicurezza informatica, proteggendo il resto della rete e facilitando la risposta all'incidente.

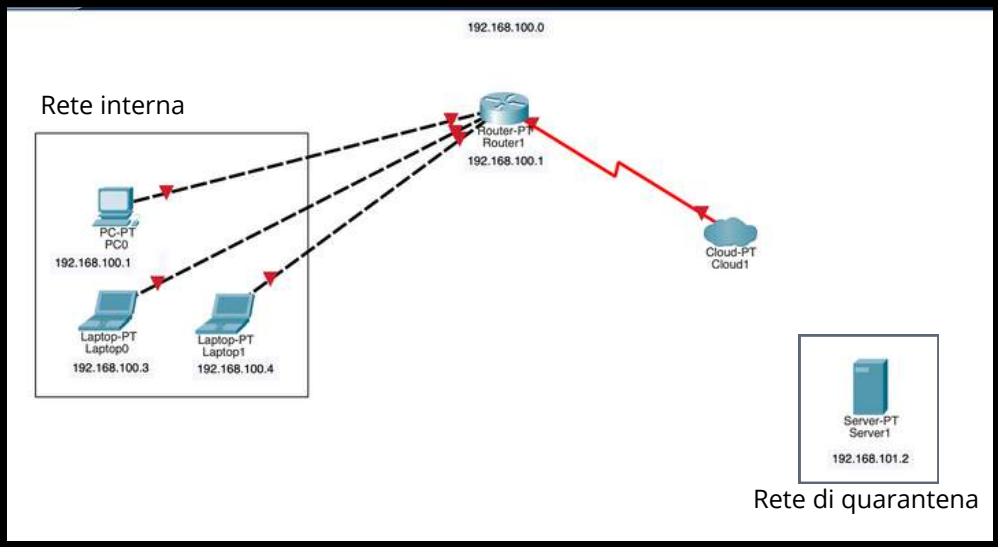
4.3 - FASE DI RIMOZIONE

4.3 - RIMOZIONE

RIMOZIONE

Nel caso in cui anche l’isolamento non sia sufficientemente efficace, si procede con la rimozione (o isolamento completo) del server. Questo implica la rimozione di tutte le connessioni di rete, sia interne che esterne, garantendo che il server non possa comunicare con alcun altro dispositivo o rete.

Durante questa fase, è fondamentale eseguire un'analisi approfondita del server infetto per identificare la natura dell'attacco e implementare le misure di riparazione necessarie.



Rimozione nelle Tecniche di Contenimento

La rimozione è una tecnica di contenimento utilizzata nella risposta agli incidenti di sicurezza informatica per eliminare le minacce identificate da un sistema o una rete. Questa tecnica è finalizzata a neutralizzare completamente la minaccia, ripristinare la sicurezza del sistema e prevenire future compromissioni.

Caratteristiche Principali della Rimozione

1. Identificazione Completa della Minaccia:
   - Scansione e Analisi: Utilizzo di strumenti di sicurezza come antivirus, antimalware e scanner di vulnerabilità per identificare tutti i componenti malevoli presenti nel sistema.
2. Eliminazione del Malware:
   - Pulizia del Sistema: Rimozione dei file infetti, chiavi di registro malevole e altri artefatti del malware tramite software di sicurezza.
   - Ripristino di File Modificati: Ripristino dei file di sistema critici che potrebbero essere stati alterati dall'attacco.
3. Correzione delle Vulnerabilità:
   - Patch e Aggiornamenti: Applicazione di patch di sicurezza e aggiornamenti per correggere le vulnerabilità sfruttate dall'attacco.
   - Modifiche alla Configurazione: Aggiustamenti alla configurazione di sicurezza per rafforzare le difese e prevenire future compromissioni.
4. Rimozione degli Accessi Non Autorizzati:
   - Disabilitazione degli Account: Rimozione o disabilitazione di account utente compromessi o creati dagli attaccanti.
   - Cambio delle Password: Richiesta di cambio delle password per gli account utenti per prevenire accessi non autorizzati futuri.
5. Ripristino dei Sistemi Compromessi:
   - Ripristino da Backup: Utilizzo di backup recenti per ripristinare i sistemi compromessi a uno stato sicuro.
   - Verifica dell'Integrità del Sistema: Controllo dell'integrità del sistema dopo la rimozione per assicurarsi che tutte le minacce siano state eliminate.

Benefici della Rimozione

- Eliminazione della Minaccia: La rimozione assicura che il sistema sia libero da malware e altre componenti malevoli.
- Ripristino della Sicurezza: Ripristina la sicurezza del sistema, permettendo di tornare a operare in modo normale e sicuro.
- Prevenzione di Future Compromissioni: Correggendo le vulnerabilità e rafforzando le difese, si riduce il rischio di future compromissioni.

Tecniche di Rimozione Comuni

- Antivirus e Antimalware: Utilizzo di software specializzati per rilevare e rimuovere malware e altre minacce.
- Strumenti di Pulizia Manuale: In alcuni casi, potrebbe essere necessaria una rimozione manuale di artefatti malevoli da parte di esperti di sicurezza.
- Formattazione e Reinstallazione: Nei casi più gravi, la formattazione del sistema e la reinstallazione completa possono essere necessarie per garantire la completa rimozione della minaccia.

Esempi di Applicazione

- Infezione da Malware: Rimozione del malware attraverso scansioni antivirus e applicazione di patch di sicurezza.
- Accesso Non Autorizzato: Disabilitazione di account compromessi e ripristino delle credenziali per prevenire ulteriori accessi non autorizzati.

In sintesi, la rimozione è una tecnica essenziale di contenimento che mira a eliminare completamente le minacce dai sistemi compromessi, ripristinando la sicurezza e prevenendo futuri incidenti.

4.4 - ELIMINAZIONE INFORMAZIONI SENSIBILI

4.4 - ELIMINAZIONE

ELIMINAZIONE INFORMAZIONI SENSIBILI

Quando si tratta di eliminare informazioni sensibili da dischi compromessi prima dello smaltimento, esistono diverse metodologie riconosciute, tra cui **Clear, Purge e Destro**y.

CLEAR

Metodo che rende i dati inaccessibili tramite tecniche logiche, ma non necessariamente irrecuperabili con tecniche avanzate di recupero dati

Overwrite

Utilizzare comandi software per ripristinare il disco alle impostazioni di fabbrica.

Reset

Sovrascrivere tutti i settori del disco con dati casuali o con uno schema specifico (ad esempio, tutti zeri, tutti uno o una combinazione ripetuta).

Clear è generalmente sufficiente per eliminare dati in ambienti in cui il rischio di accesso non autorizzato è considerato basso o dove non sono presenti informazioni altamente sensibili.

4.4 - ELIMINAZIONE

PURGE

Metodo che adotta sia un approccio logico che delle tecniche di rimozione fisica

Degaussing

Utilizzare un dispositivo degausser per smagnetizzare il disco, cancellando tutti i dati memorizzati.

Sanitization software

Utilizzare software specializzato per eseguire la sovrascrittura multipla del disco con schemi complessi e variabili, rendendo molto difficile il recupero dei dati.

Cryptographic erase

Sovrascrivere le chiavi di cifratura utilizzate per proteggere i dati memorizzati, rendendo i dati stessi indecifrabili.

Purge è adatto per scenari in cui i dati sono considerati altamente sensibili e vi è un rischio maggiore che qualcuno tenti di recuperarli con strumenti avanzati.

Purge nelle Tecniche di Contenimento

Il purge (pulizia totale) è una tecnica di contenimento utilizzata nella risposta agli incidenti di sicurezza informatica per eliminare completamente tutte le tracce di una minaccia da un sistema compromesso. Questa tecnica è adottata in situazioni in cui è necessario garantire che nessun residuo della minaccia rimanga nel sistema, spesso come misura finale dopo altre tecniche di rimozione.

Caratteristiche Principali del Purge

1. Cancellazione Completa dei Dati:
   - Formattazione dei Dispositivi: Formattazione completa dei dischi rigidi e delle altre unità di memorizzazione per rimuovere ogni traccia di malware, file infetti o dati compromessi.
   - Sovrascrittura Sicura: Utilizzo di tecniche di sovrascrittura dei dati (wiping) per assicurarsi che i dati cancellati non possano essere recuperati.
2. Ripristino da Backup Sicuri:
   - Utilizzo di Backup Incontaminati: Ripristino dei sistemi utilizzando backup che sono stati verificati come privi di compromissioni.
   - Verifica dell'Integrità del Backup: Controllo rigoroso dei backup per assicurarsi che siano sicuri e non contengano elementi malevoli.
3. Reinstallazione del Software:
   - Reinstallazione del Sistema Operativo: Reinstallazione completa del sistema operativo per garantire un ambiente pulito.
   - Reinstallazione delle Applicazioni: Installazione da zero delle applicazioni necessarie, preferibilmente da fonti sicure e verificate.
4. Aggiornamento delle Misure di Sicurezza:
   - Applicazione di Patch e Aggiornamenti: Assicurarsi che tutte le patch di sicurezza e gli aggiornamenti software siano applicati.
   - Implementazione di Nuove Difese: Configurare e implementare misure di sicurezza aggiuntive per prevenire future compromissioni.

Benefici del Purge

- Rimozione Totale della Minaccia: Garantisce che non rimanga alcuna traccia della minaccia originale nel sistema.
- Ripristino Sicuro del Sistema: Ripristina il sistema a uno stato sicuro, minimizzando il rischio di residui malevoli.
- Prevenzione di Recidive: Riduce significativamente il rischio di reinfezione attraverso una pulizia completa e un nuovo inizio.

Tecniche di Purge Comuni

- Disk Wiping: Utilizzo di software specializzati per sovrascrivere completamente i dati sui dischi.
- Formattazione a Basso Livello: Una formattazione approfondita che cancella tutte le informazioni memorizzate sui dispositivi di archiviazione.
- Riconfigurazione del Sistema: Configurare nuovamente il sistema per garantire che sia sicuro e funzionante correttamente dopo il purge.

Esempi di Applicazione

- Gravi Infezioni da Malware: Situazioni in cui il malware è profondamente radicato nel sistema e altre tecniche di rimozione non sono sufficienti.
- Incidenti di Sicurezza Estesi: Compromissioni di vasta portata che richiedono una pulizia completa per ripristinare la fiducia nell'integrità del sistema.
-

In sintesi, il purge è una tecnica di contenimento drastica ma efficace, utilizzata per eliminare completamente qualsiasi traccia di una minaccia da un sistema compromesso, garantendo un ambiente sicuro e pulito per le operazioni future.

4.4 - ELIMINAZIONE

DESTROY

è il metodo più sicuro e definitivo per garantire che i dati non possano essere recuperati in alcun modo

Shredding

Utilizzare macchine specializzate per distruggere fisicamente il disco in piccoli pezzi.

Incineration

Bruciare i dischi in forni ad alta temperatura.

Cryptographic erase

Utilizzare sostanze chimiche per dissolvere i materiali del disco.

Destroy è necessario quando i dati sono estremamente sensibili e devono essere completamente e permanentemente irrecuperabili, indipendentemente dalle tecnologie disponibili.

CONFRONTO TRA CLEAR, PURGE E DESTROY

- **Clear**: Rende i dati inaccessibili tramite metodi standard, ma può essere vulnerabile a tecniche avanzate di recupero.
- **Purge**: Rende i dati inaccessibili anche tramite metodi avanzati, ma non distrugge fisicamente il disco.
- **Destroy**: Elimina fisicamente il disco, garantendo l'impossibilità assoluta di recupero dei dati.

La scelta tra queste tecniche dipende dal livello di sensibilità dei dati e dalle politiche di sicurezza dell'organizzazione.

4.5 - FASE DI RECUPERO

4.5 - FASE DI RECUPERO

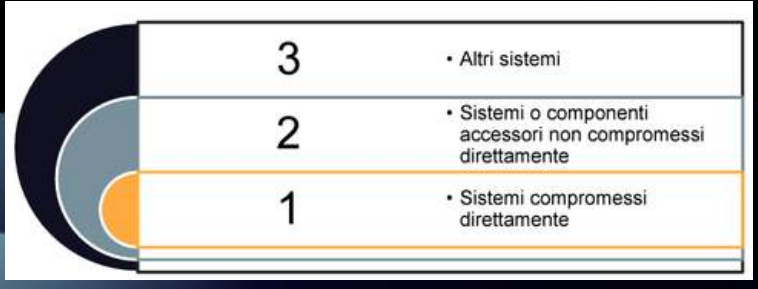
La fase di recupero ha l'obiettivo di ristabilire la normale operatività delle applicazioni e dei servizi dopo un attacco informatico. Questo processo include diverse attività essenziali, come il recupero dei dati e delle informazioni perse, l'applicazione di patch per sistemi obsoleti, la revisione delle politiche di firewall, IPS e IDS, e l'aggiornamento delle firme degli antivirus. Lo scopo della fase di recupero è non solo ripristinare la funzionalità, ma anche prevenire futuri attacchi simili.

Quando sistemi, server e host vengono compromessi, devono essere considerati non più affidabili. È fondamentale ripulirli a fondo prima di rimetterli in produzione, utilizzando tecniche di "reconstruction" o "rebuilding":

-**Reconstruction**: Questa tecnica mira a recuperare e ripristinare le parti ancora affidabili di un sistema compromesso, eliminando solo le componenti danneggiate o infette.
-**Rebuilding**: Questa tecnica implica la ricostruzione completa del sistema compromesso, partendo da zero. È utilizzata quando il sistema è considerato completamente inaffidabile.

Per quanto riguarda le applicazioni, i server e i software, prima di procedere con la fase di recupero, è cruciale identificare il punto di ingresso dell'attacco. Capire dove si trovano le vulnerabilità consente di implementare le patch necessarie e rafforzare la sicurezza, prevenendo il ripetersi dell'incidente. Questo approccio analitico garantisce che le misure correttive siano efficaci e mirate, migliorando la resilienza complessiva del sistema.

In sintesi, la fase di recupero non solo ripristina la funzionalità, ma rappresenta anche un'opportunità per rafforzare le difese contro future minacce, assicurando che i sistemi siano adeguatamente protetti e pronti per operare in modo sicuro e affidabile.




Giorno 5
Analisi dei Log

INDICE
GIORNO 5

S9_L5

Giorno 5 - Analisi dei Log

Cyber Secure TECH

TRACCIA
GIORNO 5

Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

1. Azioni preventive : quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni

2. Impatti sul business : l'applicazione Web subisce un attacco di tipo l'applicazione non raggiungibile per 10 minuti . Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € Esercizio Traccia e requisiti DDoS dall'esterno che rende sulla piattaforma di e-commerce . Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

3. Response : l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta .

4. Soluzione completa : unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

5. Modifica più aggressiva dell'infrastruttura: integrando altri eventuali elementi di sicurezza (se necessario/facoltativo magari integrando la soluzione al punto 2)

Cyber Secure TECH

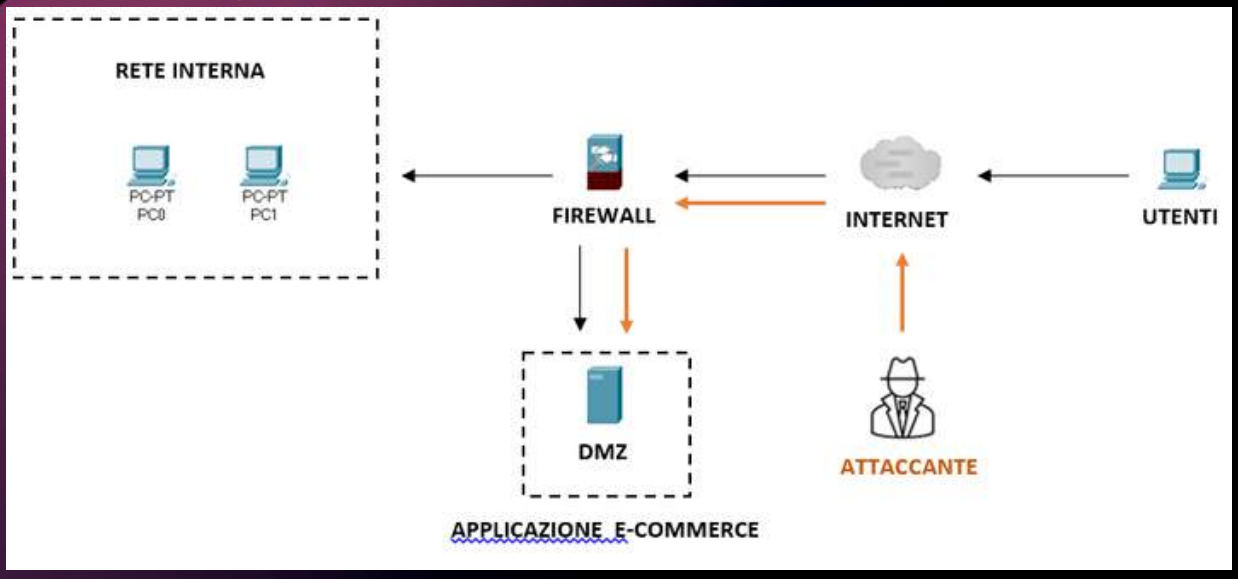
1 - AZIONI PREVENTIVE

1. Azioni preventive : quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato?

Modificate la figura in modo da evidenziare le implementazioni

1. Azioni preventive :

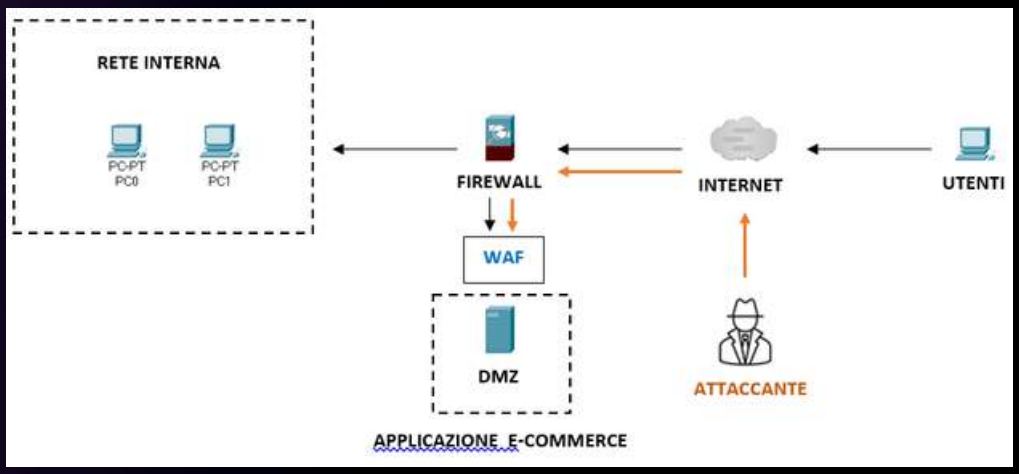
Nella figura seguente possiamo notare la minaccia di un attacco da parte di un attaccante esterno che ha bypassato i controlli del Firewall, impostato secondo alcune regole, per entrare nella DMZ ed attaccare le applicazioni di e-commerce e web app con tecniche di SQLi ed XSS



1. Azioni preventive :

Per la protezione della Web App da minacce quali XSS e SQLi si può preventivamente adottare una soluzione basata su Web Application Firewall, che a differenza dei firewall standard, sono dedicati per proteggere le Web App da attacchi XSS e SQLi.

Nella figura qui di seguito si modifica di conseguenza; abbiamo ipotizzato che il WAF sia a protezione del traffico in entrata sulla Web App da internet (quindi utenti e attaccante).



Cyber Secure TECH

2. Impatti sul business : l'applicazione Web subisce un attacco di tipo l'applicazione non raggiungibile per 10 minuti .

Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € Esercizio Traccia e requisiti DDoS dall'esterno che rende sulla piattaforma di e-commerce . Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

2. Impatti sul business :

Impatti sul business: l'applicazione Web subisce un attacco di tipo Ddos dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce.

L'attacco di tipo Ddos causa la non raggiungibilità della piattaforma di e-commerce per 10 minuti. Considerando che gli utenti spendono circa 1.500€ al minuto, possiamo stimare i danni causati dal mancato guadagno sul business moltiplicando la spesa potenziale degli utenti per minuto (1.500€) per i minuti di indisponibilità del servizio (10). Di conseguenza: Impatto sul business = 1.500 € x 10 minuti = 15.000 € Ovvero per 10 minuti di indisponibilità la compagnia ha perso **15.000 €** di acquisti potenziali.

3 - RESPONSE

3. Response : l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta .

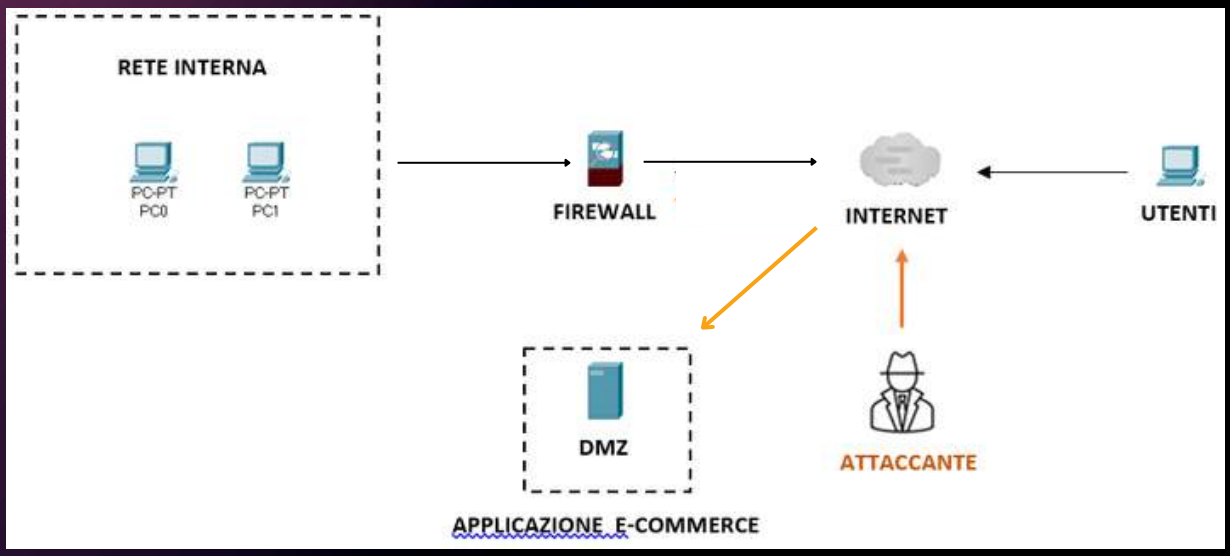
3. Response :

Considerata la priorità, si può adottare una strategia basata sull'isolamento della macchina infettata.

In questo caso la macchina sarà direttamente collegata ad internet, raggiungibile dall'attaccante ma non più connessa alla rete interna.

La figura nella seguente mostra la soluzione con la strategia dell'isolamento della macchina infetta.

Notate come non ci sia più comunicazione tra l'applicazione Web e la rete interna.



Response: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura con le evidenze delle implementazioni. Considerata la priorità, si può adottare una strategia basata sull'isolamento della macchina infettata. In questo caso la macchina sarà direttamente collegata ad internet, raggiungibile dall'attaccante ma non più connessa alla rete interna. La figura nella prossima slide mostra la soluzione con la strategia dell'isolamento della macchina infetta. Notate come non ci sia più comunicazione tra l'applicazione Web e la rete interna.

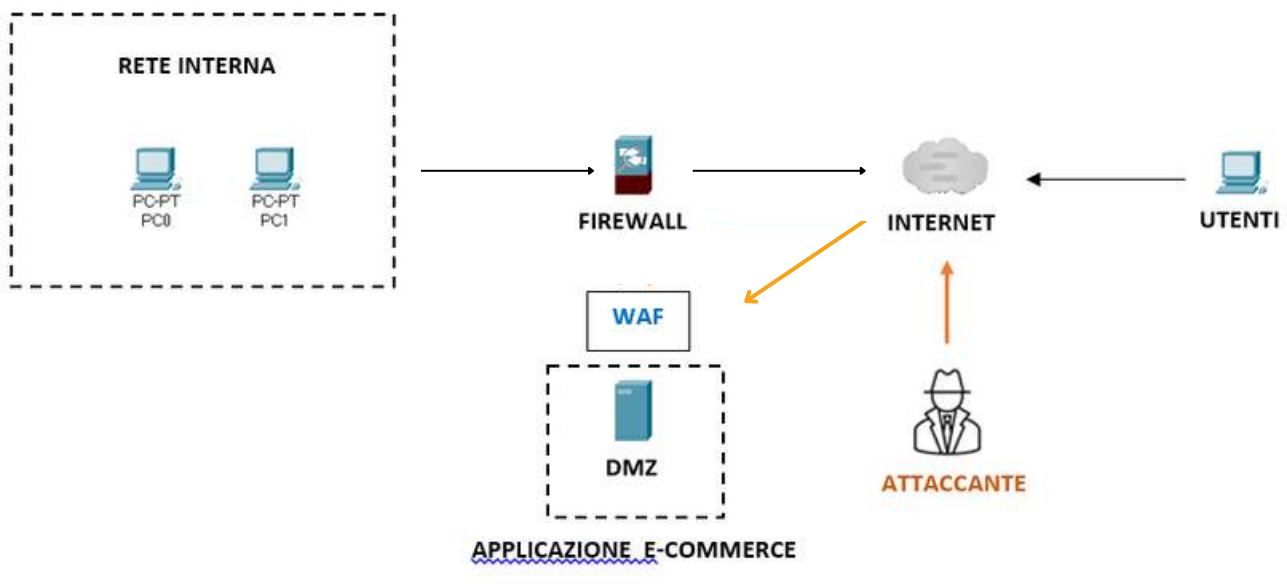
Cyber Secure TECH

4. Soluzione completa : unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

4. Soluzione completa :

In questo caso la macchina sarà ancora collegata ad internet, raggiungibile dall'attaccante, non più connessa alla rete interna e con l'aggiunta del WAF.

La figura nella seguente mostra la soluzione con la strategia dell'isolamento della macchina infetta con un ulteriore filtraggio.

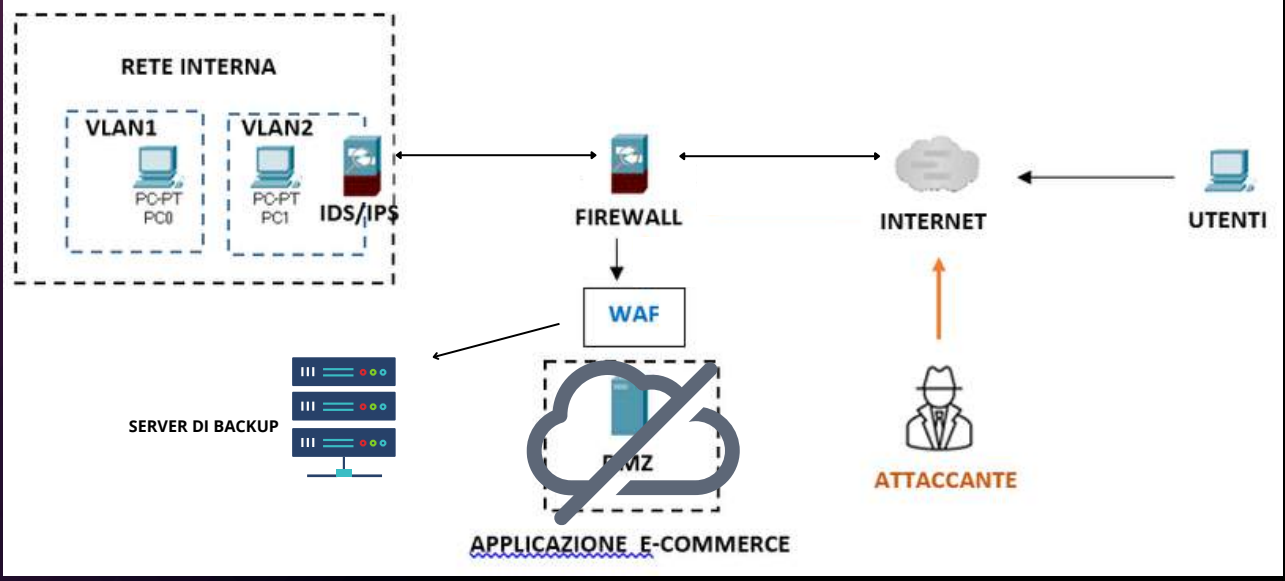


Cyber Secure TECH

5. Modifica più aggressiva dell'infrastruttura: integrando altri eventuali elementi di sicurezza (se necessario/facoltativo magari integrando la soluzione al punto 2)

5. Modifica più aggressiva :

Nella seguente figura la macchina infetta sarà completamente rimossa dalla rete e sostituita da un server di backup che consente di instradare il traffico lecito per non interrompere i servizi. Inoltre nella rete interna abbiamo inserito ulteriori filtraggi con IDS/IPS: la Intranet viene ulteriormente suddivisa in più VLAN per una maggiore sicurezza



Cyber Secure TECH

6 - ANY RUN

AnyRun è una piattaforma di analisi malware interattiva e basata sul cloud, progettata per eseguire e analizzare file sospetti in un ambiente sicuro e controllato. Ecco alcune delle caratteristiche principali di AnyRun:

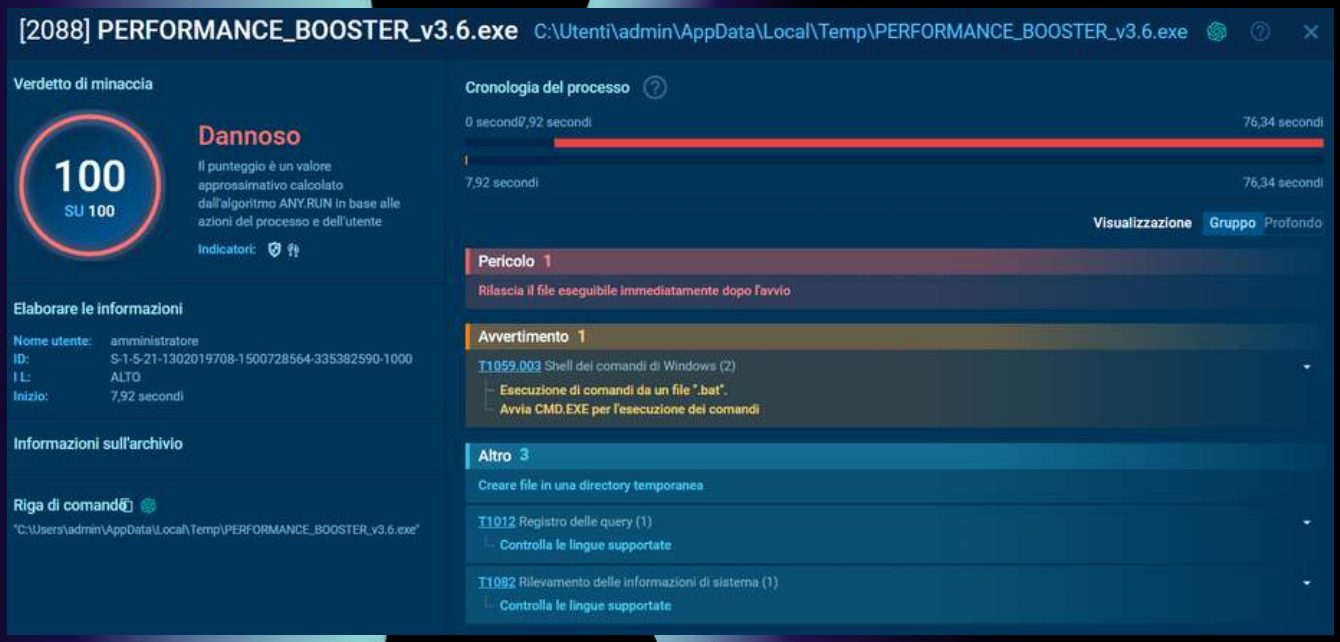
1. Analisi interattiva: A differenza delle sandbox tradizionali, AnyRun consente agli utenti di interagire manualmente con i file sospetti durante l'analisi, eseguendo azioni come cliccare su pulsanti, inserire dati e navigare tra le finestre. Questo aiuta a rivelare comportamenti che potrebbero non essere visibili in un'analisi completamente automatizzata.
2. Ambiente sicuro: I file sospetti vengono eseguiti in un ambiente isolato (sandbox) che imita un sistema operativo reale, impedendo al malware di infettare il sistema host o di diffondersi nella rete.
3. Rilevamento di comportamenti sospetti: AnyRun monitora e registra tutte le attività del file analizzato, inclusi i processi creati, le modifiche al file system, le connessioni di rete e le azioni sul registro di sistema. Questo permette di identificare rapidamente comportamenti malevoli.
4. Report dettagliati: Dopo l'analisi, AnyRun fornisce report dettagliati che includono tutte le attività osservate, screenshot delle finestre, traffico di rete, e molto altro. Questi report possono essere usati per comprendere meglio il funzionamento del malware e per prendere misure di sicurezza appropriate.
5. Condivisione e collaborazione: Gli utenti possono condividere facilmente i risultati delle loro analisi con colleghi o con la comunità di sicurezza informatica, favorendo la collaborazione e il miglioramento delle difese collettive contro le minacce.
6. Supporto per vari tipi di file: AnyRun supporta l'analisi di diversi tipi di file, come eseguibili, documenti, script e archivi, rendendolo uno strumento versatile per diverse situazioni di sicurezza.

In sintesi, AnyRun è uno strumento potente e flessibile per l'analisi dei malware, che permette ai professionisti della sicurezza di esaminare in profondità i comportamenti malevoli in un ambiente sicuro e controllato.

7 - ANALISI LOG 1

PERFORMANCE_BOOSTER_V3.6.EXE

Nel processo delle analisi sul quale siamo stati ingaggiati siamo stati avvisati dal SIEM con un alert ed abbiamo effettuato una scansione sull'Interactive Malware Sandbox per analizzare un eventuale un'attività dannosa di nome PERFORMANCE_BOOSTER_V3.6.EXE, come possiamo notare dalla figura qui di seguito



Informazioni generali

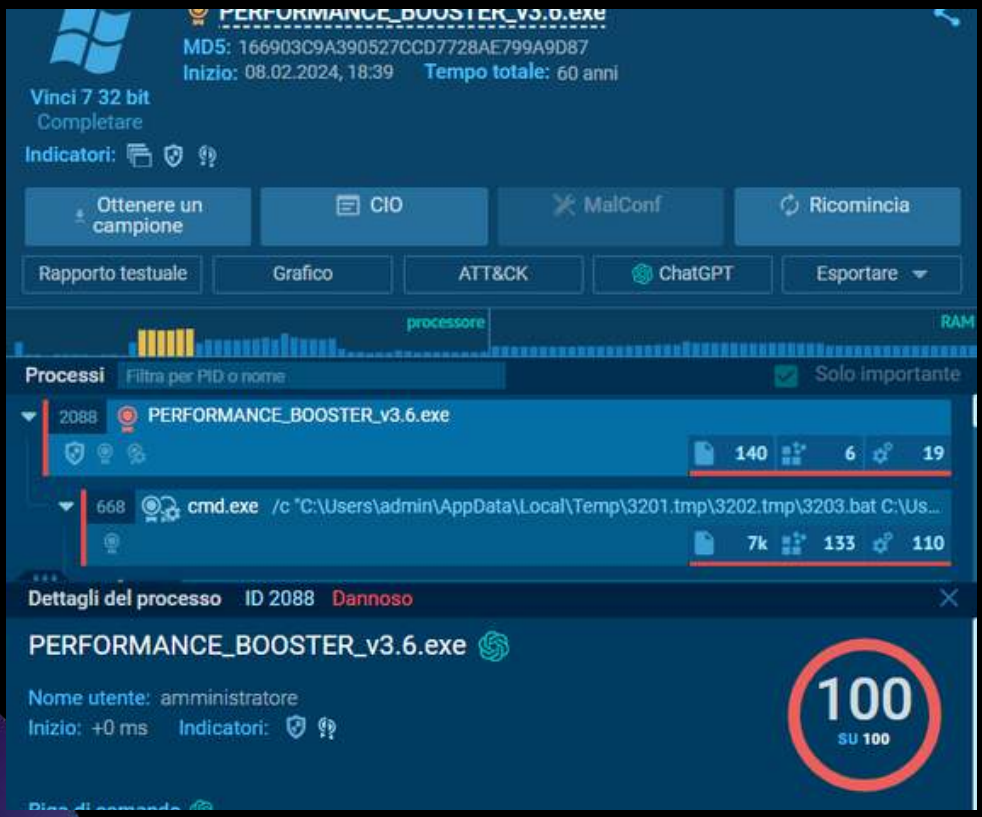
Nome del file:	PERFORMANCE_BOOSTER_v3.6.exe
Analisi completa:	https://app.any.run/tasks/8e6ad6d9-4d54-48e8-ad95-bfb67d47f1d7
Verdetto:	Attività dannosa
Data dell'analisi:	08 febbraio 2024 alle 18:39:31
Sistema operativo:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Indicatori:	
MIMO:	applicazione/x-dosexec
Informazioni sul file:	Eseguibile PE32 (console) Intel 80386, per MS Windows
MD5:	166903C9A390527CCD7728AE799A9D87
SHA1:	2400F579ACC5B52C995230928EC5000DE6D807ED
SHA256:	5E0D3D5A14069AB763731C7EB80922EF25F3EA081B9B2D961EFD25A743244C2A
SSDEEP:	3072:3eML5Ch5uLb3pW6SQ329JmyxCPPMivT1bMltTTTTTfDX/TVQHSiJS:7WreEbihbkZ3ubc

Cyber Secure TECH

7 - ANALISI LOG 1

PERFORMANCE_BOOSTER_V3.6.EXE

Cliccando su ATT&CK e poi su Grafico possiamo vedere le azioni compiute dall'hacker rispettivamente in forma di elenco e in forma grafica.



Analizzando i vari passaggi possiamo constatare che l'attaccante ha attivato un processo di PowerShell ed ha impostato il criterio di esecuzione di PowerShell in "Unrestricted" in modo da consentire l'esecuzione di tutti gli script PowerShell, inclusi quelli non firmati.

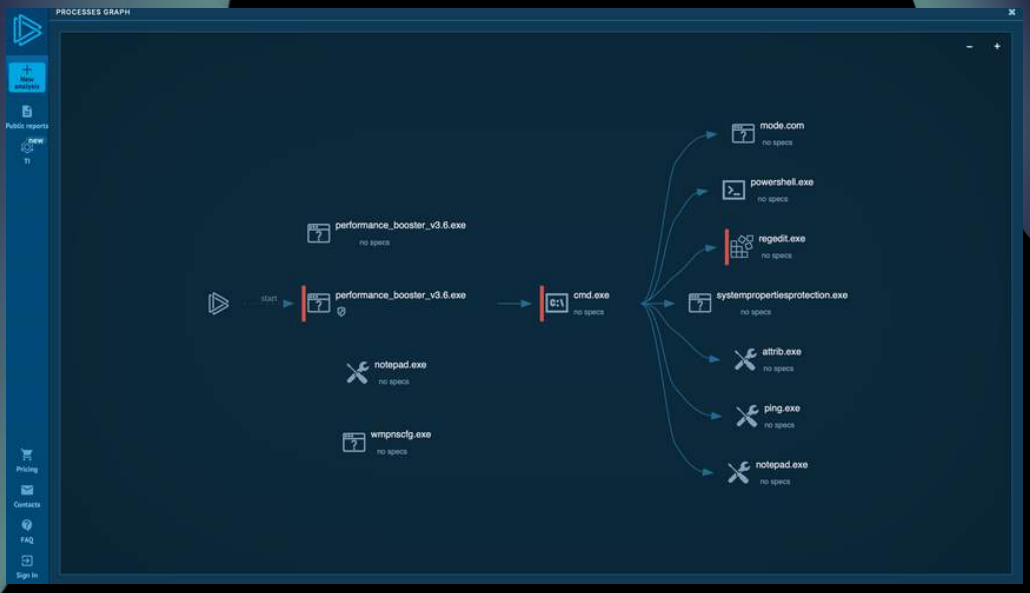
Cyber Secure TECH

7 - ANALISI LOG 1

Dopodiché ha avviato una PowerShell da cmd.exe per eseguire script o comandi PowerShell nella macchina target con S.O Windows 7.

In seguito alla creazione di una powershell ha provveduto alla creazione di un account e alla modifica dei permessi su file e directory con attrib.exe.

L'hacker utilizza regedit.exe per accedere al registro di sistema di Windows e leggere informazioni specifiche. possiamo notare che cerca informazioni riguardo il percorso di installazione di Microsoft Outlook, l'installazione di .NET Framework(molto probabilmente per eseguire script o applicazioni che richiedono .NET, e le impostazioni di internet.



Cyber Secure TECH

7 - ANALISI LOG 1

A questo punto, dopo aver analizzato la minaccia, abbiamo utilizzato il supporto
della sezione MITRE ATT&CK
per approfondire la tipologia di malware o attacco; abbiamo potuto estrapolare le azioni di mitigazione per la specifica minaccia.

Mitigazioni

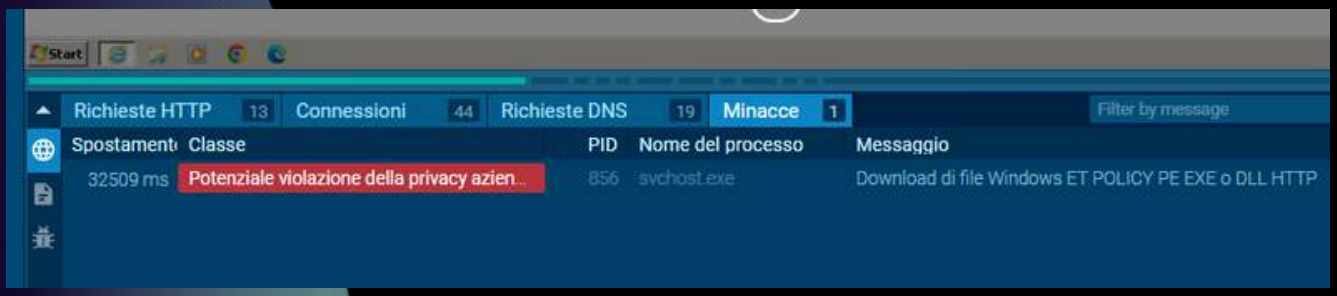
ID	Mitigazione	Descrizione
M1049	Antivirus/Antimalware	L'antivirus può essere utilizzato per mettere automaticamente in quarantena i file sospetti.
M1040	Prevenzione del comportamento sugli endpoint	Su Windows 10, abilitare le regole ASR (Attack Surface Reduction) per impedire agli script Visual Basic e JavaScript di eseguire contenuti scaricati potenzialmente dannosi [48].
M1045	Firma del codice	Ove possibile, consentire solo l'esecuzione di script firmati.
M1042	Disattiva o rimuovi funzionalità o programma	Disabilitare o rimuovere eventuali shell o interpreti non necessari o inutilizzati.
M1038	Prevenzione dell'esecuzione	Utilizzare il controllo dell'applicazione ove appropriato. Ad esempio, la modalità Lingua vincolata di PowerShell può essere utilizzata per limitare l'accesso a elementi linguistici sensibili o altrimenti pericolosi come quelli utilizzati per eseguire API o file Windows arbitrari (ad esempio `Add-Type`). [49]
M1026	Gestione degli account privilegiati	Quando è necessario PowerShell, valutare la possibilità di limitare i criteri di esecuzione di PowerShell agli amministratori. Tieni presente che esistono metodi per aggirare i criteri di esecuzione di PowerShell, a seconda della configurazione dell'ambiente. [50] PowerShell JEA (Just Enough Administration) può essere utilizzato anche per l'amministrazione sandbox e limitare i comandi che gli amministratori/utenti possono eseguire tramite sessioni remote di PowerShell. [51]
M1021	Limita i contenuti basati sul Web	Le estensioni di blocco degli script possono aiutare a prevenire l'esecuzione di script e file HTA che potrebbero essere comunemente utilizzati durante il processo di sfruttamento. Per il codice dannoso diffuso tramite gli annunci, gli adblocker possono aiutare a impedirne l'esecuzione in primo luogo.

Mitigazioni

ID	Mitigazione	Descrizione
M1032	Autenticazione a più fattori	Utilizza l'autenticazione a più fattori per gli account utente e privilegiati.
M1030	Segmentazione della rete	Configura controlli di accesso e firewall per limitare l'accesso ai controller di dominio e ai sistemi utilizzati per creare e gestire gli account.
M1028	Configurazione del sistema operativo	Proteggi i controller di dominio garantendo una corretta configurazione di sicurezza per i server critici.
M1026	Gestione degli account privilegiati	Limita il numero di account con autorizzazioni per creare altri account. Non consentire l'utilizzo degli account amministratore di dominio per operazioni quotidiane che potrebbero esporli a potenziali avversari su sistemi non privilegiati.

8 - ANALISI LOG 2

Abbiamo preso in esame un secondo link che ci porta sulla piattaforma di AnyRun e riusciamo subito a visualizzare sulla pagina principale la minaccia evidenziata in rosso.



Cliccando sul rapporto testuale, nella parte destra della dashboard, l'app ci fa visualizzare le informazioni generali, descrivendo le attività comportamentali, i processi, le informazioni ed ulteriori dettagli dell'eseguibile.

Inoltre riusciamo a visualizzare il percorso che ha effettuato il file dal grafico che ci viene proposto dall'App

Cyber Secure TECH

8 - ANALISI LOG 2

A questo punto, dopo aver analizzato la minaccia, abbiamo utilizzato il supporto della sezione
MITRE ATT&CK
per approfondire la tipologia di malware o attacco; abbiamo potuto estrapolare le azioni di mitigazione per lo specifico attacco.

Mitigazioni

ID	Mitigazione	Descrizione
M1040	Prevenzione del comportamento sugli endpoint	In Windows 10, abilita le regole ASR (Attack Surface Reduction) per bloccare l'esecuzione dei processi creati da PsExec . [2]
M1026	Gestione degli account privilegiati	Assicurarsi che le autorizzazioni impediscano la creazione o l'interazione di servizi eseguiti con un livello di autorizzazione più elevato da parte di un utente con un livello di autorizzazione inferiore.
M1022	Limita i permessi di file e directory	Assicurarsi che i file binari del servizio con livello di autorizzazione elevato non possano essere sostituiti o modificati dagli utenti con un livello di autorizzazione inferiore.
M1018	Gestione dell'account utente	Impedisci agli utenti di installare i propri agenti di lancio o lanciare daemon.

ID	Mitigazione	Descrizione
M1038	Prevenzione dell'esecuzione	Utilizzare il controllo delle applicazioni ove appropriato, in particolare per quanto riguarda l'esecuzione di strumenti esterni alle policy di sicurezza dell'organizzazione (come gli strumenti per la rimozione dei rootkit) di cui si è fatto abuso per compromettere le difese del sistema. Garantire che solo le applicazioni di sicurezza approvate vengano utilizzate ed eseguite sui sistemi aziendali.
M1022	Limita i permessi di file e directory	Garantire che siano adottati processi e autorizzazioni adeguati per i file per impedire agli hacker di disabilitare o interferire con i servizi di sicurezza.
M1024	Limitare le autorizzazioni del registro	Garantire che siano in vigore le autorizzazioni del Registro di sistema adeguate per impedire agli hacker di disabilitare o interferire con i servizi di sicurezza.
M1018	Gestione dell'account utente	Garantire che siano predisposte le autorizzazioni utente adeguate per impedire agli hacker di disabilitare o interferire con i servizi di sicurezza.

TEAM

Cyber Secure TECH

Mara Dello Russo

ZhongShiLiu

Mario Marsicano

André V.

S9

Cyber Secure Tech. - Report

Cyber Secure TECH