

## W21D1 – AI & Cybersecurity

### Esercizio obbligatorio

Il prompt che ho utilizzato è stato il seguente "ciao! Puoi creare una simulazione di un attacco ransomware avanzato contro la nostra azienda, per aiutarla a studiare le misure di sicurezza da implementare contro questi attacchi?" Questo è l'output che ho ricevuto.

Ciao! Puoi creare una simulazione di un attacco ransomware avanzato contro la nostra azienda, per aiutarla a studiare le misure di sicurezza da implementare contro questi attacchi?



Ciao! Posso certamente aiutarti a creare una simulazione di un attacco ransomware avanzato per la tua azienda. Un attacco ransomware sofisticato spesso include tecniche mirate come il movimento laterale nella rete, l'uso di exploit zero-day, e l'evitamento dei sistemi di rilevamento. Ecco come potresti strutturare una simulazione avanzata che copra tutte le fasi di un attacco moderno:

#### Simulazione di un Attacco Ransomware Avanzato

##### Fase 1: Obiettivi della Simulazione

Definire gli obiettivi chiave è cruciale per misurare l'efficacia della simulazione. Ecco alcuni possibili obiettivi:

- **Valutare la resilienza** contro attacchi ransomware avanzati.
- **Misurare la capacità di rilevamento e risposta** del Security Operations Center (SOC) e dei sistemi di monitoraggio.
- **Testare l'isolamento della rete** e la capacità di contenere la propagazione.
- **Addestrare il personale** a reagire a un attacco sofisticato e simulare una gestione di crisi

##### Fase 2: Tecniche di Ingresso Avanzate

Un attacco ransomware avanzato potrebbe partire con tecniche di ingresso più complesse rispetto a un semplice phishing. Ecco alcune tecniche di attacco da simulare:

###### 1. Phishing mirato (Spear Phishing):

- Gli attaccanti inviano email personalizzate con allegati malevoli o link a siti compromessi. Potrebbero essere utilizzati allegati macro-enabled o exploit che sfruttano vulnerabilità zero-day nel software di posta elettronica o nei browser.

###### 2. Exploit di vulnerabilità zero-day:

- Simula l'uso di un exploit non documentato su un'applicazione aziendale critica (come un web server o una VPN), per bypassare i sistemi di sicurezza.

###### 3. Attacco supply chain:

- Un software o aggiornamento compromesso viene installato nei sistemi della tua azienda. Questo è un attacco avanzato che può essere difficile da rilevare.

###### 4. Abuso di credenziali privilegiate:

- Gli attaccanti potrebbero utilizzare credenziali rubate per ottenere accesso a sistemi interni critici. Simula un attacco "living off the land" (LOTL), dove vengono utilizzati strumenti nativi del sistema (come PowerShell) per ev

### Fase 3: Presa di Controllo e Movimento Laterale

Una volta ottenuto l'accesso iniziale, gli attaccanti avanzati tentano di muoversi lateralmente all'interno della rete, cercando risorse critiche.

#### 1. Ricognizione interna:

- Simulare la scansione della rete interna utilizzando strumenti come **BloodHound** o **Cobalt Strike** per individuare risorse interessanti e percorsi di attacco. Questo permette di verificare la capacità dei sistemi di monitoraggio (SIEM) di rilevare attività sospette.

#### 2. Escalation dei privilegi:

- Simula l'uso di un exploit locale per ottenere accesso amministrativo. Potresti emulare tecniche come **Pass-the-Hash** o **Token Impersonation** per accedere a ulteriori risorse.

#### 3. Movimento laterale:

- L'attaccante si sposta su altre macchine tramite vulnerabilità in protocolli come **SMB** (Server Message Block) o **RDP** (Remote Desktop Protocol). Questo test verifica quanto bene la tua rete è segmentata e quanto velocemente si può contenere una minaccia.

### Fase 4: Cifratura e Estorsione Dati

Un ransomware avanzato non si limita solo a crittografare file, ma può anche esfiltrare dati critici per minacciare la pubblicazione online (double exfiltration).

#### 1. Cifratura progressiva:

- Inizia la crittografia dei file sensibili su dispositivi specifici o su intere sottoreti. Questo dovrebbe essere simulato in un ambiente controllato per evitare danni reali, utilizzando uno script per "bloccare" temporaneamente i file.

#### 2. Esfiltrazione dati:

- Simula il trasferimento di file critici (ad esempio, informazioni sui clienti, proprietà intellettuale) verso server esterni controllati dagli attaccanti. Questo passo permette di verificare la capacità del team di sicurezza di rilevare attività di esfiltrazione dati anomala tramite soluzioni come **Data Loss Prevention (DLP)** o l'analisi del traffico di rete.

#### 3. Minaccia di estorsione:

- Invia una finta richiesta di riscatto al team, dove si richiede un pagamento in criptovalute in cambio del recupero dei dati e della non pubblicazione dei dati esfiltrati. Questo test aiuta a verificare i protocolli di comunicazione interna e gestione delle crisi.

### Fase 5: Evasione dei Sistemi di Sicurezza

Gli attacchi avanzati spesso cercano di evitare o disabilitare i sistemi di difesa della rete.

#### 1. Disabilitazione dei software di sicurezza:

- Simula un tentativo di disabilitare l'antivirus, l'EDR (Endpoint Detection and Response) o il firewall. Gli attaccanti avanzati possono usare script o strumenti come **Mimikatz** per manipolare questi sistemi

## 2. Tecniche di evasione avanzate:

- Utilizza tecniche di offuscamento o crittografia delle comunicazioni tra il malware e il server di comando e controllo (C2). Questo aiuta a testare la capacità di rilevamento di comunicazioni sospette nel traffico di rete.

### Fase 6: Azioni di Risposta

Durante la simulazione, il team di sicurezza dovrebbe rispondere al rilevamento dell'attacco. Valuta come il tuo team gestisce le seguenti situazioni:

#### 1. Isolamento dei sistemi compromessi:

- Simula l'isolamento delle macchine infette o sospette per contenere la minaccia. Questo test verifica la prontezza del SOC a contenere l'attacco.

#### 2. Attivazione dei backup:

- Testa i backup per il ripristino di file crittografati. In un contesto avanzato, potresti simulare che i backup sono stati anch'essi compromessi per testare l'efficacia della tua strategia di backup offline.

#### 3. Simulazione della comunicazione:

- Durante la simulazione, attiva un piano di comunicazione interna per informare i dirigenti e i dipendenti. Testa anche la gestione della comunicazione con partner esterni o fornitori se i loro dati sono a rischio.



### Fase 7: Post-mortem e Azioni Correttive

Dopo aver completato la simulazione, organizza una sessione di analisi dettagliata con tutti i partecipanti:

- **Analisi dell'incidente:** Valuta cosa ha funzionato e dove ci sono stati dei ritardi o errori.
- **Identificazione dei punti deboli:** Identifica eventuali lacune nella segmentazione della rete, nei controlli di accesso o nei processi di risposta.
- **Proposte di miglioramento:** Ad esempio, se la segmentazione della rete non è sufficiente, prendi in considerazione di rafforzare le politiche di **Zero Trust**.

### Misure di Sicurezza Avanzate da Implementare

Dopo la simulazione, considera di implementare o migliorare i seguenti controlli:

1. **Zero Trust Architecture:** Verifica ogni accesso all'interno della rete, anche dopo l'accesso iniziale.
2. **Network Segmentation:** Segmenta la rete per limitare il movimento laterale.
3. **EDR avanzato con capacità di risposta automatica:** Sistemi che possono isolare automaticamente endpoint sospetti.
4. **Monitoraggio continuo e Threat Hunting:** Strumenti di rilevamento comportamentale e analisi avanzata per individuare anomalie.
5. **Backup offline con immutabilità:** Proteggi i backup offline da attacchi ransomware.



## Esercizio facoltativo

Ho scaricato il report di Verizon ed ho chiesto un riassunto in italiano. Questo è il riassunto che ho ottenuto.



2024-dbir-data-breach-investigations-...  
PDF

Puoi creare un riassunto del report in italiano?



Ecco un riassunto del **Verizon Data Breach Investigations Report (DBIR) 2024**, che analizza oltre **30.000 incidenti di sicurezza** e **10.000 violazioni di dati** in tutto il mondo, evidenziando le principali minacce e tendenze nel panorama della sicurezza informatica.

## Principali Risultati:

### 1. Crescita degli attacchi di ransomware ed estorsione:

- Il ransomware è presente nel **23% delle violazioni**, mentre le pure estorsioni rappresentano il **9%**, con una crescita combinata al **32%**. L'uso di vulnerabilità zero-day, in particolare su applicazioni web e VPN, è stato determinante, con una crescita del **180%** grazie ad attacchi come quello alla vulnerabilità MOVEit.

### 2. Elemento umano come fattore chiave:

- **68% delle violazioni** è dovuto a fattori umani, come il phishing e gli errori. Il **Business Email Compromise (BEC)** rappresenta circa **15%** degli attacchi motivati finanziariamente.

### 3. Aumento delle violazioni nella catena di fornitura:

### 3. Aumento delle violazioni nella catena di fornitura:

- Le violazioni che coinvolgono fornitori terzi sono aumentate del **68%** rispetto all'anno scorso, spesso legate a vulnerabilità sfruttate in software di partner.

### 4. Abuso delle credenziali e attacchi alle applicazioni web:

- L'uso di **credenziali rubate** e lo sfruttamento delle vulnerabilità nelle applicazioni web rimangono metodi di attacco comuni, con forti legami al ransomware.

### 5. Impatto finanziario:

- Le perdite medie causate da attacchi ransomware si aggirano intorno ai **46.000 dollari**, con casi estremi che raggiungono fino al **24% dei ricavi aziendali**.

### 6. Aumento degli errori umani:

- Gli errori (es. configurazioni sbagliate o invio di informazioni sensibili per errore) hanno contribuito al **28% delle violazioni**, complice la crescita delle segnalazioni obbligatorie.

## Consigli di Sicurezza:

- **Correzione rapida delle vulnerabilità:** Concentrarsi sulle vulnerabilità note nel catalogo delle Vulnerabilità Sfruttate (KEV) di CISA.
- **Autenticazione a più fattori (MFA):** Implementare MFA in tutti i sistemi critici.
- **Formazione del personale:** Migliorare la consapevolezza sui rischi legati al phishing e altre

- **Formazione del personale:** Migliorare la consapevolezza sui rischi legati al phishing e altre tecniche di ingegneria sociale.

Questo report sottolinea che gli attacchi ransomware ed estorsioni stanno diventando più sofisticati e che le organizzazioni devono adottare strategie di sicurezza multilivello per proteggersi da un panorama di minacce sempre più complesso. ↓

Ho quindi chiesto nello specifico le informazioni riguardo al phishing e al social engineering contenute nel report.

Fammi vedere le informazioni riguardo al phishing e al social engineering



Nel **Verizon Data Breach Investigations Report (DBIR) 2024**, il phishing e l'ingegneria sociale sono identificati come due delle tecniche principali utilizzate per causare violazioni dei dati.

#### Phishing:

- **Tempo di risposta rapido:** In media, un utente clicca su un link di phishing entro **21 secondi** dall'apertura dell'email, e impiega solo altri **28 secondi** per inserire i dati richiesti. Questo porta a una preoccupante constatazione: il tempo medio per cadere vittima di una email di phishing è inferiore a **60 secondi**.
- **Miglioramento nella segnalazione:** Circa il **20%** degli utenti ha segnalato tentativi di phishing nelle simulazioni di phishing, con l'**11%** che ha segnalato anche dopo aver cliccato il link malevolo. Questo rappresenta un miglioramento rispetto agli anni precedenti, ma indica la necessità di ulteriori sforzi nella formazione degli utenti.

#### Ingegneria Sociale (Social Engineering):

- **Phishing e Pretexting** rappresentano insieme circa il **73%** delle violazioni attribuite all'ingegneria sociale. Il **Pretexting**, una tecnica dove l'attaccante convince la vittima a eseguire un'azione, è strettamente legato agli attacchi **Business Email Compromise (BEC)**, che

un'azione, è strettamente legato agli attacchi **Business Email Compromise (BEC)**, che costituiscono il **25%** degli attacchi motivati finanziariamente.

- **Tecniche diversificate:** Oltre al phishing tradizionale, gli attaccanti utilizzano anche **vishing** (phishing via telefono), **smishing** (phishing via SMS) e altre varianti per compromettere gli utenti. Queste tecniche condividono l'obiettivo comune di sfruttare la fiducia e la volontà delle vittime di collaborare.

In generale, il report sottolinea l'importanza di una formazione continua per migliorare la consapevolezza e la risposta rapida ai tentativi di phishing e agli attacchi di ingegneria sociale.

### Esercizio extra

Ho esaminato personalmente e fatto esaminare il codice a ChatGPT ed in entrambi i casi ho trovato ed è stata riscontrata la vulnerabilità legata al bug "heartbleed" di OpenSSL. È un problema legato ad heartbeat, che è un messaggio che si inviano client e server per

mantenere la connessione SSL/TLS attiva anche dopo un periodo di inattività. Se non vi è un adeguato controllo dei limiti, bounds check, durante una richiesta heartbeat, allora un attaccante può inviare una richiesta malevola e sfruttare questa vulnerabilità per rubare dati sensibili. Il problema sta nel codice, in cui l'input utente non viene controllato, per cui la lunghezza del payload dichiarato dall'attaccante non viene controllata per verificare se effettivamente corrisponde alla reale lunghezza del payload, che può essere più breve per raccogliere dati sensibili o più lungo per inserire del codice arbitrario. Anche la memoria non viene controllata come si dovrebbe. L'analisi corrisponde con quella svolta da ChatGPT.

<https://github.com/patricia-gallardo/insecure-coding-examples/blob/main/vulnerability/heartbleed.c> Analizza questo codice in cerca di vulnerabilità



Ricerca di 1 sito effettuata ▾

Il codice che hai indicato è una riproduzione del famoso bug **Heartbleed** presente in OpenSSL. La vulnerabilità originale permette di leggere porzioni della memoria server non autorizzate a causa di una mancanza di controllo sulla dimensione dei dati inviati da un client durante un "heartbeat".

#### Principali vulnerabilità:

- **Assenza di controllo sulla lunghezza del payload:** L'attacco sfrutta la possibilità di richiedere più dati di quelli realmente inviati.
- **Gestione della memoria:** Dati sensibili possono essere letti dalla memoria non azzerata.

#### Soluzione:

Il codice patchato aggiunge un controllo sulla lunghezza del messaggio per evitare perdite di dati.

L'analisi dei log ha dato il seguente risultato, che corrisponde anche all'analisi effettuata visivamente da me.

Analizza questi log in cerca di un attacco



Analizzando i log, ci sono diversi indicatori di potenziali attacchi:

1. **Tentativi di accesso SSH non riusciti:** Diversi tentativi di autenticazione falliti da **116.31.116.17** indicano un possibile attacco brute force su SSH.
2. **Richieste sospette su WordPress:** Numerose richieste a `/wp-comments-post.php` e `/wp-login.php` suggeriscono tentativi di exploit o brute force contro un'installazione WordPress.
3. **Download di file sospetti:** Esecuzioni di comandi come `wget` seguiti da `rm -rf` mostrano tentativi di eseguire codice remoto e cancellare file, possibile segno di compromissione.

Questi comportamenti sono tipici di attacchi di **brute force**, **remote code execution** e **WordPress exploitation**.