

REPORT S5/L4

Obiettivo

Esplorare le tecniche di social engineering e imparare come difendersi da questi tipi di attacchi. Questo esercizio vi guiderà attraverso la comprensione delle varie forme di social engineering, esempi reali di attacchi e strategie di difesa efficaci.

Descrizione dell'attività

Dovrete scrivere un prompt per ChatGPT che vi permetta di ottenere informazioni dettagliate sulle tecniche di social engineering. Analizzate gli esempi forniti e sviluppate una serie di raccomandazioni per prevenire tali attacchi. Infine, create una presentazione o un documento che riassuma le vostre scoperte e raccomandazioni.

1. COMPRENDERE IL SOCIAL ENGINEERING

Prompt: "Ciao! Sono uno studente di cybersecurity di Eicode. Oggi abbiamo studiato il social engineering, l'obiettivo dell'esercizio odierno è quello di esplorare le tecniche di social engineering e imparare a difendersi da questi tipi di attacchi. Per prima cosa vorrei chiederti se potresti fornirmi una panoramica sul social engineering e sulle tecniche più comuni utilizzate dagli attaccanti."

Output: Il **Social Engineering** (ingegneria sociale) è una delle aree più affascinanti e pericolose della cybersecurity, perché non mira a violare le macchine, ma a "hackerare" le persone.

Spesso si dice che l'essere umano sia l'anello debole della catena di sicurezza (il "fattore umano"). Ecco una panoramica strutturata per il tuo esercizio.

Che cos'è il Social Engineering?

Il Social Engineering è l'arte di manipolare le persone affinché compiano azioni specifiche o divulghino informazioni riservate. A differenza degli attacchi tecnici (come exploit o brute-force), l'ingegneria sociale sfrutta la **psicologia umana** (fiducia, paura, urgenza, curiosità) per aggirare le difese tecnologiche.

Le Tecniche più Comuni

Gli attaccanti utilizzano diverse metodologie, che spaziano dal digitale al fisico. Ecco le principali che dovresti conoscere:

1. Phishing (e le sue varianti)

È la tecnica più diffusa. Consiste nell'inviare comunicazioni fraudolente (solitamente email) che sembrano provenire da fonti affidabili.

- **Mass Phishing:** Email generiche inviate a migliaia di persone (es. "Il tuo pacco è bloccato").
- **Spear Phishing:** Attacchi mirati verso un individuo o un'azienda specifica, utilizzando informazioni personalizzate per sembrare più credibili.
- **Whaling:** Un attacco di Spear Phishing rivolto a "pesci grossi" (CEO, CFO) per ottenere accessi di alto livello o trasferimenti di denaro.

2. Vishing (Voice Phishing)

L'attaccante utilizza il **telefono**. Spesso falsificano l'ID chiamante (spoofing) per sembrare un'entità legittima (es. supporto tecnico della banca o Microsoft) e convincono la vittima a fornire credenziali o installare malware.

3. Smishing (SMS Phishing)

Simile al phishing, ma avviene tramite **SMS** o app di messaggistica (WhatsApp). Sono brevi, urgenti e contengono link malevoli (es. "Il tuo conto verrà sospeso, clicca qui").

4. Pretexting (Creazione di un pretesto)

L'attaccante crea uno scenario inventato (un "pretesto") per ottenere informazioni.

Esempio: Un attaccante si finge un dipendente dell'IT che ha bisogno della tua password per "fare un aggiornamento urgente" o un sondaggista che chiede la data di nascita per una verifica.

5. Baiting (L'esca)

Sfrutta la curiosità o l'avidità della vittima.

- **Fisico:** L'attaccante lascia una chiavetta USB infetta con etichette interessanti (es. "Stipendi Dirigenti 2024") in un parcheggio o in mensa. Se inserita nel PC aziendale, installa un malware.
- **Digitale:** Download gratuiti di software o film che in realtà contengono trojan.

6. Quid Pro Quo (Do ut des)

L'attaccante promette un beneficio in cambio di informazioni o accesso.

Esempio: Un attaccante chiama a caso i numeri interni di un'azienda fingendosi il supporto tecnico, finché non trova qualcuno che ha davvero

un problema al PC. "Ti aiuto a risolverlo, ma prima disabilita l'antivirus e dammi la password".

7. Tailgating / Piggybacking

È una tecnica fisica. L'attaccante segue una persona autorizzata attraverso una porta sicura (badge o codice). Spesso l'attaccante ha le mani impegnate (scatoloni, caffè) e fa leva sulla gentilezza della vittima che gli tiene aperta la porta.

Le Leve Psicologiche

Tutte queste tecniche funzionano perché attivano specifici *bias* cognitivi:

1. **Urgenza:** "Fallo subito o perdi l'account!" (toglie tempo per ragionare).
2. **Autorità:** "Sono il CEO, esegui il bonifico" (difficile dire di no a un capo).
3. **Fiducia/Simpatia:** L'attaccante è gentile e disponibile.
4. **Paura:** "Sei sotto indagine".

2. STRATEGIE DI DIFESA

Prompt: "Ora vorrei chiederti se puoi suggerirmi e spiegarmi delle strategie e migliori pratiche per difendersi dagli attacchi di social engineering."

Output: Certamente. Questa è la parte più critica: trasformare la teoria in abitudini pratiche.

Poiché il Social Engineering aggira i firewall tecnici attaccando la mente umana, la difesa principale è **costruire un "Human Firewall"** (un firewall umano). La difesa non è mai solo software, ma un mix di **Tecnologia, Processi e Comportamento**.

Ecco le strategie fondamentali e le *best practices* per difendersi, divise per categoria.

1. Strategie Comportamentali (Mindset)

Queste sono abitudini mentali che devi sviluppare per riconoscere l'inganno prima di agire.

- **Rallenta e Verifica (La regola dello STOP):** Gli attacchi fanno leva sull'urgenza. Se ricevi una richiesta che ti mette pressione ("Fallo subito", "Scade tra 10 minuti"), fermati. Fai un respiro profondo. L'urgenza è quasi sempre un segnale di attacco.

- **Verifica "Out-of-Band" (Fuori banda):** Questa è la tecnica di difesa più potente. Se ricevi una mail strana dal tuo CEO o dalla banca, **non rispondere a quella mail.**
Come fare: Contatta il mittente attraverso un *canale diverso e sicuro*. Chiama il numero ufficiale della banca (non quello nella mail) o scrivi al CEO su Teams/Slack per chiedere: "Hai inviato tu questa richiesta?".
- **Scetticismo Sano (Zero Trust):** Non fidarti ciecamente dell'ID chiamante o del nome visualizzato nell'email. È banale falsificare un numero di telefono o un indirizzo mittente (*spoofing*).
- **Analisi dei Link (Hovering):** Prima di cliccare su qualsiasi link, passa il cursore del mouse sopra di esso (senza cliccare) per vedere l'URL reale di destinazione. Se la mail dice "Poste Italiane" ma il link punta a www.aggiornamento-sicurezza-xyz.com, è phishing.

2. Strategie Tecniche

Strumenti che riducono il rischio nel caso in cui l'errore umano avvenga.

- **MFA (Autenticazione a Più Fattori): Fondamentale.** Anche se un ingegnere sociale riesce a rubarti la password tramite phishing, se hai la MFA attiva (codice via app, token fisico o biometria), l'attaccante non potrà accedere al tuo account.
- **Filtri Antispam e Antiphishing:** Assicurati che il client di posta e il browser abbiano i filtri attivi. Spesso segnalano i siti malevoli in rosso.
- **Gestione delle Password:** Non usare mai la stessa password per servizi diversi. Se cadi in una trappola di phishing su un sito meno sicuro, l'attaccante proverà quella password su tutti gli altri tuoi account (Credential Stuffing). Usa un *Password Manager*.

3. OpSec (Sicurezza Operativa) e Privacy

Meno informazioni dai, meno l'attaccante può essere credibile.

- **Igiene sui Social Media (OSINT Defense):** Gli attaccanti studiano i tuoi profili (LinkedIn, Instagram) per creare attacchi *Spear Phishing*.
Esempio: Se posti "Felice di essere a Roma per la conferenza Cyber", un attaccante potrebbe chiamare il tuo ufficio dicendo: "Sono alla conferenza con [Tuo Nome], mi ha chiesto di farmi mandare quel file urgente...".
○ **Consiglio:** Restringi la privacy dei tuoi profili e non condividere dettagli sensibili sul lavoro o spostamenti in tempo reale.
- **Clean Desk Policy (Scrivania Pulita):** In ufficio, non lasciare documenti sensibili sulla scrivania e non scrivere password su post-it attaccati al monitor.
- **Distruzione dei Documenti (Shredding):** I documenti cartacei con dati personali o aziendali vanno distrutti col trita-carte, mai gettati interi nel cestino (per evitare il *Dumpster Diving*, ovvero frugare nella spazzatura).

4. Sicurezza Fisica

- **Anti-Tailgating:** Se hai un badge per entrare in ufficio, non tenere la porta aperta a sconosciuti, anche se sembrano gentili o hanno le mani occupate. È educato, ma insicuro. La risposta corretta è: "*Mi scusi, le policy mi impongono di non far entrare nessuno senza badge, deve passare dalla reception*".

Se ricevi...	Azione Difensiva
Email con richiesta urgente	Non cliccare. Chiama il mittente.
Telefonata dal "Supporto Tecnico" non richiesta	Riaggancia. Chiama tu il numero interno dell'IT.
Richiesta di password	Rifiuta. Nessun supporto legittimo chiede la tua password.
Chiavetta USB trovata a terra	Non inserirla nel PC. Portala all'IT o distruggila.
Vincita inaspettata (iPhone, Denaro)	Ignora. Se sembra troppo bello per essere vero, lo è.

3. ESPLORAZIONE DEI CVE

Prompt: "Per terminare l'esercizio, ho bisogno di raccogliere informazioni sui CVE di un software o sistema operativo a mia scelta. Io vorrei i CVE di Windows 10, potresti fornirmi una lista con tutti i suoi principali CVE fornendomi anche informazioni su quelli più critici, includendo anche i dettagli delle vulnerabilità e le soluzioni consigliate? "

Output: Passare dal "Social Engineering" (il fattore umano) ai **CVE** (Common Vulnerabilities and Exposures - il fattore tecnico) è il passo naturale per un analista di sicurezza.

Windows 10 ha migliaia di vulnerabilità storiche, ma per il tuo esercizio è fondamentale concentrarsi su quelle **recenti (2024-2025)** e **critiche**, poiché sono quelle che gli attaccanti stanno sfruttando attivamente *oggi*.

Ecco una selezione curata delle vulnerabilità più pericolose scoperte di recente per Windows 10, con i dettagli tecnici e le soluzioni.

Lista dei CVE Principali (Windows 10 - 2024/2025)

Qui ho selezionato tre vulnerabilità che rappresentano diverse tipologie di rischio: una che colpisce la rete (RCE), una legata a servizi specifici (MSMQ) e una che sfrutta proprio il Social Engineering.

1. CVE-2024-38063: La più critica (TCP/IP RCE)

Questa è probabilmente la vulnerabilità più grave degli ultimi mesi.

- **Gravità: Critica** (CVSS Score: **9.8/10**)
- **Tipo:** Remote Code Execution (RCE) - Esecuzione Remota di Codice.
- **Componente Colpito:** Windows TCP/IP Stack (specificamente **IPv6**).
- **Il Dettaglio Tecnico:** Esiste un errore di "Integer Underflow" nel modo in cui Windows gestisce pacchetti IPv6 appositamente creati. Un attaccante può inviare pacchetti IPv6 malevoli al tuo computer e ottenere il controllo totale del sistema (eseguire codice arbitrario a livello SYSTEM).
 1. *Nota spaventosa:* È "**Zero-Click**". Non serve che tu clicchi nulla o apra file. Basta che il PC sia connesso alla rete con IPv6 attivo.
- **Soluzione/Mitigazione:**
 1. **Patch:** Installare immediatamente gli aggiornamenti di sicurezza di Windows (rilasciati ad Agosto 2024).
 2. **Workaround:** Se non puoi aggiornare, **disabilita IPv6** nelle impostazioni della scheda di rete.

2. CVE-2024-30080: Il pericolo dei servizi nascosti (MSMQ)

Molte aziende usano servizi in background che dimenticano di avere attivi.

- **Gravità:** Critica (CVSS Score: 9.8/10)
- **Tipo:** RCE (Remote Code Execution).
- **Componente Colpito:** Microsoft Message Queuing (MSMQ)
- **Il Dettaglio Tecnico:** È una vulnerabilità di tipo "Use-After-Free". Se il servizio MSMQ è attivo (ascolta sulla porta 1801), un attaccante può inviare un pacchetto malevolo ed eseguire codice come amministratore.
- **Soluzione/Mitigazione:**
 1. **Verifica:** Controlla se il servizio "Microsoft Message Queuing" è in esecuzione sul tuo Windows 10 (spesso è spento di default, ma acceso in ambienti aziendali).
 2. **Patch:** Applica l'aggiornamento di Windows.
 3. **Workaround:** Disabilita il servizio MSMQ se non è strettamente necessario per le applicazioni aziendali.

3. CVE-2024-21412: L'alleato del Social Engineering

Questa inserisco specificamente perché si collega al tuo studio di oggi. È una vulnerabilità tecnica usata per rendere più efficaci gli attacchi di ingegneria sociale.

- **Gravità:** Alta (Sfruttata attivamente in attacchi "Zero-Day").
- **Tipo:** Security Feature Bypass (Aggiramento delle funzioni di sicurezza).
- **Componente Colpito:** Windows SmartScreen.
- **Il Dettaglio Tecnico:** Normalmente, se scarichi un file pericoloso da internet, Windows SmartScreen ti avvisa o lo blocca. Questa vulnerabilità permette agli attaccanti di creare speciali file scorciatoia ([.url](#)) che, se cliccati, scaricano ed eseguono malware **senza far scattare l'avviso di sicurezza** di SmartScreen.
 1. **Uso reale:** È stata usata dal gruppo hacker "Water Hydra" per diffondere trojan bancari nascondendoli in false immagini o documenti.
- **Soluzione:**
 1. **Patch:** Aggiornamento obbligatorio di Windows. Non esistono workaround efficaci oltre all'educazione dell'utente (non cliccare su link strani).

CVE ID	Punteggio (CVSS)	Tipo di Vulnerabilità	Descrizione Semplice	Soluzione Primaria
CVE-2024-38063	9.8 (Critico)	RCE (Rete)	Errore in IPv6 permette hackeraggio remoto senza interazione utente.	Aggiornamento Windows / Disabilitare IPv6.
CVE-2024-30080	9.8 (Critico)	RCE (Servizi)	Bug nel servizio Messaggistica (MSMQ) permette controllo totale.	Disabilitare servizio MSMQ / Patch.
CVE-2024-21412	8.1 (Alto)	Bypass Sicurezza	Permette ai virus di aggirare gli avvisi di Windows SmartScreen.	Aggiornamento Windows.