

S5 L4- ESERCITAZIONE

Cyber Security & Ethical Hacking

PROMPT CHATGPT

Per la risoluzione dell'esercizio utilizzo il seguente Prompt su ChatGPT

“Ciao, sono uno studente di cybersecurity potresti spiegare cosa è il social engineering e descrivere le tecniche più comuni utilizzate dagli attaccanti tra cui phishing e tailgating?”

Risposta:

Cos'è il Social Engineering

Il social engineering è un insieme di tecniche di attacco che sfruttano la manipolazione psicologica delle persone piuttosto che vulnerabilità tecniche dei sistemi. L'obiettivo dell'attaccante è indurre la vittima a compiere azioni dannose (ad esempio rivelare credenziali, concedere accessi, eseguire software malevolo) facendo leva su fattori umani come fiducia, paura, urgenza, curiosità o autorità.

In ambito cybersecurity, il social engineering è particolarmente pericoloso perché:

- aggira controlli tecnici avanzati;
- sfrutta l'anello più debole della sicurezza: l'essere umano;
- è difficile da rilevare con strumenti automatici.

Principi psicologici sfruttati:

Gli attaccanti fanno spesso leva su:

Autorità (fingendosi figure ufficiali o superiori);

Urgenza (creare pressione temporale);

Paura (minaccia di conseguenze);

Reciprocità (offrire qualcosa in cambio);

Curiosità (contenuti allettanti o riservati);

Abitudine e fiducia (routine lavorative).

Tecniche di Social Engineering più comuni

1. Phishing

Il phishing è una delle tecniche più diffuse. Consiste nell’invio di comunicazioni fraudolente che imitano fonti legittime (banche, aziende, servizi online) con lo scopo di rubare informazioni sensibili.

Caratteristiche principali:

uso di email, SMS (smishing), telefonate (vishing) o messaggi sui social;
link a siti web contraffatti;
richiesta di inserire credenziali, dati personali o finanziari.

Varianti rilevanti:

Spear phishing: attacco mirato a una persona o organizzazione specifica;

Whaling: targeting di figure di alto livello (CEO, CFO);

Clone phishing: copia di un'email legittima con allegati o link malevoli.

Esempio:

Un'email che sembra provenire dal reparto IT aziendale chiede di “verificare l’account” entro poche ore, fornendo un link a un falso portale di login.

2. Tailgating (o Piggybacking)

Il tailgating è una tecnica di social engineering fisico. L’attaccante ottiene accesso a un’area riservata seguendo una persona autorizzata, senza possedere credenziali valide.

Modalità tipiche:

fingere di aver dimenticato il badge;
portare oggetti ingombranti per indurre la vittima ad aprire la porta;
spacciarsi per personale esterno (manutentori, corrieri, tecnici).

Perché funziona:
sfrutta la cortesia e il senso di collaborazione;
molte persone evitano il confronto o il rifiuto.

Rischi:
accesso a infrastrutture critiche;
installazione di dispositivi malevoli;
furto di informazioni o hardware.

3. Pretexting

L’attaccante crea un pretesto credibile (una storia) per ottenere informazioni o accessi.

Esempio:
Fingendosi un nuovo dipendente del reparto IT, chiede credenziali “per risolvere un problema urgente”.

4. Baiting

Si basa sull’offerta di qualcosa di allettante.

Esempi:
chiavette USB infette lasciate in luoghi pubblici;
download gratuiti di software o contenuti pirata.

5. Quid Pro Quo

L’attaccante offre un servizio in cambio di informazioni.

Esempio:
Fingendosi supporto tecnico, offre assistenza in cambio delle credenziali di accesso.
Contromisure principali

Dal punto di vista difensivo, le strategie più efficaci includono:

formazione e awareness del personale;
procedure di verifica dell'identità;
principio del least privilege;
autenticazione multifattore (MFA);
politiche di sicurezza fisica rigorose;
simulazioni di phishing e audit periodici.

Chiedo successivamente a ChatGPT

“potresti elencare e spiegare alcune strategie efficaci per difendersi dagli attacchi di social engineering”

Risposta:

1. Formazione e Security Awareness

La **consapevolezza degli utenti** è la prima linea di difesa contro il social engineering.

- formazione periodica su phishing, vishing, smishing e tecniche emergenti;
- riconoscimento di segnali di allarme (urgenza, richieste anomale, errori nei messaggi);
- educazione alla verifica delle richieste anche quando sembrano legittime.

Un utente formato è meno incline a reagire impulsivamente.

2. Procedure di verifica dell'identità

È fondamentale stabilire **processi formali di verifica** prima di condividere informazioni o concedere accessi.

- verifica a più fattori dell'identità di chi richiede informazioni;
- policy che vietano la condivisione di credenziali via email o telefono;
- utilizzo di canali ufficiali per le richieste sensibili.

Questa misura riduce l'efficacia di pretexting e impersonation.

3. Autenticazione Multifattore (MFA)

L’MFA aggiunge un ulteriore livello di sicurezza oltre a username e password.

- anche in caso di furto delle credenziali, l’accesso risulta limitato;
 - riduce significativamente l’impatto del phishing;
 - particolarmente critica per account privilegiati e accessi remoti.
-

4. Principio del Minimo Privilegio

Ogni utente o sistema deve disporre **solo dei permessi strettamente necessari**.

- limita i danni in caso di compromissione;
 - riduce la superficie di attacco interna;
 - facilita il contenimento degli incidenti.
-

5. Simulazioni di Phishing e Test Periodici

Le simulazioni consentono di valutare il livello di preparazione reale degli utenti.

- campagne di phishing simulate;
- analisi dei comportamenti a rischio;
- feedback mirato e formazione correttiva.

Questo approccio migliora la resilienza nel tempo.

6. Sicurezza Fisica e Controllo degli Accessi

Il social engineering non è solo digitale.

- badge personali non cedibili;
- tornelli e sistemi anti-tailgating;
- politiche di “clean desk”;
- obbligo di accompagnamento per visitatori e fornitori.

Riduce il rischio di accessi non autorizzati.

7. Politiche e Procedure Chiare

Policy ben definite aiutano gli utenti a sapere **cosa è consentito e cosa no.**

- linee guida per la gestione delle informazioni sensibili;
- processi di escalation in caso di richieste sospette;
- documentazione facilmente accessibile.

La chiarezza riduce l'errore umano.

8. Strumenti Tecnologici di Supporto

Le contromisure tecniche restano un complemento fondamentale.

- filtri antispam e anti-phishing;
 - sandbox per allegati e link;
 - sistemi di email authentication (SPF, DKIM, DMARC);
 - logging e monitoraggio centralizzato.
-

9. Cultura della Sicurezza

Una cultura organizzativa orientata alla sicurezza è determinante.

- incoraggiare la segnalazione di incidenti senza penalizzazioni;
- promuovere un approccio “zero trust”;
- responsabilizzare ogni individuo.

Una cultura solida rende meno efficaci le tecniche manipolative.

10. Incident Response e Miglioramento Continuo

È essenziale essere preparati anche al fallimento delle difese.

- piani di risposta agli incidenti;
 - analisi post-evento (lessons learned);
 - aggiornamento continuo delle policy e della formazione.
-

Queste strategie, combinate tra loro, consentono di mitigare in modo significativo il rischio di attacchi di social engineering, affrontando sia il fattore umano sia quello tecnologico.

ESERCIZIO BONUS

Per l'esecuzione dell'esercizio bonus utilizzo un nuovo Prompt su una nuova chat con ChatGPT, la IA qui cita le fonti, in questo Report verranno trascritte con il colore blu

“Ciao sono uno studente di Cybersecurity potresti fornirmi una lista dei CVE riguardo windows 10 e i relativi dettagli delle vulnerabilità e soluzioni consigliate?”

Risposta:

- 1) CVE-2025-62221 — Windows Cloud Files Mini Filter Driver Elevation of Privilege

Tipologia: Escalation dei privilegi / Elevation of Privilege

Descrizione: vulnerabilità use-after-free nel driver “Cloud Files Mini Filter”, che può consentire a un attaccante di ottenere privilegi di sistema (SYSTEM) se sfruttata con successo. Questa falla è stata attivamente sfruttata in natura prima della patch.

[Tenable®](#)

Impatto: un attaccante locale può aumentare i propri privilegi fino a quelli amministrativi.

Soluzione/Mitigazione: installare gli aggiornamenti cumulativi di Dicembre 2025 Patch Tuesday tramite Windows Update o attraverso il Microsoft Update Catalog. Microsoft ha incluso la correzione nei pacchetti di sicurezza di dicembre 2025.

[Microsoft Learn](#)

- 2) CVE-2025-54100 — Windows PowerShell Invoke-WebRequest RCE

Tipologia: Remote Code Execution (RCE)

Descrizione: input non sanitizzato in Invoke-WebRequest in PowerShell potrebbe consentire a un attaccante di eseguire codice arbitrario con i privilegi dell'utente se l'utente visita contenuti malevoli.

[Malwarebytes](#)

Impatto: esecuzione remota di codice potenzialmente arbitrarie.

Soluzione/Mitigazione: applicare gli aggiornamenti di sicurezza di Dicembre 2025, rilasciati da Microsoft tramite Windows Update. Usare policy di esecuzione restrittive in PowerShell e disabilitare l'esecuzione di script non firmati nei profili di produzione.

[Microsoft Learn](#)

3) CVE-2025-64671 — GitHub Copilot for JetBrains RCE

Tipologia: Remote Code Execution

Descrizione: vulnerabilità di iniezione di comandi tramite Cross Prompt Injection nell'integrazione di GitHub Copilot nei prodotti JetBrains. Anche se non strettamente parte del core OS, è correlata al pacchetto sicurezza diffuso con Windows.

[The Hacker News](#)

Impatto: un utente locale malevolo potrebbe eseguire comandi non autorizzati.

Soluzione/Mitigazione: applicare gli aggiornamenti cumulativi di Dicembre 2025; limitare l'uso di estensioni AI integrate dove non richiesto; monitorare i processi PowerShell e i comandi eseguiti dai plugin di sviluppo.

4) CVE-2025-53779 — Windows Kerberos Elevation of Privilege

Tipologia: Escalation dei privilegi

Descrizione: vulnerabilità nel protocollo Kerberos di Windows che potrebbe consentire a un utente autenticato, con determinati permessi su attributi dMSA (Group Managed Service Accounts), di ottenere privilegi di Domain Administrator se sfruttata.

[Tom's Guide](#)

Impatto: elevazione dei privilegi all'interno di Active Directory.

Soluzione/Mitigazione: installare gli aggiornamenti di sicurezza di Agosto 2025 o successivi; assicurarsi che i controller di dominio siano aggiornati; ridurre i permessi sui dMSA e monitorare gli accessi anomali.

5) CVE-2025-33073 — Windows SMB Authentication Relay

Tipologia: RCE / Man-in-the-Middle tramite SMB

Descrizione: vulnerabilità nel protocollo SMB che può portare a esecuzione di codice o autenticazioni relay se non correttamente protetto. È stata inclusa nella lista CISA Known Exploited Vulnerabilities.

[TechRadar](#)

Impatto: compromissione di sistemi Windows non aggiornati con exploit SMB coercitivi.

Soluzione/Mitigazione: applicare patch di Giugno 2025 o successive; abilitare la firma SMB sulle reti interne; limitare l'esposizione SMB verso reti non fidate.

6) CVE-2024-43491 — Windows Update Servicing Stack Rollback Vulnerability

Tipologia: Impatto sugli aggiornamenti / Rollback dei fix

Descrizione: vulnerabilità nel servicing stack di Windows che potrebbe riportare componenti opzionali a versioni non corrette, annullando patch già applicate.

[nvd.nist.gov](#)

Impatto: i sistemi potrebbero perdere le protezioni precedenti se non gestiti correttamente.

Soluzione/Mitigazione: assicurarsi di avere il servicing stack più recente (installare aggiornamenti fino a data recente); verificare che le patch non siano state invalidate da rollback.

7) CVE-2024-21302 — Virtualization Based Security (VBS) EoP

Tipologia: Escalation dei privilegi

Descrizione: permette a un attaccante con privilegi amministrativi di sostituire file di sistema di VBS con versioni obsolete, potenzialmente reintroducendo vulnerabilità mitigate e bypassando protezioni VBS.

[nvd.nist.gov](#)

Impatto: compromissione delle protezioni VBS e possibile esfiltrazione di dati protetti.

Soluzione/Mitigazione: installare gli aggiornamenti di sicurezza che risolvono questa CVE (inclusi nei principali cumulative update Windows 10); bloccare rollback di VBS tramite policy e mantenere le build di sistema aggiornate.

Suggerimenti generali per la gestione delle CVE su Windows 10

1. Utilizzo continuo di Windows Update:

Il sistema di aggiornamenti cumulativi di Microsoft include tutte le correzioni per le CVE note; tenere sempre i sistemi aggiornati riduce l'esposizione a vulnerabilità note.

[Microsoft Learn](#)

2. Monitoraggio delle fonti ufficiali:

Per un inventario completo e aggiornato delle CVE di Windows 10, utilizzare il Microsoft Security Update Guide o il National Vulnerability Database (NVD) con query filtrate per prodotto “Windows 10”.

[simms-teach.com](#)

3. Incident response e mitigazione:

Configurare strumenti di EDR/XDR, applicare restrizioni di rete (ad esempio bloccare porte SMB non necessarie), abilitare la Credential Guard e la Virtualization Based Security dove possibile; monitorare i segnali di compromissione correlati alle CVE critiche e agli exploit in circolazione.