Pratica S5/L4

Obiettivo: l'obiettivo di questo esercizio è scrivere e utilizzare dei prompt efficaci per interagire con ChatGPT e ottenere informazioni precise su social engineering e CVE.

1) Social engineering e Tecniche di difesa

Prompt 1 (raccolta informazioni sul social engineering): ChatGPT, puoi spiegarmi in modo dettagliato il concetto di social engineering nel contesto della cybersecuirity. Descrvimi anche qualche tecnica comune utilizzate dagli attaccanti, includendo per ciascuna una breve spiegazione, un esempio pratico e dei segnali per individuare queste tecniche. Le tecniche che mi interessano sono: phishing, taigating, pretexting, vishing e baiting. Struttura la tua risposta in un formato chiaro, utlizzando magari elenchi puntati e tabelle.

Risultati:

Cos'è il Social Engineering?

- **Definizione**: Manipolazione psicologica finalizzata a ingannare le persone per ottenere accesso non autorizzato a dati, sistemi o ambienti fisici.
- **Obiettivo**: Rubare credenziali, dati sensibili, installare malware o ottenere accesso fisico a luoghi protetti.

Tecniche Comuni di Social Engineering

Tecnica	Descrizione Breve	Esempio Pratico	Segnali di Allarme
Phishing	Invio di email, messaggi o siti falsi che imitano entità legittime per rubare informazioni.	Un'email apparentemente da una banca che chiede di "verificare il tuo conto" cliccando su un link.	URL sospetti, errori grammaticali, richieste urgenti, mittente inconsueto.
Tailgating	Accesso fisico non autorizzato a un'area protetta seguendo da vicino qualcuno con accesso.	Un estraneo con le mani piene chiede di tenergli la porta di un edificio aziendale protetto.	Persone non autorizzate che chiedono di entrare, assenza di badge identificativi.
Pretexting	Creazione di una falsa identità o pretesto per ottenere informazioni sensibili.	Un finto tecnico IT chiama un dipendente dicendo che deve "verificare la sua password".	Richieste non verificate, pressioni per condividere informazioni riservate.
Vishing	Phishing via telefono: chiamate vocali per ottenere informazioni riservate.	Una telefonata che finge di essere dal supporto clienti della banca che chiede di "verificare il codice OTP".	Numeri sconosciuti, tono urgente, richiesta di dati sensibili via telefono.
Baiting	Offerta di qualcosa di allettante per indurre la vittima a eseguire un'azione dannosa.	Una chiavetta USB "smarrita" contenente malware lasciata nel parcheggio di un'azienda.	Oggetti sconosciuti trovati in luoghi pubblici, offerte troppo belle per essere vere.

Approfondimento delle Tecniche

1. Phishing

- **Descrizione**: Email o messaggi truffa che spingono l'utente a cliccare link malevoli o fornire credenziali.
- Obiettivo: Ottenere password, dati bancari, accesso a sistemi.
- Segnali:
 - o Mittente sconosciuto o sospetto
 - o Errori grammaticali
 - Richieste urgenti o minacciose
 - Link che non corrispondono all'URL ufficiale

2. Tailgating

- **Descrizione**: Un attaccante entra in un'area protetta sfruttando la cortesia altrui.
- Obiettivo: Accesso fisico non autorizzato
- Segnali:
 - o Persone senza badge che seguono i dipendenti
 - o Tentativi di forzare la porta con scuse ("Ho dimenticato il badge")

3. Pretexting

- Descrizione: L'attaccante si finge una persona autorevole (tecnico, poliziotto, collega) per ottenere fiducia.
- Obiettivo: Ottenere informazioni riservate
- Segnali:
 - o Domande troppo dettagliate su sistemi o dati personali
 - o Pressioni psicologiche ("Serve subito per evitare problemi")

4. Vishing

- **Descrizione**: Versione vocale del phishing, spesso con tecniche di spoofing del numero.
- Obiettivo: Rubare informazioni tramite conversazione telefonica
- Segnali:
 - Chiamate non richieste da "enti ufficiali"
 - o Richiesta di codici OTP, password o PIN
 - o Pressione a "fare in fretta"

5. Baiting

- **Descrizione**: Il "tranello" è fisico o digitale, come una chiavetta USB o un file "gratuito" online.
- Obiettivo: Indurre la vittima a installare malware o fornire accesso
- Segnali:
 - o Oggetti sconosciuti trovati in spazi pubblici
 - o Offerte irresistibili ("download gratuito" di software costosi)
 - o Pop-up sospetti online

Difese Contro il Social Engineering

- Formazione e consapevolezza dei dipendenti
- Politiche aziendali rigorose su accesso fisico e dati
- Verifica dell'identità prima di condividere informazioni
- Uso di filtri anti-phishing e autenticazione multifattore (MFA)
- Segnalazione immediata di incidenti sospetti all'IT Security

Prompt 2 (Tecniche di difesa): ChatGPT, basandoti sulle tecniche di social engineering che abbiamo approfondito prima, puoi fornirmi un elenco di strategie e migliori pratiche per difendersi da questi tipi di attacchi? Per ogni strategia vorrei che tu mi spiegassi come applicarla sia a livello individuale, come per esempio per un utente casalingo, sia a livello aziendale. Includi un suggerimento su alcuni strumenti tecnoligici che possono essere utili. Struttura la risposta in un formato chiaro, magari con due sezioni distinte (livello individuale e livello aziendale), includi anche se possono aiutare elenchi puntati e tabelle.

Risultati:

Strategie di Difesa contro il Social Engineering

A Livello Individuale (Utente Privato)

Strategia	Descrizione	Come Applicarla	Strumenti Utili
1. Verifica dell'identità	Non fidarti mai ciecamente di email, chiamate o messaggi.	Controlla sempre il mittente. In caso di dubbio, contatta direttamente la fonte ufficiale (es. banca, azienda).	Google SafeBrowsingTruecaller(identificazionechiamate)
2. Attenzione ai link e allegati	I file o link possono contenere malware o	Non cliccare mai su link o allegati sospetti. Passa il	- Estensioni browser come Bitdefender

Strategia	Descrizione	Come Applicarla	Strumenti Utili
	portare a siti di phishing.	mouse sopra il link per vedere dove porta.	TrafficLight o Netcraft
3. Uso dell'autenticazione a due fattori (2FA)	Aggiunge una protezione ulteriore anche se la password viene rubata.	Abilita sempre la 2FA, meglio se con app (es. Google Authenticator) e non solo SMS.	GoogleAuthenticatorAuthyMicrosoftAuthenticator
4. Formazione personale	La consapevolezza è la difesa più efficace.	Leggi guide, partecipa a webinar o corsi online sulla sicurezza informatica.	- Corsi su Cybrary , Coursera , Udemy
5. Non inserire mai dati sensibili senza verifica	Pretexting, phishing e vishing si basano sul farti "parlare".	Se qualcuno chiede PIN, password o dati personali: fermati, verifica e non fornire nulla.	- Nessun tool specifico, solo buonsenso e prudenza

📳 A Livello Aziendale (Organizzazioni)

Strategia	Descrizione	Come Applicarla in Azienda	Strumenti Tecnologici
1. Formazione continua del personale	Dipendenti consapevoli sono il primo muro di difesa.	Organizza corsi trimestrali, test di phishing simulati e materiali interattivi.	- KnowBe4 - PhishLabs - Hoxhunt
2. Controllo accessi e badge	Tailgating e baiting avvengono spesso per mancanza di sorveglianza.	Implementa tornelli, badge, e politiche "no tailgating". Richiedi segnalazione per visitatori.	Sistemi RFIDVideosorveglianzaSistemi di controllo accessi fisici
3. Politica del principio del minimo privilegio	Ogni dipendente accede solo a ciò che serve.	Limita l'accesso a file, dati e strumenti in base al ruolo.	- Microsoft ActiveDirectory- IAM (Identity AccessManagement)
4. Email gateway con filtro anti-phishing	Bloccano messaggi sospetti prima che arrivino all'utente.	Usa soluzioni avanzate che analizzano link, allegati e mittenti.	- Proofpoint- Mimecast- Microsoft Defender for Office 365
5. Simulazioni di attacchi social engineering	Allenano le risposte reali dei dipendenti.	Esegui test regolari con email e chiamate simulate per valutare reazioni.	- Cofense - Attack Simulator (Microsoft 365)
6. Politiche di segnalazione interna	Serve un processo chiaro per allertare l'IT.	Crea un canale dedicato per segnalare attività sospette (email, USB trovate, chiamate strane).	- Helpdesk ticketing (es. Zendesk, Jira Service Desk)

Consigli Trasversali (per Tutti)

- Diffida dell'urgenza: se qualcuno ti spinge a "fare in fretta", è un segnale d'allarme.
- Mai condividere credenziali: nemmeno con presunti tecnici o colleghi.
- Backup regolari: in caso di compromissione, è essenziale ripristinare i dati.
- Aggiornamenti software: sistemi obsoleti sono più vulnerabili, anche a supporto di tecniche di social engineering

2) Esplorazione dei CVE

Prompt: ChatGPT, puoi fornirmi un elenco di 5-10 CVE relativi al sistema WordPress? Focalizzati su vulnerabilità recenti o di alta gravità scoperte negli ultimi due anni. Per ogni CVE includi le seguenti informazioni:

- 1. Identificativo CVE
- 2. Breve descrizione
- 3. Gravità
- 4. Soluzione consigliata

Dopo la lista, scegli una delle vulnerabilità e spiegami in modo più approfondito come funziona l'attacco, quali sono i potenziali impatti e come si può sfruttare la vulnerabilità.

Risultati:

Tabella delle vulnerabilità

CVE	Descrizione	Gravità	Soluzione consigliata
CVE-2025-26909	Remote Code Execution nel plugin WP Ghost , tramite input non sanitizzati nella funzione showFile().	Critica (CVSS ~9.6) DailyCVE+15WP- Firewall+15NVD+15	Aggiornare a WP Ghost v. 5.4.02 o superiore.
CVE-2025-2505	Local PHP File Inclusion nel plugin Age Gate , via parametro lang, consentendo inclusione/esecuzione di file PHP.	Critica (CVSS ~9.8) feedly.comWP-Firewall	Aggiornare a Age Gate v. 3.5.4 .
CVE-2025-1661	Local File Inclusion (LFI) nel plugin HUSKY – Products Filter Professional for WooCommerce, via parametro template AJAX.	Critica (CVSS non indicata, ma catalogata come "critical") DailyCVEWP-Firewall	Aggiornare a v. 1.3.6.6 o superiore; disattivare se non aggiornabile.

CVE	Descrizione	Gravità	Soluzione consigliata
CVE-2025-22785	SQL Injection nel plugin Course Booking System , via parametri non sanitizzati da utenti Subscriber.	Alta (CVSS ~9.3) <u>wiz.io</u>	Aggiornare Course Booking System v. 6.0.7 o successivi.
CVE-2025-0723	Blind/time-based SQL Injection nel plugin ProfileGrid , attraverso parametri rid e search.	Critica (CVSS non indicata ma catalogata "Critical") <u>DailyCVE</u>	Aggiornare a ProfileGrid > v. 5.9.4.7; aggiungere WAF e sanitizzazione.

Approfondimento: CVE-2025-2505 (Age Gate plugin, Local PHP File Inclusion)

Come funziona l'attacco

- Il plugin Age Gate prima della versione 3.5.4 non valida correttamente il parametro lang.
- Un attaccante non autenticato può inviare una richiesta come:

POST /wp-login.php?lang=../../wp-config.php

oppure con payload simile che punta a file con codice PHP arbitrario.

• Il server include il file indicato e lo esegue, permettendo così inclusione/exec diretta di codice PHP.

Potenziali impatti

- Esecuzione remota di codice (RCE): l'attaccante può eseguire shell, caricare malware, modificare contenuti.
- Accesso a configurazioni sensibili (ad esempio wp-config.php, credenziali del database).
- Possibile intero compromesso del sito e accesso amministrativo.

Come può essere sfruttata

- 1. L'attaccante individua un sito con il plugin vulnerabile attivo.
- 2. Invia una richiesta HTTP manipulando lang con sequenze tipo ../../....
- 3. Se include un file malevolo precedentemente caricato (o un file di sistema sensibile), il server lo esegue.
- 4. Il codice incluso può creare una shell web o estrarre dati sensibili.

Mitigazioni efficaci

- Aggiornare immediatamente il plugin alla versione ≥ 3.5.4 (la patch rimuove il bug).
 Ameeba+6feedly.com+6WP-Firewall+6wiz.io+9WP Firewall+9Reddit+9DailyCVEReddit+1Reddit
- **Disabilitare PHP execution** nelle directory di upload (es. .htaccess: php_admin_flag engine off oppure regole nginx per bloccare .php).

- Implementare un WAF (Web Application Firewall) per bloccare richieste con sequenze ../.
- **Log e monitoraggio** regolari delle richieste ad admin-ajax.php o endpoint simili: cercare pattern sospetti.
- **Abilitare la validazione** dell'input lato server: bloccare qualsiasi parametro lang contenente traversal (../../).

Conclusione e raccomandazioni

- Aggiorna immediatamente i plugin indicati se installati.
- **Verifica regolarmente** plugin installati usando scanner come **WPScan**, Patchstack, o audit manuali.
- Limita le autorizzazioni al minimo necessario: rimuovi plugin non in uso.
- Abilita un WAF per mitigare exploit opera su pattern comuni (traversal, SQL-inject).
- Esegui backup regolari e isola i siti in ambienti segregati.

Conclusioni: in questo esercizio abbiamo visto come un'analisi approfondita e una difesa efficace dipendano in gran parte dalla qualità delle informazioni a disposizione. L'utilizzo intelligenze artificiali, come ChatGPT in questo caso, ha dimostrato che la chiave per ottenere dati precisi e ben organizzati è la struttura dei prompt.