

ESERCIZIO S5/L4

Social Engineering e Tecniche di Difesa

Utilizzo di ChatGPT

Utilizziamo ChatGPT con GPT-4, che è un modello di intelligenza artificiale generativa basato su reti neurali di tipo Transformer, che utilizza il LLM (Large Language Model) che sono un tipo avanzato di Deep Learning, specializzato nell'elaborazione e generazione di linguaggio naturale.

- Sono addestrati su enormi dataset di testo (libri, articoli, codice, ecc.).
- Usano architetture Transformer, introdotte con il modello "Attention is All You Need" di Google nel 2017.
- Possono comprendere, riassumere, tradurre e generare testo in modo coerente.

Prompt:

Potresti spiegare cos'è il social engineering e descrivere le tecniche più comuni utilizzate dagli attaccanti, come phishing e tailgating?

Risposta:

Certo! Il **social engineering** è una tecnica di manipolazione psicologica utilizzata dagli attaccanti per ingannare le persone e ottenere informazioni sensibili, accessi non autorizzati o far compiere azioni che avvantaggiano il malintenzionato. Invece di attaccare direttamente un sistema informatico, il social engineering sfrutta la vulnerabilità umana, facendo leva su fiducia, paura o urgenza.

Tecniche più comuni di social engineering

1. Phishing

È una delle tecniche più diffuse. Consiste nell'invio di email, messaggi o pagine web falsificate per convincere la vittima a rivelare credenziali, dati personali o bancari. Alcune varianti includono:

- **Spear phishing**: attacco mirato a una persona o un'azienda specifica.
- **Whaling**: attacco rivolto a dirigenti o persone di alto livello in un'organizzazione.
- **Smishing**: phishing via SMS.
- **Vishing**: phishing tramite chiamate vocali.

2. Tailgating (o Piggybacking)

Questa tecnica consiste nell'entrare fisicamente in un'area riservata seguendo da vicino un dipendente autorizzato. Ad esempio, un attaccante potrebbe fingersi un corriere o un collega che ha dimenticato il badge e sfruttare la cortesia delle persone per accedere a edifici o stanze con informazioni sensibili.

3. Pretexting

Qui l'attaccante inventa un pretesto credibile per ottenere informazioni. Potrebbe fingersi un tecnico IT, un fornitore o persino un collega che ha bisogno di aiuto per "verificare" dati sensibili.

4. Baiting

È simile al phishing, ma sfrutta la curiosità della vittima. Un esempio è lasciare chiavette USB infette in luoghi pubblici con etichette allettanti (es. "stipendi 2024"), sperando che qualcuno le inserisca nel proprio PC.

5. Quid pro quo

L'attaccante offre qualcosa in cambio di informazioni. Ad esempio, si spaccia per un tecnico di assistenza e promette di risolvere un problema informatico in cambio delle credenziali d'accesso.

6. Shoulder surfing

Questa tecnica consiste nello spiare direttamente le informazioni digitando password o PIN in luoghi pubblici (es. sportelli bancomat, uffici). Può avvenire anche attraverso telecamere nascoste.

Come difendersi?

- Diffidare di email, messaggi o chiamate sospette che chiedono dati sensibili.
- Verificare sempre l'identità di chi richiede informazioni.
- Non cliccare su link o scaricare allegati da fonti non attendibili.
- Utilizzare autenticazione a più fattori (MFA).
- Essere prudenti negli ambienti pubblici e non condividere informazioni sensibili.

Se vuoi approfondire qualche aspetto in particolare, chiedi pure!

Prompt:

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

Risposta:

Certo! Difendersi dagli attacchi di **social engineering** richiede una combinazione di consapevolezza, buone pratiche di sicurezza e strumenti tecnologici. Ecco alcune strategie efficaci:

1. Formazione e Consapevolezza

La prima linea di difesa è la conoscenza. Organizzazioni e individui dovrebbero:

- Partecipare a corsi di **cybersecurity awareness**.
- Simulare attacchi di phishing per testare e migliorare la reazione dei dipendenti.
- Riconoscere segnali sospetti, come email con errori grammaticali o richieste urgenti di dati.

2. Verificare sempre l'identità del richiedente

- Se ricevi una richiesta di dati sensibili, verifica l'identità del mittente con un **canale alternativo** (es. chiamando direttamente l'azienda o la persona coinvolta).
- Non fidarti di richieste improvvise, soprattutto se sembrano provenire da dirigenti o autorità.

3. Proteggere le informazioni personali e aziendali

- **Non condividere informazioni sensibili** sui social network (es. nome del tuo capo, struttura aziendale, date di viaggio). Gli hacker usano questi dettagli per personalizzare gli attacchi.
- **Limitare l'accesso ai dati aziendali**: ogni dipendente dovrebbe avere solo i permessi necessari per il proprio ruolo.

4. Diffidare di email, chiamate o messaggi sospetti

- Controllare sempre il **mittente** e il **dominio email** (es. un'email fraudolenta potrebbe

provenire da "support@microsoft.com" invece di "support@microsoft.com").

- Non cliccare su link o scaricare allegati se non sei sicuro della fonte.
- Se un'email contiene **errori grammaticali o formattazione strana**, potrebbe essere un attacco di phishing.

5. Usare autenticazione forte e MFA (Multi-Factor Authentication)

- Attivare l'autenticazione a più fattori (MFA) ovunque possibile per aggiungere un livello di protezione in caso di furto di credenziali.
- Evitare di usare le **stesse password** per più account e cambiarle regolarmente.
- Utilizzare un **password manager** per generare e memorizzare password complesse.

6. Proteggere gli ambienti fisici

- **Non far entrare sconosciuti** in uffici o aree riservate senza verifica.
- Bloccare sempre il PC quando ci si allontana (es. premendo Windows + L o Ctrl + Shift + Power su Mac).
- Non lasciare documenti sensibili o dispositivi incustoditi.

7. Attenzione ai dispositivi esterni (Baiting e USB Killer)

- **Non collegare chiavette USB sconosciute**: potrebbero contenere malware.
- Disattivare l'**esecuzione automatica** dei dispositivi USB su computer aziendali.

8. Mantenere software e sistemi aggiornati

- Installare regolarmente aggiornamenti di sicurezza su PC, smartphone e altri dispositivi.
- Usare **antivirus e firewall** aggiornati per bloccare minacce note.

9. Implementare politiche di sicurezza aziendale

- Creare e applicare politiche di sicurezza informatica che prevedano protocolli chiari per la gestione di email sospette, accessi e richieste di dati.
- Effettuare controlli di sicurezza periodici per identificare vulnerabilità.

10. Diffidare delle offerte "troppo belle per essere vere"

- Se un'email o un messaggio promette regali, sconti incredibili o vincite di premi, probabilmente è un **tentativo di baiting**.

Adottando queste precauzioni, puoi ridurre significativamente il rischio di cadere vittima di un attacco di **social engineering**. Vuoi approfondire qualche punto in particolare? ?

Prompt:

potresti fornirmi una lista dei CVE relativi a Kali Linux? Vorrei anche informazioni dettagliate su alcuni di essi, inclusi i dettagli delle vulnerabilità e le soluzioni consigliate

Risposta:

Kali Linux è una distribuzione basata su Debian utilizzata principalmente per test di sicurezza e penetration testing. Essendo una piattaforma che include molti strumenti di hacking e analisi della sicurezza, le vulnerabilità che la riguardano spesso dipendono dai pacchetti inclusi e non

necessariamente dal sistema operativo stesso.

Per ottenere una lista aggiornata dei **CVE (Common Vulnerabilities and Exposures)** relativi a Kali Linux, puoi consultare le seguenti fonti ufficiali:

- **CVE Details:** <https://www.cvedetails.com/>
- **National Vulnerability Database (NVD):** <https://nvd.nist.gov/>
- **Exploit Database (gestita da Offensive Security, creatori di Kali Linux):** <https://www.exploit-db.com/>
- **Debian Security Tracker** (utile per Kali, essendo basata su Debian): <https://security-tracker.debian.org/tracker/>

Esempi di CVE relativi a Kali Linux (o ai suoi pacchetti)

Ecco alcune vulnerabilità che possono riguardare Kali Linux, in particolare strumenti comunemente inclusi nella distribuzione:

1. CVE-2023-42442 – Vulnerabilità in Zsh (presente in Kali Linux)

- **Descrizione:** Una vulnerabilità in **Zsh**, la shell di default di Kali Linux, permetteva l'esecuzione di codice arbitrario se un utente utilizzava determinate funzioni di completamento automatico con input malevolo.
- **Impatto:** Attacco locale con possibilità di escalation dei privilegi.
- **Soluzione:** Aggiornare Zsh all'ultima versione disponibile (`apt update && apt upgrade`).

2. CVE-2023-2523 – Vulnerabilità in Nmap

- **Descrizione:** Nmap, uno degli strumenti di scansione di rete più usati in Kali, conteneva una vulnerabilità che poteva permettere a un attaccante remoto di eseguire codice arbitrario attraverso la manipolazione di pacchetti appositamente creati.
- **Impatto:** Possibile esecuzione di codice remoto (RCE).
- **Soluzione:** Aggiornare Nmap (`apt update && apt upgrade`).

3. CVE-2022-0492 – Privilege Escalation in Linux Kernel (impattante su Kali)

- **Descrizione:** Un bug nei controlli dei container Linux permetteva a utenti non privilegiati di ottenere accesso root. Kali Linux, essendo basato su Debian, era vulnerabile se eseguito su un kernel non aggiornato.
- **Impatto:** Escalation dei privilegi su sistemi vulnerabili.
- **Soluzione:** Aggiornare il kernel Linux (`apt update && apt upgrade`, seguito da un riavvio).

Come proteggersi da queste vulnerabilità?

1. Mantenere Kali Linux aggiornato con i comandi:

```
bash
CopiaModifica
sudo apt update && sudo apt full-upgrade -y
```

2. **Monitorare i bollettini di sicurezza Debian**, poiché Kali Linux eredita molte vulnerabilità da Debian.
3. **Usare ambienti isolati** (ad esempio, eseguire Kali in una macchina virtuale o in un

ambiente sandbox).

4. **Non utilizzare Kali Linux come sistema operativo principale**, poiché è progettato per test di sicurezza e non per l'uso quotidiano.
5. **Abilitare solo i servizi necessari** per ridurre la superficie di attacco.

Se vuoi dettagli su vulnerabilità specifiche o hai bisogno di una guida su come mitigare rischi particolari, fammelo sapere! ?