# Social Engineering e Tecniche di Difesa

*1. Comprendere il Social Engineering*

Il social engineering è una tecnica di manipolazione psicologica utilizzata dagli attaccanti per ingannare le persone e indurle a fornire informazioni sensibili, eseguire azioni rischiose o rivelare credenziali di accesso. A differenza degli attacchi puramente tecnici, il social engineering sfrutta le debolezze umane anziché le vulnerabilità dei sistemi informatici.

Tecniche di Social Engineering più comuni:

1. Phishing
    - Gli attaccanti inviano email o messaggi falsificati per ingannare le vittime e far loro rivelare credenziali, dati bancari o scaricare malware.
    - Esempio: Un'email apparentemente inviata da una banca chiede di aggiornare i dati di accesso cliccando su un link malevolo.

2. Spear Phishing
    - Variante più mirata del phishing, personalizzata per la vittima (es. email indirizzata a un dipendente con dettagli aziendali reali).

3. Vishing (Voice Phishing)
    - Gli attaccanti chiamano le vittime fingendosi operatori bancari o di supporto tecnico per ottenere dati sensibili.
    - Esempio: Una telefonata da un "bancario" che avvisa di un'attività sospetta sul conto e chiede conferma delle credenziali.

4. Smishing (SMS Phishing)
    - Simile al phishing, ma avviene tramite SMS con link fraudolenti.

5. Tailgating e Piggybacking
    - L'attaccante entra in un'area riservata sfruttando l'accesso di un dipendente autorizzato.
    - Esempio: Un estraneo segue un dipendente attraverso una porta di sicurezza dicendo di aver dimenticato il badge.

6. Pretexting
    - L'attaccante crea una falsa identità o una situazione ingannevole per ottenere informazioni.
    - Esempio: Un hacker si finge tecnico IT e chiede a un dipendente di reimpostare la password.

7. Baiting

- L’attaccante usa un’esca (es. una chiavetta USB infetta) per indurre la vittima a compromettere il proprio sistema.
- Esempio: Una USB etichettata “stipendi aziendali 2024” viene lasciata in un parcheggio per spingere qualcuno a inserirla nel proprio PC.

*2. Strategie di Difesa*

Per proteggersi dagli attacchi di social engineering, è fondamentale adottare strategie efficaci.

1. Formazione e Consapevolezza

- Educare dipendenti e utenti sui pericoli del social engineering e su come riconoscere tentativi di attacco.
- Simulazioni di phishing per allenare il personale.

2. Verifica delle Comunicazioni

- Non fidarsi mai di email, chiamate o messaggi sospetti.
- Verificare sempre con il mittente ufficiale prima di fornire informazioni sensibili.

3. Utilizzo di Autenticazione a Due Fattori (2FA)

- Anche se le credenziali vengono compromesse, un secondo fattore di autenticazione blocca l’accesso non autorizzato.

4. Politiche di Accesso Fisico

- Non consentire l’accesso a estranei senza verifica.
- Mai lasciare dispositivi o badge incustoditi.

5. Protezione contro il Phishing

- Non cliccare su link sospetti.
- Verificare sempre l’URL di login ai servizi online.
- Usare filtri anti-phishing nei browser e nelle email aziendali.

6. Politica di Password Sicure

- Utilizzare password lunghe e complesse.
- Cambiarle regolarmente e non riutilizzarle per più servizi.

7. Controllo degli Accessi e Monitoraggio

- Limitare l’accesso ai dati aziendali solo ai dipendenti autorizzati.
- Monitorare attività sospette nei sistemi informatici.

*3. Conclusione e Raccomandazioni*

Il social engineering è una minaccia concreta, perché sfrutta la psicologia umana piuttosto che vulnerabilità tecniche. Per ridurre il rischio, è essenziale:
1.Formare e sensibilizzare gli utenti
2.Implementare misure di sicurezza informatica
3.Verificare sempre l'autenticità delle comunicazioni
4.Utilizzare strumenti di protezione come 2FA e filtri anti-phishing

# Esercizio bonus: Esplorazione dei CVE tramite ChatGPT (Linux)

CVE-2021-3156 - Sudo Privilege Escalation
Una vulnerabilità in Sudo permetteva a un utente non privilegiato di eseguire comandi come root senza autenticazione. Questo problema è stato risolto con l'aggiornamento Sudo alla versione 1.9.5p2 o successiva.

CVE-2019-5736 - Docker Container Escape
Questa vulnerabilità permetteva a un processo all'interno di un container Docker di eseguire comandi arbitri sul sistema host, compromettendo il sistema. La soluzione era aggiornare Docker alla versione 18.09.2 o successiva.

CVE-2020-25712 - Linux Kernel Local Privilege Escalation
Il Linux kernel aveva una vulnerabilità che permetteva a un utente non privilegiato di ottenere i permessi di root. Questo problema è stato risolto con l'aggiornamento del kernel 5.10.17.

CVESnapd aveva una vulnerabilità che consentiva a un utente malintenzionato di ottenere privilegi elevati. L'aggiornamento a Snapd versione 2.49.1 o superiore ha risolto il problema.

CVE-2017-1000367 - Polkit Local Privilege Escalation
Una vulnerabilità in Polkit permetteva a un utente malintenzionato di elevare i privilegi. Questo bug è stato corretto con l'aggiornamento di Polkit alla versione 0.105 o superiore.