REPORT : Social Engineering e Tecniche di Difesa

Obiettivo: Esplorare le tecniche di social engineering e imparare come difendersi da questi tipi di attacchi.
In questo report sarà presente un prompt per Gemini che permette di ottenere informazioni dettagliate sulle tecniche di social engineering.

Prompt:

"Sono uno studente che sta seguendo un corso sulla cybersecurity, ho bisogno di una guida tecnica e pratica sul Social Engineering per un progetto. Per favore, elabora una risposta strutturata nei seguenti punti:

1. ***Definizione e Psicologia**: Spiega cos'è il Social Engineering e quali leve psicologiche sfrutta (es. urgenza, autorità).*
2. ***Vettori di Attacco**: Elenca e descrivi nel dettaglio le tecniche più comuni, distinguendo tra quelle digitali (come Phishing, Vishing, Smishing) e quelle fisiche (come Tailgating, Baiting). Fornisci un breve esempio concreto per ciascuna.*
3. ***Strategie di Difesa**: Fornisci raccomandazioni pratiche per la mitigazione del rischio, suddividendole in controlli tecnologici, procedurali e formazione umana.*

Introduzione: L'Hacking dell'Essere Umano

Il **Social Engineering** non mira a vulnerabilità software o hardware, ma sfrutta i "bug" nel sistema operativo umano. È l'arte di manipolare le persone affinché compiano azioni o divulghino informazioni riservate.

Gli attaccanti fanno leva sui Bias Cognitivi e sulle emozioni:

- **Urgenza/Paura**: Inibisce il pensiero critico (es. "Il tuo account verrà bloccato").
- **Autorità**: Sfrutta la tendenza a obbedire alle gerarchie (es. "Sono il CEO").
- **Fiducia/Simpatia**: Abbassa le difese naturali.
- **Curiosità**: Spinge all'azione impulsiva (es. "Vedi allegato").

Analisi delle Tecniche di Attacco (Vettori)

Abbiamo classificato gli attacchi in tre categorie principali:

A. Minacce Digitali (Remote)

- **Phishing**: Invio massivo di email fraudolente.
- **Spear Phishing / Whaling**: Attacchi mirati costruiti su informazioni raccolte precedentemente (OSINT). Il *Whaling* colpisce specificamente i dirigenti (C-Level).
- **Vishing** (Voice Phishing): Frodi telefoniche, spesso con spoofing del numero chiamante.
- **Smishing:** Phishing via SMS o app di messaggistica.

B. Minacce Fisiche (On-Premise)

- **Tailgating (Piggybacking)**: L'attaccante accede a un'area sicura accodandosi a una persona autorizzata che apre la porta.
- **Baiting:** L'uso di "esche" fisiche, come chiavette USB infette lasciate in luoghi pubblici per sfruttare la curiosità della vittima.

C. Minacce Basate sullo Scenario

- **Pretexting:** Creazione di uno scenario inventato (es. finto tecnico IT) per estorcere informazioni tramite il dialogo.

Raccomandazioni e Strategie di Difesa

La difesa efficace richiede un approccio a livelli (Defense in Depth).

Livello 1: Difesa Tecnologica

- **MFA (Multi-Factor Authentication)**: Essenziale. Blocca l'accesso anche se le credenziali vengono rubate.
- **Filtri Email (SEG)**: Utilizzo di gateway che analizzano link e allegati in sandbox.
- **Marcatura Email Esterne**: Banner visivi per email provenienti da fuori l'organizzazione.

Livello 2: Difesa Procedurale

- **Verifica "Out-of-Band"**: Mai fidarsi del canale su cui arriva la richiesta. Se arriva una mail urgente dal CEO, verificare chiamandolo al telefono (canale diverso).
- **Processi di Smaltimento**: Distruzione sicura dei documenti cartacei.
- **Clean Desk Policy:** Non lasciare informazioni sensibili sulle scrivanie.

Livello 3: Difesa Umana (Il Firewall Umano)

- **Formazione Continua**: Pillole formative frequenti invece di corsi annuali.
- **Simulazioni di Phishing**: Test a sorpresa non punitivi.
- **Cultura "No Blame"**: Incoraggiare la segnalazione immediata degli errori senza paura di ritorsioni, per garantire una risposta rapida agli incidenti.

Secondo Obiettivo: l'obiettivo è imparare a utilizzare L'IA per raccogliere informazioni sui CVE Common Vulnerabilities and Exposures).

Prompt:
"Sono uno studente che sta frequentando un corso sulla cybersecurity. Ho bisogno di identificare le vulnerabilità storiche e recenti più gravi per quanto riguarda MYSQL che permettono di compromettere l'integrità dei dati o ottenere l'accesso al sistema operativo sottostante.

Nello specifico:

1. *3 CVE critiche*
2. *Per ciascuna, crea una scheda tecnica con:*
    - *ID CVE e Punteggio CVSS.*
    - *Il Difetto Tecnico: (es. Buffer Overflow, Logic Error, Config Injection).*

    - *Vettore di Attacco: Cosa deve fare l'attaccante? (es. serve essere già loggati? Serve accesso di rete?).*
    - *Impatto: (es. Bypass autenticazione, Root Shell).*
    - *Soluzione: La versione correttiva.*

Spiega anche come un database può essere usato per attaccare il sistema operativo (Privilege Escalation)."

CVE e Vulnerabilità di MYSQL

Questi esempi dimostrano che il database non è solo un contenitore di dati, ma un potenziale punto di ingresso per prendere il controllo dell'intero server.

1. CVE-2016-6662 ("MySQL Remote Root Code Execution")

- **Tipo**: Privilege Escalation / Remote Command Execution.
- **Punteggio CVSS**: 10.0 (Critico).
- **Il Difetto Tecnico**: Questa vulnerabilità riguarda il modo in cui MySQL gestisce i file di configurazione (`my.cnf`). Un attaccante che ha accesso al database (anche con permessi limitati, ad esempio tramite una SQL Injection su un sito web) può iniettare impostazioni malevole nel file di configurazione tramite il comando `SET GLOBAL general_log_file.`
- **Vettore di Attacco:** L'attaccante imposta una libreria malevola come `malloc_lib` nel file di configurazione. Al successivo riavvio del servizio MySQL (o caricamento della libreria), il codice malevolo viene eseguito con i privilegi di root (o dell'utente sistema che esegue MySQL).
- **Impatto**: Compromissione totale del server. Da un semplice accesso SQL, si ottiene una shell di sistema con privilegi massimi.
- **Soluzione**: Aggiornare alle versioni 5.7.15 / 5.6.33 e assicurarsi che i file di configurazione non siano scrivibili dall'utente mysql.

2. CVE-2012-2122 ("The 1 in 256 Bug")

- **Tipo**: Authentication Bypass (Logic Error).

- **Punteggio CVSS**: 5.1 (Medium) - *Nota: Basso punteggio CVSS teorico, ma impatto catastrofico se presente.*
- **Il Difetto Tecnico**: Un incredibile errore di programmazione nel codice C di MySQL/MariaDB. La funzione `memcmp` (che confronta l'hash della password corretta con quella fornita dall'utente) restituiva un valore che, a causa di un cast errato di variabili, veniva interpretato come "Zero" (cioè "Password Corretta") in circa 1 caso su 256, indipendentemente dalla password inserita.
- **Vettore di Attacco**: Un attaccante poteva lanciare uno script che tentava di loggarsi come `root` con una password a caso ripetutamente. Statisticamente, entrava in pochi secondi (circa 300 tentativi).
- **Impatto**: Accesso completo al database come amministratore root senza conoscere la password.
- **Soluzione:** Patchare immediatamente (Versioni 5.1.63 / 5.5.24). È un caso di studio famoso sulla qualità del codice.

3. CVE-2022-21351 (Oracle MySQL Server)

- **Tipo**: Library Misconfiguration / Unsafe Linking.
- **Punteggio CVSS**: 7.2 (High).
- **Il Difetto Tecnico**: Una vulnerabilità nel componente *Server: Optimizer*. Permette a un utente autenticato con privilegi alti (es. un attaccante che ha rubato credenziali di un DBA) di sfruttare debolezze nella gestione delle librerie condivise.
- **Vettore di Attacco**: Sfruttando procedure o trigger specifici, l'attaccante può causare il caricamento di oggetti non sicuri, portando al crash del servizio o potenzialmente all'esecuzione di codice.
- **Impatto:** Denial of Service (DoS) del database o Takeover completo in scenari specifici.
- **Soluzione:** Aggiornare tramite l'Oracle Critical Patch Update (Jan 2022).

CONCLUSIONE

Il report ha analizzato due aspetti complementari della sicurezza: quello umano (**Social Engineering**) e quello tecnologico (Software Security).

L'elemento chiave emerso è che l'efficacia della sicurezza informatica non può basarsi su un'unica linea di difesa:

- **Sicurezza Umana** (Parte 1 - Social Engineering): Abbiamo osservato come un aggressore possa bypassare le protezioni più avanzate sfruttando l'errore umano, la distrazione o la manipolazione psicologica. In questo scenario, la difesa non è un aggiornamento di codice, ma l'investimento nella formazione del personale.
- **Sicurezza del Software** (Parte 2 - CVE MySQL): Abbiamo constatato che anche prodotti software ampiamente utilizzati e maturi possono contenere vulnerabilità critiche che rendono inefficace qualsiasi altra protezione. Qui, la soluzione è puramente tecnica: applicazione immediata di patch e hardening dei sistemi.

In sintesi, una strategia di difesa veramente efficace richiede un approccio integrato. Proteggere la tecnologia (risolvendo le CVE) è insufficiente se si ignorano i rischi derivanti dall'ingegneria sociale. Allo stesso modo, dipendenti ben addestrati non possono compensare server con database che presentano vulnerabilità note e non risolte. La vera resilienza aziendale deriva dalla loro fusione sinergica.