

S5L4

Social engineering

Obiettivo:

Esplorare le tecniche di social engineering e imparare come difendersi da questi tipi di attacchi. Questo esercizio vi guiderà attraverso la comprensione delle varie forme di social engineering, esempi reali di attacchi e strategie di difesa efficaci.

Gemini, sono uno studente di cybersecurity, potresti spiegarmi cos'è il social engineering e descrivere le tecniche più comuni utilizzate dagli attaccanti, come phishing e tailgating?



Spiegazione:

Il **Social Engineering** (Ingegneria Sociale) è l'arte di manipolare psicologicamente le persone per indurle a compiere determinate azioni o a divulgare informazioni riservate, a differenza degli attacchi informatici "tecnici" che sfruttano vulnerabilità software o hardware, il social engineering prende di mira l'anello più debole della catena di sicurezza: l'essere umano.

L'attaccante (social engineer) non cerca di hackerare un computer, ma di "hackerare" la mente della vittima, facendo leva su istinti ed emozioni come:

- Fiducia:** fingersi una persona autorevole (un tecnico, un manager, un agente di polizia).
 - Urgenza e paura:** creare una situazione di finta urgenza (es. "Il tuo account sta per essere bloccato").
 - Curiosità o avidità:** offrire qualcosa di allettante (un premio, un file confidenziale)
 - Senso di colpa o desiderio di aiutare:** Sfruttare la naturale tendenza degli esseri umani ad essere cortesi.
-

1) Tecniche più comuni

Phishing

È la tecnica più conosciuta, consiste nell'invio massivo di comunicazioni (solitamente **email**, ma anche SMS, detti **Smishing**, o messaggi su app di chat) che sembrano provenire da una fonte legittima e affidabile (es. una banca, un corriere, un social network, l'ufficio IT aziendale).

Con l'obiettivo di ingannare la vittima per:

-**Rubare credenziali:** il messaggio contiene un link che porta a un sito web clone (es. una pagina di login identica a quella della vera banca). La vittima inserisce nome utente e password, che vengono così catturati dall'attaccante.

-**Installare malware:** il messaggio contiene un allegato (es. una finta fattura in PDF, un documento .zip) che, una volta aperto, infetta il computer con un virus, un ransomware o uno spyware.

Varianti:

-**Spear fishing:** È un attacco di phishing mirato e altamente personalizzato. Invece di inviare migliaia di email generiche, l'attaccante studia la sua vittima (o l'azienda target) e crea un'email su misura, usando nomi e contesti reali per sembrare estremamente credibile.

-**Whaling:** Phishing mirato ai dirigenti e alle persone di alto profilo all'interno di un'organizzazione.

Tailgating (o Piggybacking)

Questa è una tecnica di **sicurezza fisica**, non digitale. Il "tailgating" (letteralmente "stare in coda") consiste nel **seguire una persona autorizzata per superare un punto di accesso fisico controllato**, come una porta con un badge o un tornello.

L'obiettivo è ottenere l'accesso fisico non autorizzato a un'area riservata (uffici, data center, archivi) sfruttando la cortesia umana, ad esempio avvicinandosi alla porta con le mani occupate (es. portando un pacco o delle tazze di caffè) e chiedendo alla persona autorizzata che sta entrando di tenergli la porta, fingendosi un collega distratto che ha "dimenticato il badge" in auto o alla scrivania o accodandosi semplicemente e molto velocemente prima che la porta di sicurezza si richiuda, sperando di non essere notato.

Pretexting

Nel pretexting, l'attaccante crea uno **scenario fittizio (un "pretesto")** e lo usa per ottenere informazioni dalla vittima. Questa tecnica richiede più interazione rispetto al phishing.

L'obiettivo è estrarre dati sensibili (informazioni personali, dati finanziari, dettagli sulla struttura aziendale) impersonando qualcuno che avrebbe una ragione legittima per fare certe domande.

Esempi:

-L'attaccante chiama un dipendente fingendosi del **supporto IT** e afferma che c'è un problema urgente sul suo account. Per "verificare la sua identità" e risolvere il problema, chiede al dipendente di confermare la sua password o di rispondere a domande di sicurezza.

-L'attaccante si finge un **sondaggista** o un **addetto di una società partner** per raccogliere informazioni apparentemente innocue sulla tecnologia usata in azienda, che userà poi per un attacco più mirato.

Baiting (Adescamento)

Il baiting (da *bait*, esca) fa leva sulla **curiosità** o sull'**avidità** della vittima.

L'obiettivo è indurre la vittima a installare malware o a cadere in una trappola per esempio lasciando una **chiavetta USB** infetta in un luogo pubblico (parcheggio, mensa, ascensore) con un'etichetta allettante come "Stipendi" o "Foto Confidenziali", la curiosità spinge qualcuno a inserirla nel proprio PC, infettandolo, o in maniera digitale, per esempio con link per il download **gratuito** di film, musica o software costosi, che in realtà nascondono codice malevolo.

Vishing (Voice phishing)

Il **Vishing** è una forma di attacco di **phishing** che avviene tramite **chiamate telefoniche** o messaggi vocali. È una contrazione dei termini inglesi "Voice" (voce) e "Phishing".

Mentre il phishing tradizionale sfrutta la posta elettronica, il vishing utilizza la voce per manipolare la vittima e indurla a divulgare informazioni sensibili, come dati finanziari, codici di accesso, o a effettuare trasferimenti di denaro.

2) Come difendersi:

Gemini, potresti elencare e spiegare alcune strategie efficaci per difendersi dagli attacchi di social engineering?

Dato che il social engineering attacca la psicologia, la difesa principale è la **consapevolezza** (Security Awareness).

Le principali tecniche di difesa sono:

-**Essere scettici:** Non fidarsi ciecamente di email o messaggi inaspettati, specialmente se creano urgenza o chiedono dati sensibili.

Verificare sempre: Se ricevi una richiesta sospetta, contatta il presunto mittente attraverso un canale diverso e ufficiale (es. chiama la banca usando il numero sul loro sito web, non quello nell'email).

Non cliccare e non aprire: Evita di cliccare su link sospetti (passa il mouse sopra per vedere l'URL reale) o di aprire allegati da mittenti sconosciuti.

Difesa fisica: Non tenere mai la porta aperta a sconosciuti in aree riservate (contro il tailgating). È compito della sicurezza, non di cortesia, verificare chi entra.

3)Esplorazione dei CVE

Gemini, potresti fornirmi una lista dei CVE relativi a Windows 10? Vorrei anche informazioni dettagliate su alcuni di essi, inclusi i dettagli delle vulnerabilità e le soluzioni consigliate.

Come trovare i CVE di Windows:

Le fonti ufficiali e più affidabili per tracciare le vulnerabilità sono:

- Microsoft Security Response Center (MSRC):** È la fonte primaria. Pubblica la "Security Update Guide" (Guida agli aggiornamenti di sicurezza) ogni mese, di solito il secondo martedì ("Patch Tuesday"). Qui puoi filtrare per prodotto (es. "Windows 10 Version 22H2") e vedere tutti i CVE affrontati in un dato aggiornamento.
- Database MITRE CVE:** È l'archivio centrale e pubblico di tutti i CVE noti. Puoi cercare per fornitore ("Microsoft") e prodotto ("Windows 10").

Esempi di vulnerabilità recenti id windows 10:

Esempio 1: CVE-2025-30397 (Zero-Day critico)

-Dettagli della vulnerabilità: Questa era una vulnerabilità *zero-day* (cioè sfruttata attivamente dai cybercriminali prima che una patch fosse disponibile) scoperta a maggio 2025. Si trattava di una falla di tipo Remote Code Execution (RCE). Sfruttava una modalità nascosta di Internet Explorer ancora presente in Microsoft Edge, permettendo a un utente malintenzionato di eseguire codice dannoso sul sistema della vittima semplicemente visitando un sito web compromesso.

-Impatto: Critico, un aggressore poteva prendere il pieno controllo del computer.

-Soluzione: Installare immediatamente gli aggiornamenti di sicurezza di maggio 2025. Per Windows 10 (versione 22H2), la patch specifica era inclusa nell'aggiornamento cumulativo **KB5058379**.

Esempio 2: CVE-2025-50173 (Escalation di privilegi)

-Dettagli della vulnerabilità: Questa vulnerabilità, patchata ad agosto 2025, era di tipo **elevation of privilege (EoP)** nel servizio Windows Installer.

-Impatto: Importante, un utente malintenzionato che avesse già ottenuto un accesso base al sistema (con bassi privilegi) avrebbe potuto sfruttare questa falla per ottenere i massimi privilegi (SYSTEM), compromettendo così l'intero computer.

-Soluzione: Installare l'aggiornamento di sicurezza di agosto 2025, identificato come **KB5063709**. (Nota: questa patch ha inizialmente causato alcuni problemi con i prompt UAC per gli utenti non amministratori, risolti poi in un aggiornamento successivo a settembre).