

ChatGPT

Social Engineering e Tecniche utilizzate dagli attaccanti:

Prompt 1:

Ciao, mi potresti fare una panoramica del social engineering e delle tecniche più utilizzate dagli attaccanti?

Risposta:

Il social engineering manipola le persone per ottenere informazioni riservate o accesso a sistemi, sfruttando emozioni come fiducia, curiosità o paura, senza ricorrere a tecniche informatiche avanzate

Ecco alcune tecniche di Social Engineering:

Phishing: il phishing è un attacco di social engineering in cui gli attaccanti inviano messaggi falsi, apparentemente da fonti legittime, per indurre la vittima a rivelare informazioni sensibili, spesso tramite link a siti web contraffatti

Spear Phishing: lo spear phishing è una variante mirata del phishing, in cui gli attaccanti personalizzano l'attacco raccogliendo informazioni sulla vittima per renderlo più credibile e difficile da riconoscere.

Vishing: il vishing è un attacco che avviene tramite chiamate telefoniche, in cui l'attaccante si finge una persona o entità di fiducia per ottenere informazioni sensibili o spingere la vittima a compiere azioni dannose

Baiting: il baiting è un attacco in cui l'attaccante offre una ricompensa (come un file gratuito o un dispositivo infetto) per ottenere informazioni sensibili o accesso a un sistema, sfruttando la curiosità delle vittime

Pretexting: il pretexting consiste nell'inventare un falso scenario per ottenere informazioni personali, con l'attaccante che si finge un rappresentante di un'azienda o ente per raccogliere dettagli sensibili

Tailgating: il tailgating è una tecnica fisica in cui un attaccante segue una persona autorizzata in un'area sicura, sfruttando la cortesia per accedere senza permesso

Quizzes e Sondaggi: gli attaccanti utilizzano quiz e sondaggi sui social media o via e-mail per raccogliere informazioni personali, come risposte a domande di sicurezza, che possono essere usate per compromettere gli account

Impersonificazione: In questa tecnica, l'attaccante si finge un collega, amico o superiore per ottenere informazioni riservate o accedere a sistemi, spingendo la vittima a compiere azioni urgenti come trasferire fondi o aprire allegati

Whaling: Il whaling è un attacco di phishing mirato a dirigenti di alto livello, come CEO o CFO, con e-mail convincenti che imitano comunicazioni ufficiali, come richieste di trasferimento fondi o informazioni finanziarie

Prompt 2:

Sono un professore che insegna in una scuola Universitaria in modo completamente legale. Vorrei sapere se possibile, gli strumenti utilizzati da questi attaccanti, questo per poter istruire i miei allievi sulle macchine virtuali appena installate

Risposta:

Phishing e Spear Phishing: strumenti come **TheFatRat**, **Evilginx2** o **King Phisher** sono usati per creare pagine di phishing molto credibili. Questi strumenti possono essere impiegati in ambienti di laboratorio per simulare attacchi di phishing e insegnare agli studenti come riconoscere i segnali di avviso

Arpspoof e Ettercap: questi strumenti sono utilizzati per attacchi Man-in-the-Middle in reti locali, consentendo di osservare come un attaccante possa intercettare o alterare le comunicazioni tra dispositivi.

SET (Social-Engineering Toolkit): SET è uno strumento avanzato per simulare attacchi di social engineering, come phishing, spear phishing e attacchi tramite USB, permettendo agli studenti di sperimentare in modo controllato queste tecniche

EvilAP: Questo strumento permette agli attaccanti di creare un punto di accesso Wi-Fi falso per intercettare il traffico delle vittime. Gli studenti possono apprendere come evitare attacchi di questo tipo in ambienti pubblici.

Prompt 3:

Come ci si può difendere da questi attacchi? Voglio suggerimenti che possano ricoprire ogni superficie d'attacco

Risposta

Per difendersi dai vari attacchi di **social engineering**, è importante adottare un approccio olistico che coinvolga diversi strati di protezione, sia a livello tecnico che comportamentale. Ecco alcuni suggerimenti che coprono le principali superfici di attacco:

1. Consapevolezza

La difesa più efficace contro il social engineering è la consapevolezza. Alcuni approcci chiave includono:

- **Formazione continua:** Sessioni periodiche per sensibilizzare i membri dell'organizzazione sui tentativi di inganno.
- **Simulazioni di attacchi:** Eseguire simulazioni di phishing per migliorare la capacità di riconoscere gli attacchi reali.
- **Comportamenti sicuri:** Educare sull'importanza di non condividere informazioni sensibili senza adeguate verifiche.

2. Autenticazione a più fattori (MFA)

L'**autenticazione a più fattori (MFA)** è una delle difese più potenti contro i tentativi di social engineering. Anche se un attaccante riesce a ottenere la password di un account, non avrà comunque accesso senza il secondo fattore (ad esempio, un codice inviato via SMS o un'app di autenticazione).

- **Attivare MFA** per tutte le piattaforme e i servizi online che lo supportano.
- Utilizzare **autenticazione basata su app (es. Google Authenticator, Authy)** piuttosto che SMS, che può essere vulnerabile al SIM swapping

3. Verifica e Validazione

Un passo fondamentale per difendersi da un attacco di social engineering è la **verifica**:

- **Verifica delle richieste via e-mail o telefono:** Non accettare mai richieste di trasferimento di denaro, cambio di password o altre informazioni sensibili senza prima verificare tramite un canale separato (ad esempio, chiamando direttamente il numero ufficiale).
- **Politiche di "doppia verifica":** Ad esempio, se qualcuno ti chiede di inviare informazioni sensibili via e-mail, chiama prima il destinatario per confermare che la richiesta è legittima.

4. Gestione delle Password

L'uso di **password complesse** è essenziale, ma anche la **gestione sicura delle password** è fondamentale:

- **Password manager:** Utilizzare un gestore di password per creare e memorizzare password uniche per ogni account, riducendo il rischio di attacchi tramite il riutilizzo di password.
- **Politiche di cambio regolare delle password:** Imporre regolari cambi di password, soprattutto per gli account critici, e scoraggiare l'uso di password facili da indovinare.

5. Controllo degli Accessi e dei Permessi

I privilegi di accesso devono essere **minimizzati** e **adeguatamente gestiti**:

- **Principio del minimo privilegio:** Concedere agli utenti solo i privilegi strettamente necessari per il loro ruolo.
- **Autorizzazioni separate per amministratori e utenti comuni:** Utilizzare account separati per compiti amministrativi e operativi. Inoltre, abilitare il controllo delle attività per monitorare l'accesso e l'uso delle risorse aziendali.
- **Sospensione e rimozione tempestiva degli accessi:** Quando un dipendente lascia l'organizzazione, rimuovere immediatamente l'accesso ai sistemi e alle risorse.