

Social Engineering e tecniche più utilizzate

Prompt: Ciao Chat, sto effettuando una ricerca per il corso che sto seguendo sulla Cybersecurity. Potresti fornirmi delle informazioni dettagliate di social engineering e spiegarmi le tecniche più utilizzate? Grazie.

Risposta: Certo, Francesco! Il social engineering è una tecnica usata per manipolare le persone al fine di ottenere informazioni confidenziali, accedere a sistemi o compiere azioni che compromettono la sicurezza. Questo approccio sfrutta le debolezze umane, come la fiducia, la curiosità o la paura, piuttosto che cercare di aggirare difese tecniche.

Tecniche più utilizzate nel social engineering:

1. Phishing:

- L'attaccante invia email, messaggi o link apparentemente legittimi per indurre l'utente a fornire credenziali, scaricare malware o condividere informazioni sensibili.
- Varianti:
 - Spear phishing: Target mirati, come individui specifici o dipendenti di un'organizzazione.
 - Whaling: Presa di mira di figure di alto profilo, come dirigenti aziendali.
 - Smishing: Uso di messaggi SMS ingannevoli.
 - Vishing: Truffe telefoniche.

2. Pretexting:

- L'attaccante si finge qualcun altro (ad esempio, un dipendente del reparto IT o un fornitore) per convincere le vittime a condividere informazioni riservate o accedere a sistemi.

3. Baiting:

- Offerta di qualcosa di allettante, come un file gratuito o una pen drive apparentemente smarrita, che contiene malware. Una volta collegata al computer, può compromettere il sistema.

4. Tailgating (o Piggybacking):

- L'attaccante segue una persona autorizzata per accedere a un'area protetta senza fornire credenziali, spesso sfruttando la cortesia o la distrazione.

5. Quid Pro Quo:

- L'attaccante promette qualcosa in cambio, come assistenza tecnica o un vantaggio, inducendo la vittima a fornire dati sensibili o ad eseguire determinate azioni.

6. Impersonation:

- Fingere di essere una figura autorevole o affidabile (ad esempio, un collega o un responsabile) per manipolare le vittime.

7. Watering Hole Attack:

- Compromissione di un sito web spesso visitato da un target specifico, così da infettare gli utenti con malware o sottrarre dati.

8. Dumpster Diving:

- Raccolta di informazioni riservate gettate via senza precauzioni, come documenti aziendali, password scritte o dispositivi scartati.

Prevenzione:

- Consapevolezza: Formazione regolare per riconoscere e segnalare tentativi di social engineering.
- Autenticazione a più fattori (MFA): Riduce l'efficacia delle credenziali rubate.
- Politiche di sicurezza: Creare procedure per la verifica dell'identità, soprattutto in caso di richieste non usuali.
- Monitoraggio: Implementare sistemi di rilevamento per comportamenti sospetti.
- Verifica fisica: Protezione delle aree riservate con badge elettronici, sorveglianza, e controlli di accesso rigorosi.

Prompt: Potresti descrivere più dettagliatamente il Tailgating, il Watering Hole Attack e il Dumpster Diving?

Risposta: Certamente, Francesco! Ecco una descrizione più dettagliata di ciascuna tecnica:

Tailgating (o Piggybacking)

Cos'è:

Il tailgating è una tecnica di social engineering fisico in cui un attaccante entra in un'area riservata o protetta approfittando della presenza di una persona autorizzata. Questa tecnica sfrutta la cortesia umana, come tenere aperta una porta per un'altra persona, o la distrazione.

Come funziona:

1. Seguire una persona autorizzata:

- L'attaccante può simulare situazioni di urgenza (ad esempio, fingere di avere le mani occupate con documenti o dispositivi).
- Spesso indossa abiti o badge che lo fanno sembrare un dipendente o un fornitore.

2. Accesso non autorizzato:

- Una volta all'interno, l'attaccante può accedere a sistemi, dispositivi, o raccogliere informazioni sensibili lasciate incustodite.

Prevenzione:

- Politiche aziendali che proibiscono l'apertura della porta a persone non identificate.
 - Utilizzo di sistemi di badge elettronici o biometrici per l'accesso.
 - Formazione del personale per riconoscere comportamenti sospetti.
-

Watering Hole Attack

Cos'è:

Il watering hole attack prende il nome dalle abitudini degli animali di frequentare gli stessi punti d'acqua. In questa tecnica, un attaccante compromette un sito web che è frequentemente visitato dal target (come un sito di un fornitore, un forum di settore o un portale aziendale).

Come funziona:

1. Ricerca del target:

- L'attaccante identifica i siti o le piattaforme online utilizzate regolarmente dalla vittima o dal gruppo di vittime.

2. Compromissione del sito:

- Viene inserito malware nel sito tramite vulnerabilità note o sfruttando accessi amministrativi.

3. Infezione della vittima:

- Quando la vittima accede al sito, il malware viene scaricato o eseguito automaticamente, consentendo all'attaccante di rubare informazioni, installare spyware o compromettere reti interne.

Prevenzione:

- Mantenere aggiornati i software e i sistemi di navigazione.
 - Monitorare i siti web visitati dal personale e utilizzare soluzioni di sicurezza, come firewall e sandboxing.
 - Evitare di accedere a siti non sicuri da dispositivi aziendali.
-

Dumpster Diving

Cos'è:

Il dumpster diving consiste nel recuperare informazioni utili rovistando nei rifiuti di un'organizzazione o di un individuo. Queste informazioni possono includere documenti cartacei, dispositivi elettronici o materiali eliminati impropriamente.

Come funziona:

1. Raccolta di materiali scartati:

- Gli attaccanti cercano informazioni gettate nei cestini, come appunti con password, dati personali, fatture, contratti o dispositivi smaltiti.

2. Utilizzo delle informazioni:

- Le informazioni recuperate possono essere usate per ottenere accessi non autorizzati o per lanciare attacchi di phishing mirati.

Esempi:

- Trovare un foglio con credenziali scritte.
- Raccogliere dispositivi di archiviazione non correttamente cancellati.

Prevenzione:

- Utilizzo di distruggidocumenti per i materiali cartacei sensibili.
- Politiche di smaltimento sicuro per dispositivi elettronici.
- Creazione di processi di sensibilizzazione sul valore delle informazioni.

Prompt: Grazie. Potresti anche spiegarmi come prevenire ed eventualmente difendermi da attacchi di social engineering?

Risposta: Certamente, Francesco! La prevenzione e la difesa contro il social engineering si basano su una combinazione di consapevolezza, buone pratiche e strumenti di sicurezza. Ecco una guida dettagliata:

1. Formazione e Consapevolezza

Perché è importante:

Gli attacchi di social engineering si basano principalmente sull'errore umano. Una forza lavoro consapevole e ben formata è il primo scudo.

Azioni:

- **Corsi di formazione regolari:**
 - Insegnare a riconoscere i segnali di un attacco, come email sospette o richieste insolite.
 - **Simulazioni di attacco:**
 - Testare i dipendenti con esercizi di phishing o pretexting per misurare la loro preparazione.
 - **Politiche aziendali chiare:**
 - Stabilire procedure per verificare richieste di informazioni sensibili, anche se apparentemente legittime.
-

2. Protezioni Tecnologiche

Strumenti essenziali:

- **Autenticazione a più fattori (MFA):**
 - Aggiunge un ulteriore livello di sicurezza anche se le credenziali vengono rubate.
- **Firewall e software di sicurezza:**
 - Blocca siti web pericolosi e tentativi di installare malware.

- **Email Filtering:**
 - Identifica e filtra email sospette o con contenuti ingannevoli.
 - **Aggiornamenti regolari:**
 - Mantenere i sistemi e i software aggiornati per ridurre le vulnerabilità.
-

3. Verifica e Controllo

Strategie:

- **Politiche di verifica dell'identità:**
 - Prima di fornire informazioni o accedere a un sistema, richiedere verifiche rigorose.
 - Ad esempio, non accettare richieste telefoniche o via email senza ulteriori controlli.
 - **Limitazione degli accessi:**
 - Concedere accessi solo alle persone che ne hanno stretta necessità (principio del minimo privilegio).
 - **Registri di accesso:**
 - Monitorare chi entra e chi esce dalle aree fisiche e dai sistemi.
-

4. Sicurezza Fisica

Misure preventive:

- **Badge di accesso e controlli biometrici:**
 - Impediscono il tailgating e garantiscono che solo il personale autorizzato possa accedere.
 - **Distruggidocumenti:**
 - Eliminare in modo sicuro documenti sensibili per prevenire il dumpster diving.
 - **Controllo delle aree riservate:**
 - Utilizzare telecamere di sorveglianza e procedure di verifica del personale.
-

5. Comunicazione e Segnalazione

Best practices:

- **Canali per segnalare sospetti:**
 - Creare un sistema semplice per permettere ai dipendenti di segnalare email o comportamenti sospetti.
- **Cultura della sicurezza:**
 - Promuovere l'idea che tutti sono responsabili della sicurezza, incoraggiando una mentalità proattiva.

6. Strategie per Rispondere a un Attacco

Cosa fare se sospetti un attacco:

1. Non agire impulsivamente:

- Non cliccare su link sospetti, non condividere informazioni, e non scaricare file non richiesti.

2. Segnala immediatamente:

- Informare il team di sicurezza o il responsabile IT.

3. Analizza il danno:

- Verifica se dati sensibili sono stati esposti e attua misure di contenimento (ad esempio, reimpostare password).

4. Avvisa le parti interessate:

- In caso di compromissione di account o dati, informare collaboratori o clienti coinvolti.

Esempi di Regole Pratiche

- **Non fidarsi dell'urgente o dell'insolito:**

- Gli attacchi spesso sfruttano la pressione del tempo.

- **Verifica indipendente:**

- Ad esempio, se ricevi una telefonata da "IT", richiama al numero ufficiale, non a quello fornito dall'interlocutore.

- **Evita di condividere informazioni sui social media:**

- Gli attaccanti spesso raccolgono informazioni da profili pubblici per creare attacchi mirati.

Esercizio BONUS: Esplorazione dei CVE tramite ChatGPT

Prompt: Potresti fornirmi un report delle CVE (Common Vulnerabilities and Exposures) di WhatsApp?

Risposta: Ecco alcune vulnerabilità (CVE) rilevanti associate a WhatsApp negli ultimi anni:

1. **CVE-2019-11932:** Un attacco di tipo "double-free" nel parser delle immagini GIF. Questa vulnerabilità consentiva a un attaccante remoto di eseguire codice arbitrario o causare un crash, sfruttando una GIF appositamente creata su WhatsApp per Android, prima della versione 2.19.244.
2. **CVE-2020-1907:** Una vulnerabilità che interessava WhatsApp per Android e iOS, legata alla gestione non sicura dei dati nella memoria durante alcune operazioni. Questo problema poteva consentire l'esecuzione di codice arbitrario se sfruttato.
3. **CVE-2021-24027:** Un problema di overflow del buffer durante la gestione delle chiamate RTP. Questa vulnerabilità poteva essere sfruttata per eseguire codice remoto su dispositivi vulnerabili.

4. **CVE-2024-45607 e CVE-2024-6670:** Vulnerabilità più recenti, ancora in analisi approfondita, che riguardano rispettivamente la configurazione della cache TLS e possibili problemi di sicurezza nella gestione delle richieste API. Maggiori dettagli potrebbero essere disponibili man mano che vengono pubblicati i report completi.

Come proteggerti

- **Aggiorna regolarmente l'app:** WhatsApp rilascia patch per risolvere vulnerabilità conosciute.
- **Non aprire contenuti sospetti:** Evita di visualizzare file multimediali (GIF, immagini, ecc.) o cliccare su link provenienti da fonti non affidabili.
- **Usa una rete sicura:** Preferisci connessioni protette (ad esempio, VPN o reti Wi-Fi sicure).

Per ulteriori dettagli sulle vulnerabilità specifiche, puoi consultare i database CVE ufficiali come [CVE.org](https://cve.org).

Traccia EXTRA: Creazione di una mail di phishing

Notifica urgente: indagini in corso sul suo account Telegram

from: Francesco Orrù <francesco.orrù@aiss.com>



Gentile **Archimede DeLaurentis**,

abbiamo ricevuto segnalazioni e prove concrete, da parte di un Suo parente stretto, relative alla Sua partecipazione a gruppi su Telegram associati alla distribuzione di materiale pedopornografico, violando gravemente le leggi nazionali e internazionali.

Le autorità competenti stanno conducendo un'indagine approfondita. Le attività sospette sono state registrate, e i dettagli del Suo account (**Telegram nickname:P3d0Bear69**), inclusi IP (**151.40.126.200**) e posizione (**Via Giorgio Washington 106, 20126, Milano**) sono stati segnalati.

Le offriamo la possibilità di cooperare per evitare la divulgazione delle accuse o l'immediato inoltro del caso alle Forze dell'Ordine. Per discutere i termini di quest'ultima, anche insieme al parente che ci ha fornito le informazioni (si è reso disponibile a collaborare), la preghiamo di visitare il seguente link e a compilare il modulo richiesto: <https://dichiarazione.aiss.com/>
Nota bene: il mancato riscontro entro 24 ore comporterà l'attivazione delle procedure legali previste. Restiamo in attesa di un Suo riscontro.

Cordiali saluti,

Francesco Orrù

AISS Reparto Anti-Abusi



Il link nella mail porterà al download di un software malevolo che ci consentirà di accedere in remoto al PC/Smartphone della vittima, rubando ancora più informazioni che ci permetteranno di continuare l'attacco al malcapitato criminale.