

TRACCIA TASK 05/12/24

Social Engineering e Tecniche di Difesa

Dovrete scrivere un prompt per ChatGPT che vi permetta di ottenere informazioni dettagliate sulle tecniche di social engineering. Analizzate gli esempi forniti e sviluppate una serie di raccomandazioni per prevenire tali attacchi. Infine, create una presentazione o un documento che riassume le vostre scoperte e raccomandazioni.

Esercizio BONUS Esplorazione dei CVE tramite ChatGPT

Dovrete scrivere un prompt per ChatGPT che vi permetta di ottenere informazioni sui CVE rilevanti per un determinato software o sistema operativo. Utilizzate il prompt per ottenere una lista di vulnerabilità, quindi scegliete alcune di esse per approfondire le informazioni fornite.

TASK 05/12/24

Prompt per social engineering e tecniche di attacco

"Potresti spiegarmi cos'è il social engineering e descrivere in dettaglio le tecniche più comuni utilizzate dagli attaccanti, come il phishing, il tailgating e il pretexting etc.?"

Motivazione:

Ho scelto questo prompt dato che secondo me copre due aspetti fondamentali:

1. Introduce il concetto di social engineering.
2. Elenca tecniche specifiche, permettendo di ottenere una descrizione chiara e dettagliata delle strategie.

Output:

Certo! Il **social engineering** è una forma di manipolazione psicologica che gli attaccanti utilizzano per ingannare le persone e spingerle a compiere azioni specifiche o a rivelare informazioni riservate. Invece di violare direttamente i sistemi informatici, i social engineer sfruttano la fiducia, l'ignoranza o la disattenzione delle vittime per raggiungere i loro obiettivi.

Tecniche più comuni di social engineering

1. Phishing

- **Descrizione:** L'attaccante invia comunicazioni false (email, messaggi, o siti web) che sembrano provenire da fonti legittime, come banche, aziende o istituzioni.
- **Obiettivo:** Indurre la vittima a cliccare su un link malevolo, scaricare malware o fornire credenziali di accesso.
- **Varianti:**
 - Spear Phishing: Messaggi altamente personalizzati, mirati a specifiche persone o organizzazioni.
 - Whaling: Phishing rivolto a figure di alto profilo come dirigenti o amministratori.
 - Smishing: Phishing tramite SMS.
 - Vishing: Phishing tramite telefonate.

2. Tailgating (o Piggybacking)

- **Descrizione:** L'attaccante si intrufola in aree riservate seguendo fisicamente una persona autorizzata, spesso sfruttando la cortesia o la distrazione della vittima.

- **Esempio:** Un attaccante si presenta come un corriere e chiede di essere fatto entrare in un ufficio senza un badge.
-

3. Pretexting

- **Descrizione:** L'attaccante crea una falsa identità (il "pretesto") per ottenere informazioni riservate o accesso non autorizzato.
 - **Esempio:** Fingere di essere un tecnico IT che necessita delle credenziali per "risolvere un problema".
 - **Obiettivo:** Costruire una narrativa convincente che convinca la vittima a fidarsi.
-

4. Baiting

- **Descrizione:** L'attaccante offre qualcosa di attraente (es. un dispositivo USB o un download gratuito) per indurre la vittima a scaricare malware o a fornire informazioni.
 - **Esempio:** Una chiavetta USB lasciata "accidentalmente" in un parcheggio con un'etichetta come "stipendi aziendali".
-

5. Quid Pro Quo

- **Descrizione:** L'attaccante promette qualcosa in cambio di informazioni o accesso.
 - **Esempio:** Fingere di essere un ricercatore che offre un buono regalo in cambio di dettagli personali.
-

6. Dumpster Diving

- **Descrizione:** Gli attaccanti cercano informazioni utili nei rifiuti, come documenti stampati, vecchi dispositivi, o appunti.
 - **Obiettivo:** Recuperare informazioni come credenziali, numeri di conto o dettagli aziendali.
-

7. Shoulder Surfing

- **Descrizione:** Osservare qualcuno mentre digita una password, un PIN o altre informazioni sensibili.
 - **Esempio:** Guardare uno schermo da dietro una persona in un luogo pubblico.
-

8. Impersonation (Impersonificazione)

- **Descrizione:** L'attaccante si finge una persona autorizzata per ottenere accesso fisico o digitale.
- **Esempio:** Presentarsi come un dipendente nuovo e chiedere aiuto per accedere a un sistema.

Il social engineering è particolarmente efficace perché sfrutta il "fattore umano", spesso il punto più vulnerabile nella sicurezza. Riconoscere queste tecniche e adottare misure preventive è essenziale per proteggersi!

Prompt per strategie di difesa contro il social engineering

Scelta:

"Puoi descrivere alcune strategie pratiche per educare i dipendenti e aumentare la consapevolezza riguardo ai rischi del social engineering?"

Motivazione:

Ho selezionato questo prompt perché punta direttamente sulla prevenzione, che ritengo la difesa più efficace contro il social engineering. Fornire raccomandazioni pratiche migliora l'applicabilità delle informazioni e rende il prompt utile sia per aziende che per singoli individui.

Output:

Certamente! Educare i dipendenti sui rischi del **social engineering** è fondamentale per proteggere l'azienda da attacchi. Ecco alcune **strategie pratiche** per aumentare la consapevolezza e promuovere comportamenti sicuri:

1. Programmi di formazione regolari

- **Organizza corsi periodici** sulla sicurezza informatica, con particolare attenzione al social engineering.
- **Esempio pratico:** Simulazioni di phishing in cui i dipendenti ricevono email false create per testare la loro capacità di riconoscere un tentativo di phishing.
- **Scopo:** Insegnare a identificare segnali sospetti, come indirizzi email falsi o richieste urgenti di azioni.

2. Comunicazione chiara e continua

- **Newsletter di sicurezza:** Invia aggiornamenti regolari su nuove minacce o incidenti noti.
- **Poster e promemoria visivi:** Colloca materiali informativi in aree comuni, come uffici e sale riunioni.
- **Esempio:** Un poster con il titolo "Pensa prima di cliccare" e una checklist per identificare tentativi di phishing.

3. Simulazioni e test sul campo

- **Organizza esercitazioni pratiche:**
 - Fai simulazioni di attacchi come il phishing o il tailgating.
 - Osserva come i dipendenti reagiscono e fornisci feedback personalizzato.
- **Scopo:** Rendere i dipendenti più consapevoli delle tattiche reali usate dagli attaccanti.

4. Workshop interattivi

- **Sessioni di role-playing:** I dipendenti possono essere messi in scenari realistici dove devono rispondere a tentativi di social engineering (es. una telefonata di pretexting o un attacco di baiting).
- **Esempio:** Un workshop dove un facilitatore simula una chiamata fingendosi del supporto tecnico.

5. Incentivi e premi

- **Premia comportamenti corretti:** Offri incentivi per il personale che segnala tentativi di attacco o dimostra buone pratiche di sicurezza.
- **Esempio:** Un premio mensile per il "campione della sicurezza" scelto tra chi ha segnalato potenziali minacce.

6. Politiche di sicurezza chiare

- **Definisci procedure ben documentate:** Specifica cosa fare in caso di email sospette, telefonate strane o altre potenziali minacce.
 - **Esempio:** Fornisci un protocollo dettagliato su come verificare l'identità di chiunque richieda informazioni sensibili.
-

7. Racconta storie reali

- **Condividi casi di studio:** Mostra esempi di attacchi di social engineering avvenuti realmente, preferibilmente casi che abbiano coinvolto aziende simili.
 - **Esempio:** Racconta un caso in cui una persona è stata vittima di phishing e spiega le conseguenze.
-

8. Autenticazione e verifica

- **Promuovi la regola del "verificare prima di fidarsi":** I dipendenti devono sempre verificare l'identità di chi richiede informazioni.
 - **Esempio pratico:** Se qualcuno si presenta come un tecnico, chiedi un documento o conferma con il responsabile.
-

9. Politiche di accesso fisico

- **Allenamento sul tailgating:** Spiega che anche un gesto gentile, come tenere aperta una porta, può rappresentare un rischio.
 - **Esempio:** Mostra video che illustrano come un attaccante potrebbe intrufolarsi in un'area protetta.
-

10. Creare una cultura della sicurezza

- **Incoraggia la segnalazione:** Rendi chiaro che segnalare attività sospette non è solo accettabile, ma incoraggiato.
 - **Esempio:** Fornisci un canale anonimo per segnalare incidenti di sicurezza.
-

11. Uso di strumenti tecnologici

- **Filtri e avvisi:** Implementa strumenti come filtri anti-phishing e software di sicurezza che avvisano i dipendenti in caso di link sospetti.
 - **Esempio:** Software che mostra un messaggio "Questa email potrebbe non essere sicura" su email sospette.
-

12. Valutazioni regolari

- **Misura la consapevolezza:** Usa quiz o valutazioni per verificare quanto i dipendenti abbiano appreso.
 - **Esempio:** Dopo una formazione, invia un quiz con domande su come riconoscere un attacco di phishing.
-

Obiettivo principale

Queste strategie servono a **trasformare i dipendenti nella prima linea di difesa** contro il social engineering. Una combinazione di formazione continua, simulazioni pratiche e una cultura aziendale consapevole dei rischi aiuta a ridurre le vulnerabilità umane.

Se hai bisogno di approfondire uno specifico argomento, fammi sapere! 😊

Raccomandazioni:

Formazione e sensibilizzazione: Educare le persone a riconoscere i tentativi di manipolazione.

Verifica dell'identità: Non fornire informazioni sensibili senza verificare l'identità dell'interlocutore.

Uso di tecnologie di sicurezza: Implementare filtri anti-phishing e autenticazione multi-fattore.

Segnalazione di attività sospette: Segnalare immediatamente qualsiasi comunicazione o comportamento sospetto.

Prompt per CVE

Scelta:

"Potresti fornirmi una lista dei CVE più recenti relativi a **Zoom** con una breve descrizione e le possibili soluzioni?"

Motivazione:

Ho selezionato questo prompt perché si concentra su vulnerabilità aggiornate. Richiedendo soluzioni, il prompt permette di ottenere non solo una descrizione delle problematiche, ma anche indicazioni pratiche per risolvere o mitigare i rischi.

Output:

Ecco un elenco delle vulnerabilità CVE più recenti relative a Zoom, con una breve descrizione e le possibili soluzioni:

1. **CVE-2024-45422:** Vulnerabilità di validazione impropria dell'input in alcune app di Zoom che potrebbe consentire a un utente non autenticato di condurre un attacco di denial of service tramite accesso alla rete.
2. **CVE-2024-45421:** Overflow del buffer in alcune app di Zoom che potrebbe permettere a un utente autenticato di eseguire codice arbitrario o causare un crash dell'applicazione.
3. **CVE-2024-45420:** Consumo incontrollato delle risorse in alcune app di Zoom che potrebbe consentire a un utente autenticato di causare un denial of service.
4. **CVE-2024-45419:** Validazione impropria dell'input in alcune app di Zoom che potrebbe permettere a un utente non autenticato di divulgare informazioni tramite accesso alla rete.
5. **CVE-2024-45418:** Vulnerabilità di "Symbolic Link Following" nelle app di Zoom per macOS che potrebbe consentire a un utente autenticato di ottenere privilegi elevati o accedere a file non autorizzati.

Possibili Soluzioni:

- **Aggiornamento del Software:** È fondamentale mantenere tutte le applicazioni Zoom aggiornate all'ultima versione disponibile, poiché gli aggiornamenti includono patch di sicurezza che risolvono le vulnerabilità note.
- **Configurazioni di Sicurezza:** Verificare e configurare correttamente le impostazioni di sicurezza all'interno delle applicazioni Zoom per limitare l'accesso non autorizzato e prevenire potenziali exploit.
- **Consapevolezza degli Utenti:** Educare gli utenti sulle pratiche di sicurezza, come evitare di cliccare su link sospetti o condividere informazioni sensibili senza adeguate misure di protezione.

Per ulteriori dettagli e aggiornamenti, è consigliabile consultare i [Bollettini di Sicurezza di Zoom](#).

Output di approfondimento di alcuni punti:

Certamente, ecco un approfondimento sulle vulnerabilità identificate come **CVE-2024-45421**, **CVE-2024-45419** e **CVE-2024-45418**, incluse le loro descrizioni dettagliate e le soluzioni consigliate:

1. CVE-2024-45421: Buffer Overflow in alcune applicazioni Zoom

- **Descrizione:** Questa vulnerabilità è un buffer overflow che potrebbe consentire a un utente autenticato di eseguire un escalation dei privilegi tramite accesso alla rete. Con un punteggio CVSS di 8.5, è considerata di alta gravità.
[Tenable](#)

- **Impatto:** Un attaccante autenticato potrebbe sfruttare questa vulnerabilità per eseguire codice arbitrario o causare un crash dell'applicazione, compromettendo l'integrità e la disponibilità del sistema.
- **Soluzione:** Aggiornare le applicazioni Zoom interessate alla versione 6.2.0 o successiva, disponibile al sito ufficiale di Zoom. L'aggiornamento risolve la vulnerabilità correggendo la gestione del buffer.

2. CVE-2024-45419: Validazione impropria dell'input in alcune applicazioni Zoom

- **Descrizione:** Questa vulnerabilità riguarda una validazione impropria dell'input che potrebbe permettere a un utente non autenticato di divulgare informazioni tramite accesso alla rete. Ha un punteggio CVSS di 8.1, indicando una gravità elevata.
[Tenable](#)
- **Impatto:** Un attaccante potrebbe sfruttare questa falla per accedere a informazioni sensibili senza necessità di autenticazione, compromettendo la riservatezza dei dati.
- **Soluzione:** È essenziale aggiornare le applicazioni Zoom interessate alla versione 6.2.0 o successiva, disponibile al sito ufficiale di Zoom. L'aggiornamento implementa controlli di input più rigorosi per prevenire exploit.

3. CVE-2024-45418: Vulnerabilità di "Symbolic Link Following" negli installer di Zoom per macOS

- **Descrizione:** Questa vulnerabilità riguarda la gestione impropria dei collegamenti simbolici negli installer di alcune applicazioni Zoom per macOS, che potrebbe consentire a un utente autenticato di ottenere privilegi elevati tramite accesso alla rete. Ha un punteggio CVSS di 5.4, classificata come gravità media.
[Feedly](#)
- **Impatto:** Un attaccante potrebbe sfruttare questa vulnerabilità per eseguire operazioni con privilegi elevati, potenzialmente modificando file o configurazioni critiche del sistema.
- **Soluzione:** Aggiornare gli installer delle applicazioni Zoom per macOS alla versione 6.1.5 o successiva, disponibile al sito ufficiale di Zoom. Questo aggiornamento corregge la gestione dei collegamenti simbolici, prevenendo l'escalation dei privilegi.

Raccomandazioni Generali:

- **Aggiornamenti Regolari:** Assicurarsi che tutte le applicazioni Zoom siano sempre aggiornate all'ultima versione disponibile per beneficiare delle ultime patch di sicurezza.
- **Monitoraggio del Sistema:** Implementare misure di monitoraggio per rilevare attività sospette che potrebbero indicare tentativi di sfruttamento di vulnerabilità.
- **Consapevolezza degli Utenti:** Educare gli utenti sull'importanza di applicare tempestivamente gli aggiornamenti e sulle pratiche di sicurezza per prevenire exploit.