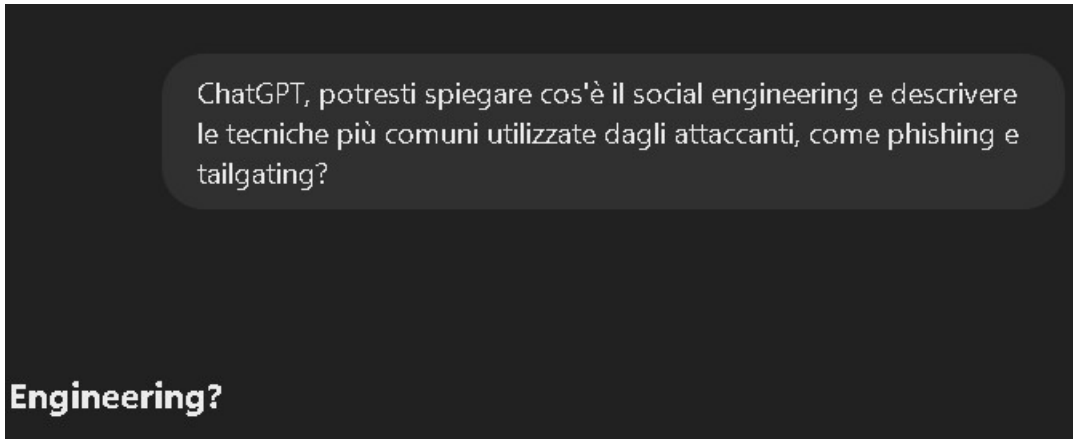


Report S5 L4

Nell'esercizio di oggi andremo ad utilizzare un Intelligenza artificiale (chatgpt) utilizzando dei prompt come:

"ChatGPT, potresti spiegare cos'è il social engineering e descrivere le tecniche più comuni utilizzate dagli attaccanti, come phishing e tailgating?"



ChatGPT, potresti spiegare cos'è il social engineering e descrivere le tecniche più comuni utilizzate dagli attaccanti, come phishing e tailgating?

Engineering?

Questa è stata la sua risposta:

Certamente!

Cos'è il Social Engineering?

Il social engineering è una tecnica di manipolazione psicologica utilizzata dagli attaccanti per indurre le persone a compiere azioni dannose o a divulgare informazioni sensibili. Invece di violare direttamente un sistema informatico, i criminali sfruttano la fiducia, l'inganno e la pressione psicologica per ottenere accessi o dati riservati.

💡 **Esempio pratico:** Un hacker si finge un tecnico dell'IT per convincere un dipendente a fornirgli la password aziendale.

Principali Tecniche di Social Engineering

✉ **Phishing**

Il phishing è un attacco che utilizza email, messaggi o siti web falsi per ingannare le vittime e ottenere dati sensibili (es. credenziali, numeri di carte di credito).

Esempio: Un'email che sembra provenire da PayPal ti chiede di "verificare il tuo account" cliccando su un link fasullo.

Difesa:

Controllare sempre il mittente dell'email.

Non cliccare su link sospetti.

Verificare direttamente sul sito ufficiale.

L'ho trovata molto utile e continuo la mia documentazione:

- secondo prompt:

"ChatGPT, potresti elencare e spiegare alcune strategie efficaci per difendersi dagli attacchi di social engineering"

risposta:

Certamente! Ecco alcune strategie efficaci per difendersi dagli attacchi di social engineering, suddivise per categoria di attacco.

1. Strategie Generali di Difesa

Queste tecniche sono valide per tutti i tipi di attacco basati sul social engineering.

- ✓ **Consapevolezza e formazione** → La miglior difesa è conoscere i rischi. Le aziende dovrebbero formare i dipendenti su come riconoscere le minacce.
- ✓ **Verificare sempre le fonti** → Non fornire mai informazioni sensibili senza una verifica indipendente dell'identità dell'interlocutore.
- ✓ **Regola del "Stop, Think, Verify"** → Se un'email o una richiesta sembra strana, fermarsi, riflettere e verificare prima di agire.
- ✓ **Usare l'autenticazione a due fattori (2FA)** → Anche se le credenziali vengono rubate, il 2FA impedisce l'accesso non autorizzato.
- ✓ **Non condividere dati sensibili pubblicamente** → Gli attaccanti spesso raccolgono informazioni dai social per creare attacchi personalizzati.

2. Difesa contro il Phishing (Email e SMS Fraudolenti)

- ✓ **Controllare l'indirizzo email del mittente** → Spesso gli hacker usano indirizzi molto simili a quelli legittimi (es. support@paypall.com invece di support@paypal.com).

✓ Non cliccare su link sospetti → Passare il mouse sopra il link per vedere l'URL reale prima di cliccare.

✓ Attenzione agli allegati → Non aprire file sospetti, soprattutto .exe, .zip o .doc con macro attivate.

✓ Usare filtri anti-phishing → Attivare i filtri di sicurezza nelle email per bloccare tentativi di phishing.

✓ Verificare i siti web → Se una email chiede di accedere a un servizio, visitare il sito ufficiale digitandolo manualmente nel browser, non cliccando il link.

3. Difesa contro il Vishing (Telefonate Fraudolente)

✓ Non fornire mai informazioni personali al telefono → Le banche e le aziende serie non chiedono mai PIN o password telefonicamente.

✓ Richiamare sempre il numero ufficiale → Se si riceve una chiamata sospetta, terminare la conversazione e richiamare il numero ufficiale dell'azienda o istituto.

✓ Fidarsi, ma verificare → Anche se la voce sembra affidabile, chiama sempre l'azienda per conferma prima di agire.

4. Difesa contro lo Smishing (SMS Fraudolenti)

✓ Diffidare di SMS con link sospetti → Non cliccare su link provenienti da numeri sconosciuti.

✓ Verificare direttamente con l'ente ufficiale → Se un SMS dice di contattare una banca o un'azienda, chiamare il numero ufficiale, non quello fornito nel messaggio.

✓ Bloccare e segnalare numeri sospetti → Gli smartphone permettono di bloccare i numeri di spam e segnalare tentativi di truffa.

5. Difesa contro il Pretexting (Finti tecnici, colleghi, autorità)

✓ Non fidarsi ciecamente dell'identità di qualcuno → Anche se sembra un tecnico IT o un collega, verificare sempre prima di fornire informazioni.

✓ Non condividere credenziali o dati aziendali senza verifica → Nessun tecnico IT chiederà mai la password di un utente per "risolvere un problema".

✓ Chiamare direttamente la persona o l'azienda → Se qualcuno dice di essere un dirigente o un dipendente, chiamare il numero aziendale ufficiale per verificare.

6. Difesa contro il Baiting (Esche digitali o fisiche)

✓ Non inserire chiavette USB sconosciute nel computer → Potrebbero contenere malware. Se si trova una chiavetta in un luogo pubblico, consegnarla al reparto IT.

✓ Scaricare software solo da fonti ufficiali → Gli hacker spesso usano versioni gratuite di programmi popolari per diffondere malware.

✓ Usare antivirus aggiornati → Un buon antivirus può rilevare e bloccare software malevolo installato tramite baiting.

7. Difesa contro il Tailgating (Accessi non autorizzati)

✓ Non tenere aperte porte o accessi per sconosciuti → Anche se sembra un dipendente o un tecnico, chiunque entri in un'area riservata deve essere identificato.

✓ Usare badge o sistemi di controllo accessi → Le aziende dovrebbero avere procedure di autenticazione per l'ingresso.

✓ Chiedere sempre l'identificazione → Se una persona sconosciuta cerca di accedere senza credenziali, segnalarlo immediatamente.

💡 Conclusione

Il social engineering sfrutta la psicologia umana per indurre le vittime a compiere azioni pericolose. La miglior difesa è la formazione, la consapevolezza e un sano scetticismo. Quando si riceve una richiesta sospetta, la regola d'oro è:

✓ STOP - THINK - VERIFY → Fermarsi, riflettere e verificare prima di agire.

Esercizio Bonus:

Esplorazione dei CVE tramite ChatGPT, chiedendo all'I.A con il prompt sottostante andremo ad approfondire la lista dei CVE ovvero le vulnerabilità note, ho scelto windows 7 perchè lo usa come VM per simulazioni di penetration testing e perchè lo vedo un livello intermedio tra windows XP (troppo facile) e windows 11 (molto più difficile da attaccare per ora)

"ChatGPT, potresti fornirmi una lista dei CVE relativi a windows 7? Vorrei anche informazioni dettagliate su alcuni di essi, inclusi i dettagli delle vulnerabilità e le soluzioni consigliate."

Risposta:

Certamente! Ecco un elenco di alcune vulnerabilità note (CVE) relative a Windows 7, con dettagli su ciascuna e le soluzioni consigliate:

1. CVE-2023-34367

Descrizione: Questa vulnerabilità consente un attacco di hijacking completo e cieco del protocollo TCP/IP su Windows 7. L'attaccante può sfruttare questa falla per intercettare o manipolare il traffico di rete senza che la vittima ne sia consapevole.

Soluzione: Microsoft ha classificato questa vulnerabilità come a bassa gravità e potrebbe non aver rilasciato una patch specifica. Si consiglia di:

Utilizzare firewall per monitorare e controllare il traffico di rete.

Aggiornare a una versione più recente di Windows, poiché Windows 7 non è più supportato ufficialmente.

2. CVE-2018-8562

Descrizione: Una vulnerabilità di elevazione dei privilegi esiste in Windows quando il componente Win32k gestisce in modo improprio gli oggetti in memoria. Un attaccante che sfrutta con successo questa vulnerabilità potrebbe eseguire codice arbitrario in modalità kernel.

Soluzione: Microsoft ha rilasciato aggiornamenti di sicurezza per risolvere questa vulnerabilità. Si consiglia di:

Installare gli ultimi aggiornamenti di sicurezza disponibili per Windows 7.

Considerare l'aggiornamento a una versione di Windows attualmente supportata.

3. CVE-2018-8453

Descrizione: Questa vulnerabilità riguarda l'elevazione dei privilegi in Windows quando il componente Win32k non gestisce correttamente gli oggetti in memoria. Un attaccante potrebbe ottenere il controllo completo del sistema interessato.

Soluzione: Microsoft ha rilasciato una patch per questa vulnerabilità. Si raccomanda di:

Applicare tutti gli aggiornamenti di sicurezza disponibili per Windows 7.

Valutare la migrazione a un sistema operativo più recente e supportato.

4. CVE-2017-0147

Descrizione: Il server SMBv1 in Windows 7 consente agli attaccanti remoti di eseguire codice arbitrario tramite pacchetti appositamente predisposti, noto come "Windows SMB

Remote Code Execution Vulnerability".

Soluzione: Disabilitare il protocollo SMBv1 e applicare le patch di sicurezza rilasciate da Microsoft. Inoltre, considerare l'aggiornamento a una versione più recente di Windows.

5. CVE-2014-4114

Descrizione: Conosciuta come la vulnerabilità "Sandworm", permette agli attaccanti di eseguire codice arbitrario attraverso un oggetto OLE appositamente creato in un documento di Microsoft Office su sistemi Windows 7.

Soluzione: Microsoft ha rilasciato aggiornamenti di sicurezza per affrontare questa vulnerabilità. È fondamentale:

Installare tutte le patch di sicurezza disponibili.

Evitare di aprire documenti da fonti non attendibili.

Nota Bene: Il supporto ufficiale per Windows 7 è terminato il 14 gennaio 2020. Pertanto, non vengono più rilasciati aggiornamenti di sicurezza per questo sistema operativo, rendendolo vulnerabile a nuove minacce. Si raccomanda vivamente di aggiornare a una versione più recente di Windows per garantire una protezione adeguata.

Le informazioni apprese mi saranno molto utili nelle future simulazioni di pen testing.

Grazie chatGPT.

Luca Tavani