

Esercizio S5L4 - Prompt design per ChatGPT

L'esercizio di oggi richiedeva la creazione di vari prompt per intavolare un discorso con l'IA al fine di meglio comprendere il concetto di social engineering e le sue applicazioni. Qui sotto la conversazione proposta con le mie domande in blu e le risposte del GPT.

Ciao ChatGPT, mi potresti dare una definizione di social engineering volto a un attacco informatico? Potresti darmi un po' di idee di quali sono esempi rilevanti in campo cybersecurity? Puoi anche aggiungere una metafora esplicativa, alla fine del discorso?

ChatGPT ha detto:



Ciao! Felice di aiutarti.

Social engineering in ambito di cybersecurity si riferisce a tecniche manipolative usate per indurre le persone a rivelare informazioni riservate o a compiere azioni che compromettono la sicurezza informatica. Gli attaccanti sfruttano errori umani, facendosi passare per figure di fiducia o utilizzando altri mezzi per ingannare la vittima e ottenere dati sensibili come password, accessi a sistemi o informazioni personali.

Esempi di Social Engineering in Cybersecurity

1. **Phishing:** Il tipo di attacco più comune, dove l'attaccante invia e-mail o messaggi falsi fingendosi un'entità legittima, come una banca o un'azienda nota. L'obiettivo è indurre la vittima a cliccare su un link dannoso o a inserire credenziali personali in un sito falso.
2. **Pretexting:** Qui l'attaccante inventa un pretesto per raccogliere informazioni, come fingere di essere un responsabile IT che ha bisogno di verificare l'identità di un dipendente. Questa tecnica si basa sulla creazione di una storia plausibile che spinga la vittima a rivelare informazioni importanti.
3. **Baiting:** Questo tipo di attacco offre alla vittima una "ricompensa" (ad esempio, un link per scaricare un software o un file interessante) che, una volta cliccata, infetta il dispositivo con malware.
4. **Quid Pro Quo:** L'attaccante promette un beneficio in cambio di informazioni o accesso. Ad esempio, potrebbe chiamare fingendosi un tecnico e offrire assistenza tecnica gratuita per risolvere un problema, chiedendo però l'accesso al sistema.
5. **Tailgating o Piggybacking:** Qui l'attaccante cerca di entrare in un'area riservata seguendo una persona autorizzata, approfittando della cortesia o della distrazione altrui, senza aver bisogno di badge o credenziali.

Metafora esplicativa

Pensa al social engineering come a un ladro che bussa alla porta fingendo di essere un postino. Se si presenta vestito di tutto punto e con un pacco in mano, la persona all'interno della casa potrebbe non sospettare nulla e lasciarlo entrare. Il social engineering sfrutta proprio questo tipo di fiducia ingannevole, inducendo le persone a ignorare le loro normali misure di sicurezza in base a una percezione di legittimità.

Essere consapevoli di queste tecniche può aiutare a riconoscerle prima che si concretizzino in una violazione della sicurezza.

Hai detto:

In sostanza, è come il lupo che mette la mano nella farina per fingersi un agnello, e si fa aprire così la porta dall'agnellino che pensa che sia la mamma?

ChatGPT ha detto:



Esattamente! Hai colto il concetto perfettamente.

Proprio come il lupo che si trucca da agnello per ingannare e farsi aprire la porta, il social engineer maschera le proprie intenzioni dietro una falsa identità o un'apparenza rassicurante. L'agnellino, fidandosi della facciata, apre la porta senza sospettare nulla, proprio come una vittima di social engineering che potrebbe rivelare informazioni o concedere accessi pensando di interagire con una figura legittima.

È un perfetto esempio di come la manipolazione psicologica sia alla base di molti attacchi di social engineering. Chi attacca non cerca solo di superare barriere tecniche, ma punta prima di tutto a bypassare la fiducia e la vigilanza di chi sta dall'altra parte.

Hai detto:

Quali possono essere i migliori metodi di difesa dai metodi di social engineering che mi hai elencato?

ChatGPT ha detto:



Ottima domanda! Difendersi dal social engineering richiede consapevolezza e alcune buone pratiche, dato che gli attacchi puntano sulle debolezze umane più che su falle tecniche. Ecco alcuni dei metodi di difesa più efficaci:

1. Formazione e Consapevolezza

- **Sensibilizzazione continua:** La prima linea di difesa è formare le persone sui rischi del social engineering. Esempi di attacchi, esercitazioni di phishing simulate e

workshop aumentano la consapevolezza, riducendo la probabilità che qualcuno cada nella trappola.

- **Diffidare dell'urgenza:** Gli attacchi di social engineering spesso si basano sul creare un senso di fretta o urgenza. È importante prendere tempo e riflettere prima di agire o di condividere informazioni.

2. Verifica dell'Identità

- **Autenticazione diretta:** Se si riceve una richiesta di informazioni riservate o di accesso, verificare sempre l'identità del richiedente tramite un canale ufficiale. Ad esempio, contattare direttamente la persona o l'azienda che ha fatto la richiesta, senza usare i contatti forniti nell'e-mail o nel messaggio sospetto.
- **Doppia autenticazione:** In caso di informazioni sensibili, ricorrere a una seconda conferma, ad esempio, richiedendo la conferma di un collega o un supervisore.

3. Protezione contro il Phishing

- **Analisi dei link e degli indirizzi email:** Controllare sempre l'indirizzo email del mittente, evitando di cliccare su link sospetti. Si possono passare i link con il mouse senza cliccare, per vedere l'URL di destinazione.
- **Utilizzo di filtri anti-phishing:** Molti servizi e-mail dispongono di filtri anti-phishing, ma strumenti specifici (come i filtri nei browser o software antivirus avanzati) possono aggiungere un ulteriore livello di protezione.

4. Regole Rigide per il Controllo degli Accessi

- **Politica del "Need-to-Know":** Concedere l'accesso solo a chi ne ha realmente bisogno per svolgere il proprio lavoro. Limitare l'accesso ai dati e alle aree riservate riduce il rischio di compromissione in caso di attacco.
- **No tailgating:** Essere sempre attenti a chi si trova nelle vicinanze in aree riservate. Ad esempio, nei luoghi di lavoro, si può implementare l'uso di badge o sistemi biometrici per evitare che persone non autorizzate possano accedere.

5. Implementazione di una "Cultura del Dubbio"

- **Pensare sempre che un attacco sia possibile:** Inculcare l'abitudine di essere prudenti e critici, specialmente per richieste non ordinarie o messaggi di persone che si presentano come autorità (responsabili IT, manager, ecc.).
- **Condivisione immediata di possibili tentativi di attacco:** Incoraggiare le persone a segnalare subito qualsiasi messaggio o telefonata sospetta al dipartimento IT o alla sicurezza. Anche una falsa segnalazione è meglio di un'intrusione riuscita.

6. Sistemi di Autenticazione a Due Fattori (2FA)

- **Aggiunta di una barriera ulteriore:** Il 2FA rende difficile per un attaccante accedere anche se dovesse riuscire a ottenere la password. Ogni tentativo di accesso richiederà un secondo codice che arriva via SMS o tramite app di autenticazione.

7. Utilizzo di Software Antivirus e Firewall Aggiornati

- **Protezione contro i malware:** Strumenti come antivirus, firewall e antimalware, regolarmente aggiornati, possono bloccare molti degli allegati o dei download dannosi distribuiti tramite e-mail o link di phishing.

Metafora esplicativa

Difendersi dal social engineering è come tenere la porta di casa ben chiusa e verificare sempre chi c'è dall'altra parte prima di aprire. Potrebbe esserci il "lupo" mascherato da amico, quindi bisogna allenare l'occhio e la pazienza, verificando chi è realmente, magari chiedendo una conferma o passando la richiesta a qualcun altro in casa. Meglio fare un controllo in più, che trovarsi un intruso all'interno!

Ciao ChatGPT, potresti elencarmi le CVE rispettivamente per Windows XP e Windows 11, e come si sono evolute nel tempo rispetto a quanto si sono evoluti i sistemi operativi stessi?

ChatGPT ha detto:



Ciao! Esplorare le CVE di Windows XP e Windows 11 rivela come la sicurezza dei sistemi operativi Microsoft sia migliorata in risposta alla crescente sofisticazione delle minacce. Le CVE (Common Vulnerabilities and Exposures) sono identificatori univoci per vulnerabilità note, e osservare la loro evoluzione per questi sistemi aiuta a comprendere come sono cambiati gli approcci alla sicurezza.

1. Windows XP (2001 - Supporto terminato nel 2014)

- **Totale delle vulnerabilità:** Windows XP ha avuto centinaia di CVE, con un picco di vulnerabilità tra il 2006 e il 2014, quando il sistema era ancora ampiamente utilizzato.
- **Tipi di vulnerabilità comuni:**
 - **Esecuzione di codice remoto (RCE):** Spesso legata a servizi di rete come il famigerato **WannaCry** (CVE-2017-0144), che sfruttava un exploit chiamato EternalBlue per diffondersi tramite SMB.
 - **Privilege Escalation:** Permetteva agli attaccanti di ottenere privilegi elevati una volta penetrato nel sistema.
 - **Buffer Overflow:** Molte vulnerabilità di Windows XP erano legate a difetti di memoria, soprattutto dovuti all'assenza di sistemi avanzati di protezione della memoria.
- **Evoluzione della sicurezza:** Windows XP fu sviluppato in un'epoca in cui le minacce informatiche erano meno sofisticate e non vennero adottate molte delle protezioni moderne come ASLR (Address Space Layout Randomization) e DEP (Data Execution Prevention), che oggi sono standard.

- **Fine del supporto:** Nel 2014, con la fine del supporto, Microsoft smise di pubblicare patch di sicurezza per XP, lasciando aperte molte vulnerabilità.

2. Windows 11 (2021 - Oggi)

- **Totale delle vulnerabilità:** Windows 11, lanciato nel 2021, ha finora accumulato molte meno CVE rispetto a Windows XP, grazie agli avanzamenti nella sicurezza intrinseca del sistema operativo.
- **Tipi di vulnerabilità comuni:**
 - **Sicurezza del Kernel e dei Driver:** Windows 11 contiene meccanismi per limitare l'accesso non autorizzato al kernel, ma alcune vulnerabilità recenti hanno riguardato driver di terze parti e potenziali escalation di privilegi.
 - **Misure anti-malware e ransomware:** Windows 11 è dotato di protezioni avanzate contro il malware, integrate con strumenti come Microsoft Defender e sandboxing per le applicazioni, anche se gli attacchi di phishing e di social engineering rimangono un rischio.
 - **Crittografia e Sicurezza TPM:** Con l'adozione obbligatoria di TPM 2.0 e Secure Boot, Windows 11 è progettato per proteggere meglio le chiavi crittografiche e impedire attacchi al bootloader.
- **Evoluzione della sicurezza:**
 - **Virtualization-Based Security (VBS) e Hypervisor-Protected Code Integrity (HVCI):** Introdotti per isolare parti sensibili del sistema operativo in ambienti virtualizzati, riducendo il rischio di attacchi diretti alla memoria.
 - **Ransomware e Anti-exploit:** Tecniche avanzate contro l'esecuzione di codice malevolo sono ora integrate con il supporto alla protezione contro il ransomware.
 - **Supporto continuativo:** Windows 11 riceve aggiornamenti regolari e patch di sicurezza mensili (Patch Tuesday), il che riduce il rischio di vulnerabilità sfruttabili.

Evoluzione generale dal punto di vista della sicurezza

- **Da XP a Windows 11,** Microsoft ha adottato sempre più misure proattive e sistemi avanzati di protezione per mitigare gli attacchi:
 - **Difese integrate:** Strumenti come Windows Defender e SmartScreen, introdotti con Windows 8 e potenziati fino a Windows 11, oggi proteggono gli utenti da molte minacce online.
 - **Virtualizzazione e isolamento:** Funzionalità di sicurezza basate su virtualizzazione, assenti in Windows XP, sono ora essenziali per mantenere sicuro l'ambiente operativo in Windows 11.
 - **Patch management:** Con l'evoluzione del Patch Tuesday e degli aggiornamenti automatici, Microsoft è in grado di distribuire rapidamente patch, limitando la durata delle vulnerabilità attive rispetto a quanto accadeva con XP.
 - **Integrazione di AI e machine learning:** Oggi, sistemi avanzati di machine learning rilevano e bloccano minacce in tempo reale, rendendo Windows 11 significativamente più sicuro rispetto a XP.

Conclusione

L'evoluzione delle CVE da Windows XP a Windows 11 riflette l'aumento delle minacce informatiche e la risposta di Microsoft con misure di sicurezza sempre più avanzate.

Windows XP era privo di molti degli strumenti di sicurezza che oggi consideriamo standard, mentre Windows 11 è progettato per affrontare un panorama di minacce in continua crescita.