

S5-L4

Chatgpt prompt command



Obiettivo: Esplorare tecniche di social engineering

Lato attacco

Comprendere il social engineering utilizzando i prompt di Chatgpt ottenendo informazioni avendo una panoramica generale su cos'è e sulle tecniche che utilizzano gli attaccanti in questo campo

Lato difesa

Ottenerne tramite Chatgpt una panoramica generale su come ci si può difendere da questi attacchi concentrandoci sulle tecniche più efficaci.

AI

Lato attacco

ChatGPT

Potresti spiegarmi cos'è il social engineering e le tecniche più avanzate che utilizza un attaccante in questo ambito?

Il social engineering è una tecnica di manipolazione psicologica usata dagli attaccanti per indurre le persone a rivelare informazioni riservate o compiere azioni specifiche, come scaricare malware o condividere credenziali di accesso. Gli attacchi di social engineering si basano sulla fiducia e spesso sfruttano emozioni come paura, curiosità o urgenza. La vittima viene manipolata per bypassare le misure di sicurezza, diventando il punto di accesso per l'attaccante a un sistema o a una rete.

Ecco alcune delle tecniche di social engineering più avanzate:

1. Phishing mirato (Spear Phishing)

- A differenza del phishing generico, il **spear phishing** è personalizzato per un individuo o un piccolo gruppo. Gli attaccanti studiano le vittime e creano email o messaggi apparentemente autentici. Ad esempio, possono simulare comunicazioni dall'azienda della vittima o addirittura inviare richieste via SMS (smishing) o telefonate (vishing).
- Tecniche avanzate:** Gli attaccanti utilizzano spesso informazioni pubbliche, come social media e comunicati stampa, per rendere i messaggi più credibili.

2. Pretexting

Scrivi un messaggio a ChatGPT

ChatGPT può commettere errori. Considera di verificare le informazioni importanti.

Per avere una panoramica migliore, ho chiesto a chatgpt di fare un riassunto per potermi eventualmente informare sui tipi di attacco singolarmente

Domanda generale sul social engineering e su quali tipi di attacco si utilizzano nel settore

ChatGPT

Potresti riassumermelo?

Certo!

Il **social engineering** è una tecnica di manipolazione psicologica usata dagli attaccanti per ingannare le persone e ottenere informazioni o accesso a sistemi. Gli attacchi sfruttano la fiducia e spesso manipolano emozioni come urgenza o curiosità.

Ecco un riassunto delle tecniche principali:

- 1. Spear Phishing:** Email o messaggi personalizzati per ingannare specifiche persone, spesso basati su informazioni pubbliche per sembrare autentici.
- 2. Pretexting:** L'attaccante si finge una figura di fiducia (come un tecnico IT) per ottenere dati.
- 3. Quid Pro Quo:** Promette un aiuto o un servizio in cambio di accesso o informazioni.
- 4. Baiting:** Usa esche come chiavette USB "dimenticate" o download gratuiti per infettare dispositivi.
- 5. Tailgating:** Infiltrazione fisica seguendo un dipendente per entrare in un edificio o accedere a dispositivi.
- 6. Business Email Compromise (BEC):** Compromette email aziendali di dirigenti per inviare istruzioni fraudolente.

Scrivi un messaggio a ChatGPT

ChatGPT può commettere errori. Considera di verificare le informazioni importanti.

Lato Difesa

Con questo prompt, essendo l'IA già consapevole dell'argomento inserito prima, ho chiesto semplicemente come posso difendermi e se può anche riassumerlo in modo da avere una panoramica migliore anche in questo caso.

The screenshot shows a ChatGPT interface. At the top left is the 'ChatGPT' logo with a dropdown arrow. On the right are a 'Condividi' button with a share icon and a purple circular profile picture with the letters 'MD'. The main area has a light gray background with a dark gray sidebar on the left. A message bubble from the user asks: 'Come posso difendermi al meglio da questo tipo di attacco? Potresti anche riassumerlo?'. Below it, a response from 'ChatGPT' (indicated by a small circular icon with a swirl) provides tips: 'Per difenderti al meglio dal social engineering, è importante essere sempre vigile e adottare alcune misure preventive:' followed by a numbered list of six items. At the bottom is a text input field with the placeholder 'Scrivi un messaggio a ChatGPT' and a small info icon. A note at the bottom states: 'ChatGPT può commettere errori. Considera di verificare le informazioni importanti.' There are also up and down arrows and a question mark icon in the bottom right corner.

Come posso difendermi al meglio da questo tipo di attacco? Potresti anche riassumerlo?

Per difenderti al meglio dal social engineering, è importante essere sempre vigile e adottare alcune misure preventive:

1. **Formazione:** Impara a riconoscere tecniche comuni di inganno e segnali sospetti. Anche le aziende dovrebbero fornire regolare formazione di sicurezza ai dipendenti.
2. **Doppia Verifica:** Prima di condividere informazioni sensibili o fare operazioni, verifica sempre con una seconda fonte (come una chiamata diretta) l'identità di chi lo richiede.
3. **Password Sicure e 2FA:** Usa password robuste, evita di riutilizzarle e attiva l'autenticazione a due fattori (2FA) dove possibile.
4. **Diffida di Email e Link Sospetti:** Non aprire allegati o link da mittenti sconosciuti o strani. In caso di dubbio, contatta direttamente la persona o l'azienda.
5. **Limitare le Informazioni Personalari Pubbliche:** Evita di condividere informazioni personali sui social media che potrebbero essere usate per personalizzare un attacco.
6. **Procedure di Sicurezza Interne:** Se sei in azienda, adotta protocolli di conferma specifici per transazioni e accesso alle informazioni sensibili.

Scrivi un messaggio a ChatGPT

ChatGPT può commettere errori. Considera di verificare le informazioni importanti.

Conclusioni

L'intelligenza artificiale oggi rappresenta una forza di cambiamento profonda, automatizzando compiti ripetitivi, migliorando la produttività, e facilitando decisioni più informate grazie all'analisi avanzata dei dati. Viene usata in vari settori, dal business alla sanità, offrendo supporto nel servizio clienti, nella gestione delle risorse, e persino nella diagnosi medica. Allo stesso tempo, però, l'IA solleva questioni etiche e sociali, come la privacy e il futuro del lavoro umano, spingendo verso una riflessione sul suo ruolo e sul suo impatto nella società.



Thank You!

Mattia Di Donato