

Rapporto

Ho iniziato il compito di oggi chiedendo a ChatGPT qual è il modo corretto di sollecitare per assicurarmi che mi risponda:

Ciao, come stai?



Ciao! Sto bene, grazie! E tu come stai? 😊

Anch'io. Sarebbe meglio se mi dicessi come dovrei scrivere un prompt per farti una domanda specifica per essere sicuro che tu risponda correttamente a quella domanda



Per ottenere risposte precise e utili, è importante scrivere un prompt chiaro e ben definito. Essere diretti e dettagliati aiuta a evitare ambiguità, permettendo a chi risponde di comprendere esattamente cosa desideri sapere. Fornire contesto aggiuntivo, come il progetto su cui stai lavorando, è fondamentale per ottenere una risposta mirata. Inoltre, specificare il formato della risposta (elenco, spiegazione passo-passo, ecc.) può garantire che le informazioni siano presentate nel modo più utile per te. Non dimenticare di indicare la lingua in cui preferisci ricevere la risposta e cerca di fare una domanda alla volta per mantenere la conversazione chiara e focalizzata. Con questi accorgimenti, riuscirai a ottenere risposte più precise e pertinenti alle tue necessità.

🗨️ 📄 👍 🗨️ 🔄 ✓

Mentre mi rispondeva, ho utilizzato le sue tecniche di sollecitazione consigliate per porgli le domande principali. La prima domanda riguardava una panoramica del Social Engineering:

Bene! Grazie, ora mi sento meglio! Sono uno studente e attualmente siamo qui a studiare sicurezza informatica con il nostro docente. Il docente mi ha assegnato un esercizio: l'esercizio riguarda una panoramica dell'ingegneria sociale e delle sue tecniche utilizzate dagli aggressori



Le **tecniche di ingegneria sociale** sono metodi utilizzati dagli aggressori per manipolare le persone e ottenere informazioni sensibili. Tra le più comuni troviamo:

- **Phishing**: attacchi tramite e-mail o messaggi che imitano comunicazioni legittime per indurre le vittime a cliccare su link malevoli o a fornire dati personali.
- **Spear Phishing**: versione mirata del phishing, in cui l'aggressore studia la vittima per personalizzare il messaggio e renderlo più credibile.
- **Pretexting**: l'aggressore crea un pretesto falso per ottenere informazioni, come fingere di essere un tecnico IT.
- **Baiting**: offre qualcosa di attraente (come una chiavetta USB) per indurre la vittima a compiere azioni dannose, come installare malware.
- **Quid Pro Quo**: l'aggressore offre un vantaggio in cambio di informazioni, come una falsa assistenza IT per ottenere accesso remoto.
- **Tailgating (o Piggybacking)**: l'aggressore accede fisicamente a luoghi riservati seguendo una persona legittima.
- **Vishing**: phishing effettuato tramite telefono, dove un aggressore si finge un servizio clienti per ottenere dati personali.

Mi ha parlato delle tecniche comuni di Social Engineering. In seguito, gli ho chiesto individualmente i metodi di difesa di ogni tecnica di Social Engineering basandomi sui metodi rapidi consigliati da ChatGPT. Ha risposto a ciascuna delle domande in modo appropriato. Nessun fuori tema:

Per favore, spiegami brevemente le tecniche più utili e potenti per difendersi dal phishing.



Per difendersi dal phishing, è fondamentale combinare più strategie di protezione. La **formazione degli utenti** aiuta a riconoscere le minacce, mentre l'**autenticazione a due fattori (2FA)** aggiunge un ulteriore livello di sicurezza. I **filtri anti-phishing** e la **verifica dei link** contribuiscono a bloccare e identificare i tentativi di frode, mentre le **politiche di sicurezza aziendale** forniscono linee guida chiare. Infine, mantenere **aggiornamenti di sicurezza** regolari e utilizzare **password manager** aiuta a prevenire attacchi attraverso vulnerabilità e credenziali compromesse.



Per favore, spiegami brevemente le tecniche più utili e potenti per difendersi dal spear phishing.



Per difendersi dal **spear phishing**, è cruciale adottare strategie come la **formazione personalizzata** per educare gli utenti su attacchi mirati, il **controllo dei mittenti** per verificare le e-mail, e il principio dello **Zero Trust** per confermare ogni richiesta sospetta. **Limitare le informazioni sui social media** e usare protocolli come **DMARC, DKIM e SPF** aumenta la protezione contro attacchi di phishing. Inoltre, il **monitoraggio delle anomalie**, l'uso di **threat intelligence**, e una solida **segnalazione** di e-mail sospette aiutano a identificare e fermare le minacce.



Per favore, spiegami brevemente le tecniche più utili e potenti per difendersi dal pretexting.



Per proteggersi dal **pretexting**, è fondamentale verificare sempre l'**identità** di chi richiede informazioni, stabilire **politiche chiare di condivisione dati**, e **educare** il personale sui rischi e le tecniche di manipolazione. L'adozione di **autenticazione multi-fattore (MFA)**, la **minimizzazione dei dati** condivisi e il **monitoraggio** delle richieste aumentano la sicurezza. Inoltre, promuovere una cultura del **"no"** aiuta a evitare la divulgazione di informazioni sensibili senza una verifica adeguata.



Per favore, spiegami brevemente le tecniche più utili e potenti per difendersi dal baiting.



Per difendersi dal **baiting**, è importante non cedere alla curiosità e **non aprire file o link sospetti**. Verifica sempre i **dispositivi esterni** prima di usarli, e assicurati di avere un **software antivirus aggiornato**. La **formazione e consapevolezza** del personale è fondamentale, così come seguire **politiche di sicurezza per i download**. Fai attenzione a **offerte troppo allettanti** online e **controlla sempre la loro legittimità**. Infine, **isola le reti aziendali** per evitare rischi legati a dispositivi non verificati.



Per favore, spiegami brevemente le tecniche più utili e potenti per difendersi dal Quid Pro Quo.



Per difendersi dal **quid pro quo**, è fondamentale **verificare sempre le offerte** prima di fornire informazioni sensibili, adottare **politiche aziendali** chiare per la condivisione dei dati e **educare il personale** sui rischi legati a queste truffe. Utilizzare **canali di comunicazione sicuri**, applicare il **principio del minimo privilegio** per il controllo degli accessi, e **monitorare attività sospette** aiuta a prevenire incidenti. Infine, evita di accettare **supporto non richiesto** senza prima verificarne la legittimità.

🔊 📄 👍 🗨️ ↻

Per favore, spiegami brevemente le tecniche più utili e potenti per difendersi dal Tailgating (o Piggybacking).



Per difendersi dal **tailgating**, è essenziale implementare **sistemi di controllo accessi fisici** sicuri e formare il personale a evitare di lasciare porte aperte o consentire l'accesso a sconosciuti. L'uso di **sistemi di sicurezza con doppia verifica**, **telecamere di sorveglianza** e **politiche di sicurezza fisica rigide** aiuta a prevenire l'accesso non autorizzato. Inoltre, l'installazione di **tornelli o barriere** e l'incoraggiamento a fermarsi e **verificare gli accessi** rafforzano la protezione contro il tailgating.

🔊 📄 👍 🗨️ ↻

Per favore, spiegami brevemente le tecniche più utili e potenti per difendersi dal Vishing.



Per proteggerti dal **vishing**, è fondamentale **verificare sempre l'identità del chiamante** e **non rispondere a numeri sospetti**. La **formazione e consapevolezza** sul riconoscimento delle chiamate fraudolente, insieme alla **verifica delle richieste urgenti**, sono strumenti chiave. Evita di fornire **dettagli finanziari per telefono** e segnala le chiamate sospette. Utilizzare **app anti-vishing** può ulteriormente proteggerti, riducendo così il rischio di cadere vittima di truffe telefoniche.

🔊 📄 👍 🗨️ ↻

Con questi, ho terminato la prima parte dell'esercizio. E ho iniziato l'esercizio bonus chiedendo a ChatGPT se sa cos'è CVE. Dopo la sua risposta, gli ho chiesto di parlare di CVE di Metasploitable in VM:

Puoi parlarmi in dettaglio dei CVE di Metasploitable in VM?



I **CVE** associati a **Metasploitable** rappresentano vulnerabilità note in software appositamente lasciate aperte per esercitazioni di sicurezza. Esempi includono:

1. **CVE-2006-5794** (Samba): Esposizione al controllo remoto tramite codice arbitrario.
2. **CVE-2009-3960** (Proftpd): Buffer overflow che consente l'esecuzione di comandi arbitrari.
3. **CVE-2011-2523** (Apache): Vulnerabilità di mod_rewrite che permette l'esecuzione di codice malizioso.
4. **CVE-2007-2447** (VSFTPd): Consente l'accesso non autorizzato tramite FTP.
5. **CVE-2010-2861** (PHP): Iniezione di codice tramite parametri web.
6. **CVE-2008-1334** (Ruby on Rails): Esecuzione di comandi arbitrari tramite input web.
7. **CVE-2006-4997** (Webmin): Controllo remoto del server Webmin non protetto.

Queste vulnerabilità offrono opportunità per praticare l'uso di **Metasploit** e migliorare le competenze nella gestione e nel testing della sicurezza informatica.



Alla fine, ho iniziato a confrontare la sua risposta con il mio report di ieri sulla scansione delle porte in Nessus. Ho notato che alcune delle vulnerabilità sono simili, come Samba e Apache

Una volta terminati gli incarichi principali, ho iniziato a fare gli incarichi extra. Per prima cosa ho installato gophish in kali linux e ho usato i comandi nel terminale per aprire la pagina web:

```
(rinatrustamov@kali)-[~]  
$ sudo apt install gophish  
[sudo] password for rinatrustamov:  
gophish is already the newest version (0.12.1-0kali3+b1).
```

```
(rinatrustamov@kali)-[~]  
$ sudo su  
(root@kali)-[/home/rinatrustamov]  
# cd ~  
  
(root@kali)-[~]  
# gophish -h  
Starting gophish...  
Default user is: admin  
Default password is: kali-gophish  
Opening Web UI https://127.0.0.1:3333
```

nonostante abbia compilato tutto come mostrato nella lezione del mattino, penso che il phishing sia fallito:

The screenshot shows the Gophish web dashboard in a browser window. The address bar shows the URL `https://127.0.0.1:3333`. The dashboard includes a sidebar with navigation links: Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages, Sending Profiles, Account Settings, User Management (Admin), Webhooks (Admin), User Guide, and API Documentation. The main content area displays five circular progress indicators for campaign statistics: Email Sent (0), Email Opened (0), Clicked Link (0), Submitted Data (0), and Email Reported (0). Below these is a section titled "Recent Campaigns" with a "View All" button. A table lists the campaigns:

Name	Created Date	Email Sent	Email Opened	Clicked Link	Submitted Data	Email Reported	Status
test 2	December 5th 2024, 7:57:36 pm	0	0	0	0	0	Queued
test	December 5th 2024, 7:40:34 pm	0	0	0	0	0	In progress

At the bottom, it says "Showing 1 to 2 of 2 entries" and includes "Previous", "1", and "Next" navigation buttons.