

S5L4

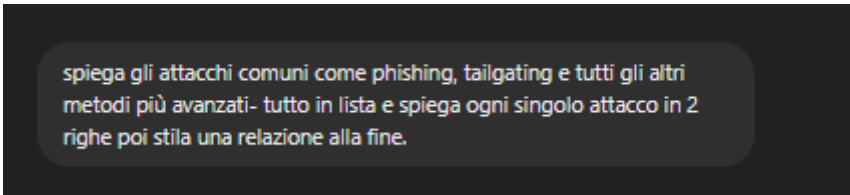
Social Engineering e Tecniche di Difesa Obiettivo:

Esplorare le tecniche di social engineering e imparare come difendersi da questi tipi di attacchi. Questo esercizio vi guiderà attraverso la comprensione delle varie forme di social engineering, esempi reali di attacchi e strategie di difesa efficaci.

Descrizione dell'attività:

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.

Abbiamo fatto il primo prompt con:



spiega gli attacchi comuni come phishing, tailgating e tutti gli altri metodi più avanzati- tutto in lista e spiega ogni singolo attacco in 2 righe poi stila una relazione alla fine.

E il risultato è questo:

Elenco dei principali attacchi di social engineering e cyber security

1. **Phishing:** Truffa online che utilizza email, messaggi o siti web falsi per ingannare gli utenti, spingendoli a fornire informazioni personali o credenziali di accesso.
2. **Spear Phishing:** Variante mirata del phishing che prende di mira una persona specifica, utilizzando informazioni personalizzate per rendere il messaggio più credibile.
3. **Vishing (Voice Phishing):** Phishing telefonico in cui gli attaccanti chiamano la vittima fingendosi figure di autorità per ottenere dati sensibili o accesso a sistemi.
4. **Smishing (SMS Phishing):** Versione del phishing tramite SMS o messaggistica istantanea, in cui l'attaccante invia un messaggio ingannevole per ottenere dati sensibili.
5. **Tailgating (o Piggybacking):** Tecnica fisica in cui un intruso segue una persona autorizzata per accedere ad aree riservate, spesso approfittando della fiducia o della distrazione.
6. **Pretexting:** Metodo che implica la creazione di un pretesto fittizio per ingannare la vittima e convincerla a condividere informazioni riservate.
7. **Baiting:** Uso di un'esca (come un'unità USB compromessa) per attirare la vittima e indurla a collegarla al proprio dispositivo, infettandolo con malware.
8. **Quid Pro Quo:** Attacco in cui l'hacker offre un servizio o un favore in cambio di informazioni, sfruttando il desiderio di ottenere un beneficio.
9. **Man-in-the-Middle (MitM):** Intercettazione delle comunicazioni tra due parti senza che esse lo sappiano, permettendo all'attaccante di rubare dati o modificarli.
10. **Watering Hole:** Attacco che compromette siti web frequenti delle vittime, infettandoli con malware per colpire obiettivi specifici.
11. **Whaling:** Variante del phishing mirata ai dirigenti di alto livello per accedere a informazioni aziendali cruciali.
12. **Shoulder Surfing:** Osservazione diretta di schermi o dispositivi, di solito in ambienti pubblici, per ottenere password o informazioni sensibili.
13. **Pharming:** Tecnica che manipola i DNS per reindirizzare gli utenti verso siti fraudolenti, anche inserendo l'URL corretto.
14. **Denial of Service (DoS):** Sovraccarico di un sistema o rete per renderlo inaccessibile agli utenti legittimi, spesso con lo scopo di interrompere le operazioni.
15. **Brute Force Attack:** Tentativo sistematico di scoprire una password provando tutte le possibili combinazioni finché non si trova quella corretta.

ed infine con il Secondo prompt:

Definisci strategie e migliori pratiche per difendersi dagli attacchi di social engineering suddividili per categoria e prendi in considerazione questi nella lista. prendi nota delle tecniche di difesa per ogni metodo e consiglia come fare in 2 righe

Con questo ultimo risultato:

1. Difese contro Attacchi di Social Engineering Psicologici

- **Phishing, Spear Phishing, Vishing, Smishing:** Utilizzare soluzioni anti-phishing, evitare di aprire link sospetti e confermare sempre la provenienza di messaggi e chiamate.
- **Pretexting:** Verificare sempre l'identità di chi richiede informazioni, anche se sembra provenire da fonti fidate.
- **Baiting:** Non inserire dispositivi esterni (USB, CD) di origine sconosciuta e istruire il personale sui rischi.
- **Quid Pro Quo:** Diffidare di richieste che offrono benefici in cambio di dati e usare formazione sulla sicurezza.
- **Whaling:** Implementare protocolli di verifica multi-fattore per i dirigenti e formare il personale dirigenziale sui rischi.
- **Shoulder Surfing:** Utilizzare protezioni visive per schermi e prestare attenzione a chi può osservare in ambienti pubblici.

2. Difese contro Attacchi Fisici di Accesso Non Autorizzato

- **Tailgating (Piggybacking):** Installare badge di accesso individuali, sensibilizzare sull'importanza di non far accedere sconosciuti.
- **Shoulder Surfing:** Usare schermi di protezione per impedire la visione laterale in uffici e spazi pubblici.

3. Difese contro Attacchi Tecnici di Manipolazione delle Comunicazioni

- **Man-in-the-Middle (MitM):** Utilizzare connessioni criptate e VPN; evitare di utilizzare reti pubbliche non protette per attività sensibili.
- **Watering Hole:** Mantenere sempre aggiornati i sistemi di sicurezza e limitare l'accesso solo a siti sicuri.
- **Pharming:** Utilizzare DNS sicuri e impostare sistemi di allerta in caso di modifiche sospette.

4. Difese contro Attacchi di Disruptive Force

- **Denial of Service (DoS):** Utilizzare firewall e sistemi di protezione da attacchi DoS; implementare filtri IP per bloccare il traffico malevolo.
- **Brute Force Attack:** Abilitare l'autenticazione a più fattori (MFA) e limitare i tentativi di accesso falliti.

Conclusione

Gli attacchi di social engineering si dividono in quattro categorie principali: attacchi psicologici, attacchi fisici di accesso non autorizzato, attacchi di manipolazione delle comunicazioni e attacchi di forza "distruttiva". Ciascuna categoria sfrutta differenti debolezze negli utenti o nei sistemi, richiedendo strategie di difesa e prevention mirate. Gli attacchi psicologici – come phishing, spear phishing, vishing e smishing – puntano a ingannare l'utente per ottenere informazioni. La difesa ideale è mantenere elevata la consapevolezza degli utenti e adottare soluzioni di verifica multi-fattore. Anche il pretexting e il baiting rientrano in questa categoria e si prevengono tramite la sensibilizzazione del personale a non fornire dati a chiunque si presenti con pretesti sospetti o promesse di vantaggi.

Negli attacchi fisici di accesso non autorizzato, come il tailgating e lo shoulder surfing, un intruso accede a spazi riservati o osserva dati da schermi visibili. La migliore difesa è l'adozione di badge individuali e protezioni per schermi, insieme a una maggiore consapevolezza del personale sul non consentire accessi non verificati.

Gli attacchi di manipolazione delle comunicazioni, tra cui man-in-the-middle (MitM) e watering hole, mirano a intercettare o reindirizzare il traffico. Qui, l'uso di VPN, connessioni criptate e accesso a siti verificati e sicuri rappresenta una difesa efficace. Anche il pharming, che dirotta gli utenti su siti falsi, richiede sistemi di DNS sicuri e strumenti di rilevamento per intervenire tempestivamente.

Infine, per contrastare gli attacchi di forza distruttiva come il denial of service (DoS) e i brute force attack, che tentano di sovraccaricare il sistema o violarlo, sono essenziali firewall, MFA e limiti sui tentativi di accesso. La combinazione di protezioni tecniche avanzate e un'attenta gestione delle credenziali minimizza questi rischi.

In sintesi, una difesa completa richiede una strategia che unisce tecnologie di protezione avanzate, formazione continua e protocolli rigorosi per un approccio integrato e sempre aggiornato contro le minacce informatiche.

EXTRA

Obiettivo: L'obiettivo di questo esercizio è imparare a utilizzare ChatGPT per raccogliere informazioni sui CVE (Common Vulnerabilities and Exposures). Questo esercizio vi guiderà attraverso il processo di formulazione di una richiesta (prompt) efficace per ottenere una lista di CVE e informazioni dettagliate su ciascuno di essi. **Descrizione dell'attività:** 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.

Primo prompt:

Elencami i principali CVE (Common Vulnerabilities and Exposures) rilevanti per Windows 11, spiegando per ciascuno la natura della vulnerabilità, l'impatto sul sistema, e le possibili azioni correttive. Indica anche se è stato rilasciato un aggiornamento o una patch per risolvere il problema. elencami quelle più gravi e fai una lista di 10 utilizzabili oggi

Risultato:

Ecco una lista delle principali vulnerabilità critiche (CVE) attualmente rilevanti per Windows 11, insieme alla loro descrizione e le azioni correttive consigliate:

- CVE-2024-43583 (Winlogon Elevation of Privilege):** Esploita il processo di accesso tramite editor di metodo di input (IME) non Microsoft, permettendo a un attaccante di ottenere privilegi di sistema. La patch di ottobre 2024 ha disabilitato gli IME di terze parti durante l'accesso. Rimuovere gli IME di terze parti è consigliato come ulteriore misura di sicurezza.
- CVE-2024-20659 (Hyper-V Container Escape):** Consente a un attaccante di compromettere il kernel dell'hypervisor su hypervisor UEFI-specifici. È disponibile una patch, ma è raccomandato anche il controllo delle configurazioni Hyper-V per minimizzare i rischi.
- CVE-2024-43573 (MSHTML XSS):** Vulnerabilità di spoofing in MSHTML, esposta in exploit in-the-wild, che consente cross-site scripting. Microsoft raccomanda di aggiornare a un rollup mensile per includere la correzione, specialmente per Windows Server.
- CVE-2024-6197 (cURL Remote Code Execution):** Permette l'esecuzione di codice dannoso attraverso cURL, quando un utente si connette a un server malevolo. Microsoft ha rilasciato una patch, e si consiglia di limitare l'uso di cURL o aggiornare tempestivamente.
- CVE-2024-43572 (Management Console RCE):** Attacco RCE che sfrutta file MSC creati appositamente. Una patch disabilita i file MSC non attendibili per prevenire l'esecuzione non autorizzata.
- CVE-2024-63582 (Win32k Privilege Escalation):** Permette l'elevazione di privilegi attraverso exploit noti per l'interfaccia Win32k. Microsoft ha rilasciato una patch, consigliando una rapida applicazione dell'aggiornamento per evitare l'accesso non autorizzato a livello di sistema.
- CVE-2024-5066 (Graphics Component Privilege Escalation):** Colpisce il componente grafico di Windows, consentendo l'elevazione di privilegi. Una patch è stata distribuita e Microsoft consiglia di mantenere aggiornato il sistema.
- CVE-2024-30947 (Windows Networking Stack):** Consente attacchi di denial of service tramite la pila di rete. Applicare la patch di sicurezza e utilizzare firewall per limitare accessi non necessari.
- CVE-2024-54698 (Remote Desktop Protocol RCE):** Un exploit nel protocollo RDP permette l'esecuzione di codice. La patch è stata rilasciata, e disabilitare RDP non necessario è un'ulteriore misura preventiva.
- CVE-2024-74723 (Print Spooler Elevation of Privilege):** Colpisce il Print Spooler di Windows per elevare privilegi. Microsoft ha distribuito una patch, e si consiglia di disabilitare il servizio Print Spooler se non essenziale.

Relazione WIN 11 (oct 31)

Iniziamo con la CVE-2024-43583, che può permettere a un malintenzionato di guadagnare privilegi elevati usando strumenti di input non certificati. Microsoft, ha rilasciato una patch che disabilita questi strumenti. È raccomandato di non utilizzare se non costretti software di terze parti non verificati.

invece la CVE-2024-20659, che colpisce l'hypervisor Hyper-V, consentendo potenzialmente a un attaccante di entrare nel sistema. Anche qui, l'aggiornamento è fondamentale. È consigliato anche limitare l'accesso ad hyperV

Un'altra vulnerabilità da tenere d'occhio è la CVE-2024-43573. rendendo possibile un attacco di cross-site scripting (XSS). aggiornamento anche qui obbligatorio.

Passando alla CVE-2024-6197, questa vulnerabilità sfrutta cURL per eseguire codice dannoso. È meglio essere cauti e assicurarti di utilizzare sempre la versione più recente di cURL. evitare di connettersi a server sconosciuti può mitigare la cosa
la CVE-2024-43572, che consente l'esecuzione di codice malevolo attraverso file MSC. La patch disabilita l'uso di file non affidabili, non aprire mai file da fonti dubbie.

La CVE-2024-63582 è una minaccia per l'interfaccia Win32k, e può portare a una grave elevazione dei privilegi. Oltre a installare la patch, è meglio tenere d'occhio gli account utente e assicurarsi che non abbiano più privilegi di quelli necessari.

Con la CVE-2024-30947, puoi affrontare attacchi di denial of service. Qui, la soluzione è impostare un firewall robusto e monitorare attentamente il traffico di rete.

Poi c'è la CVE-2024-54698, che riguarda il protocollo RDP. si può disabilitare ma se va usato, implementare l'autenticazione a più fattori per aggiungere un ulteriore strato di sicurezza (2FA o Multy)

Infine, la CVE-2024-74723 è legata al servizio Print Spooler. Disabilitare il servizio se non è necessario e applicare subito le patch. è una buona soluzione.

In sintesi rimanere al sicuro su Windows 11 richiede una combinazione di aggiornamenti regolari, configurazioni di sicurezza rigorose e un po' di buon senso. È fondamentale essere proattivi e Mantenere il sistema aggiornato è solo l'inizio; educare gli utenti e adottare buone pratiche quotidiane può fare la differenza tra una sicurezza robusta e un disastro informatico. Quindi, controllare sempre le patch, fare attenzione a cosa si scarica e rimanere vigili. La sicurezza informatica è una responsabilità condivisa.