

Consegna S5L4

Domande a chatGPT

Domanda 1

1. Comprendere il Social Engineering:

- Formulate un prompt per ChatGPT per ottenere una panoramica del social engineering e delle tecniche utilizzate dagli attaccanti.

modello GPT 4

Prompt:

Potresti spiegare cos'è l'ingegneria sociale e descrivere le tecniche più comuni utilizzate dagli attaccanti, come il phishing e il tailgating? Include una descrizione dettagliata di come queste tecniche vengono impiegate per manipolare o ingannare le persone al fine di ottenere accesso non autorizzato a informazioni riservate. Aggiungi esempi specifici di attacchi di ingegneria sociale che illustrano queste tecniche in azione.

Risposta:

Ingegneria Sociale

L'ingegneria sociale è una tecnica di manipolazione che mira a indurre le persone a compiere azioni specifiche o a divulgare informazioni riservate. Si basa sulla psicologia umana piuttosto che su attacchi tecnici per violare la sicurezza. Gli attaccanti utilizzano l'ingegneria sociale perché spesso è più semplice sfruttare la naturale inclinazione umana all'errore piuttosto che superare misure di sicurezza tecnologiche avanzate.

Tecniche Comuni

1. Phishing

- **Descrizione:** Il phishing è una delle tecniche più note di ingegneria sociale, che consiste nell'invio di email fraudolente che sembrano provenire da fonti legittime. L'obiettivo è indurre le vittime a fornire dati sensibili, come credenziali di accesso o informazioni finanziarie.
- **Esempio:** Un attacco di phishing potrebbe coinvolgere un'email che sembra provenire da una banca nota, con un link che porta a una pagina web contraffatta simile alla vera pagina di login della banca. L'utente, pensando che la richiesta sia legittima, inserisce le proprie credenziali, che vengono rubate dall'attaccante.

2. Tailgating

- **Descrizione:** Il tailgating, noto anche come "piggybacking", implica l'accesso non autorizzato a edifici o altre aree sicure seguendo da vicino una persona autorizzata senza che questa si accorga di essere seguita.
- **Esempio:** Un attaccante potrebbe fingere di essere un corriere e attendere che un dipendente apra la porta di un'area sicura di un'azienda. L'attaccante poi entra rapidamente dietro di loro, guadagnando accesso senza essere notato.

3. Pretexting

- **Descrizione:** Il pretexting è una forma di ingegneria sociale in cui un attaccante inventa uno scenario (pretesto) per ingannare la vittima e indurla a rivelare informazioni riservate. Questo spesso richiede una preparazione significativa e la creazione di una storia credibile.
- **Esempio:** L'attaccante potrebbe contattare la vittima fingendosi un funzionario dell'IRS che richiede informazioni personali per "verificare l'identità" della vittima nell'ambito di una revisione fiscale.

4. Baiting

- **Descrizione:** Il baiting simile al phishing, ma con l'aggiunta di un incentivo. L'attaccante "esca" la vittima offrendo qualcosa di desiderabile per indurla a compiere un'azione che comprometterà la sua sicurezza.
- **Esempio:** Distribuzione di dispositivi USB infetti etichettati come contenenti software o film importanti in luoghi strategici, come un parcheggio aziendale. La curiosità spinge le vittime a inserire l'USB nei loro computer, installando così malware.

5. Quid Pro Quo

- **Descrizione:** Una tecnica in cui l'attaccante promette un beneficio in cambio di informazioni. Questo può includere l'offerta di assistenza tecnica in cambio di password o altre credenziali.
- **Esempio:** Un attaccante potrebbe chiamare utenti casuali come tecnico IT e offrire un "controllo di sicurezza gratuito", durante il quale chiede le credenziali dell'utente per "verificare" le impostazioni del loro account.

Impatto dell'Ingegneria Sociale

L'ingegneria sociale può avere conseguenze devastanti, consentendo agli attaccanti di ottenere accesso non solo a informazioni personali, ma anche a reti aziendali protette, spesso facendo leva su un singolo punto di fallimento: il fattore umano.

Per difendersi efficacemente dall'ingegneria sociale, è fondamentale educare continuamente gli utenti sui rischi e su come riconoscere gli attacchi. Le strategie di difesa includono la formazione degli utenti, l'implementazione di politiche di sicurezza stringenti e la verifica regolare dei sistemi di sicurezza.

Domanda 2

Strategie di Difesa:

- Chiedete a ChatGPT di suggerire strategie e migliori pratiche per difendersi dagli attacchi di social engineering. Prendete nota delle tecniche di difesa più efficaci.

modello GPT4

Prompt:

Potresti elencare e spiegare dettagliatamente alcune strategie efficaci per difendersi dagli attacchi di ingegneria sociale? Include metodi per identificare e prevenire comuni tecniche come il phishing, il tailgating, e il pretexting. Fornisci anche consigli pratici su come le organizzazioni e gli individui possono rafforzare la loro sicurezza contro questi tipi di attacchi. Aggiungi specifiche politiche o procedure di sicurezza che le organizzazioni dovrebbero implementare, esempi di come le aziende hanno efficacemente contrastato attacchi di ingegneria sociale, e informazioni su strumenti o tecnologie che possono aiutare a rilevare tentativi di ingegneria sociale.

Risposta:

Strategie Efficaci per Difendersi dagli Attacchi di Ingegneria Sociale

1. Educazione e Formazione Continua

- **Formazione dei dipendenti:** Organizzare sessioni regolari per insegnare ai dipendenti a riconoscere i tentativi di phishing, pretexting e tailgating. Utilizzare esempi reali e simulazioni di attacchi per migliorare la loro capacità di identificarli.
- **Aggiornamenti regolari:** Mantenere i dipendenti aggiornati sulle nuove tecniche di ingegneria sociale e su come evitarle.

2. Politiche di Sicurezza Stringenti

- **Autenticazione multifattoriale (MFA):** Implementare MFA per aggiungere un ulteriore livello di sicurezza oltre la password.
- **Politiche di controllo dell'accesso:** Limitare l'accesso fisico e digitale ai dati sensibili solo al personale autorizzato.
- **Verifica delle identità:** Adottare procedure per verificare l'identità di individui che richiedono accesso a informazioni o aree protette, sia internamente che esternamente (es. chiamate di servizio, richieste via email).

3. Strumenti e Tecnologie

- **Software anti-phishing:** Utilizzare strumenti che rilevano e bloccano email sospette, link dannosi e tentativi di phishing.
- **Monitoraggio della sicurezza:** Impiegare soluzioni di monitoraggio continuo per rilevare comportamenti insoliti che potrebbero indicare un tentativo di ingegneria sociale.

4. Politiche di Verifica e Risposta

- **Procedure di risposta agli incidenti:** Avere un piano chiaro su come rispondere a un attacco di ingegneria sociale può ridurre il danno e migliorare il tempo di ripresa.
- **Audit di sicurezza regolari:** Eseguire audit di sicurezza per valutare e migliorare le pratiche di sicurezza correnti.

5. Misure Fisiche

- **Sistemi di controllo accessi:** Installare sistemi di sicurezza per controllare l'accesso fisico agli edifici.
- **Segnaletica e formazione sul tailgating:** Insegnare ai dipendenti a essere cauti quando qualcuno cerca di seguire qualcun altro attraverso una porta controllata senza le credenziali appropriate.

Esempi Pratici

- **Google e l'uso di chiavi di sicurezza hardware per MFA:** Google ha notevolmente ridotto il successo degli attacchi di phishing contro i suoi dipendenti implementando l'uso obbligatorio di chiavi di sicurezza hardware per l'autenticazione.
- **IBM e le simulazioni di phishing:** IBM conduce regolarmente test di phishing simulato e utilizza i risultati per formare meglio i suoi dipendenti a riconoscere e segnalare tentativi di phishing.

Considerazioni Finali

L'efficacia nella difesa dagli attacchi di ingegneria sociale si basa sull'essere proattivi e sul mantenimento di un approccio di sicurezza multilivello che comprende tanto la tecnologia quanto la formazione umana. Le organizzazioni devono adottare un approccio olistico, aggiornando continuamente le proprie politiche e formazione per fronteggiare le evoluzioni nelle tecniche di attacco.

Domanda 3

Esplorazione dei CVE tramite ChatGPT

Formulazione del prompt:

- Scrivete un prompt per ChatGPT che chieda di elencare i CVE relativi al software o sistema operativo scelto.

modello GPT 4o

Prompt:

Trova e fornisci una lista delle CVE più recenti relative a Cisco Webex con un livello di gravità elevato. Per ciascuna vulnerabilità, includi:

Una descrizione dettagliata della vulnerabilità.

Le possibili conseguenze se sfruttata.

Le soluzioni consigliate, con passaggi dettagliati per implementarle su sistemi Windows.

Riferimenti ufficiali o documentazione Cisco pertinenti per ogni CVE.

Assicurati che le istruzioni siano precise, dettagliate e adattate per essere seguite da un amministratore che utilizza una piattaforma Windows.

Risposta

Vulnerabilità Recenti Relative a Cisco Webex con Grado di

Gravità Elevato

CVE-2024-20395: Vulnerabilità di Esposizione del Token di Sessione nell'App Cisco Webex

- **Descrizione:**

Una vulnerabilità nella funzionalità di recupero dei media dell'app Cisco Webex potrebbe consentire a un attaccante non autenticato e adiacente di accedere a informazioni sensibili della sessione.

[Cisco Security Advisory](#)

- **Possibili Conseguenze:**

Se sfruttata, questa vulnerabilità potrebbe permettere a un attaccante di ottenere token di sessione, potenzialmente consentendo l'accesso non autorizzato a riunioni o dati associati.

- **Soluzioni Consigliate:**

1. **Aggiornamento dell'App Webex:**

Assicurarsi di utilizzare l'ultima versione dell'app Cisco Webex, poiché Cisco ha rilasciato aggiornamenti che risolvono questa vulnerabilità.

2. **Verifica della Versione:**

- Su Windows, aprire l'app Webex.
- Cliccare sull'icona del profilo in alto a destra.
- Selezionare "Informazioni su" per visualizzare la versione corrente.

3. **Procedura di Aggiornamento:**

- Visitare il sito ufficiale di Cisco Webex.
- Navigare alla sezione Download.
- Scaricare e installare l'ultima versione compatibile con Windows.

- **Riferimenti Ufficiali:**

[Cisco Security Advisory: cisco-sa-webex-app-ZjNm8X8j](#)

CVE-2024-20396: Vulnerabilità nei Gestori di Protocollo dell'App Cisco Webex

- **Descrizione:**

Una vulnerabilità nei gestori di protocollo dell'app Cisco Webex potrebbe consentire a un attaccante non autenticato e remoto di accedere a informazioni sensibili.

[GitHub Advisory](#)

- **Possibili Conseguenze:**

Sfruttando questa vulnerabilità, un attaccante potrebbe indurre l'app a inviare richieste che, se intercettate, potrebbero rivelare informazioni sensibili, inclusi dati di credenziali.

- **Soluzioni Consigliate:**

1. Aggiornamento dell'App Webex:

Installare l'ultima versione dell'app Cisco Webex che contiene le patch per questa vulnerabilità.

2. Evitare Link Sospetti:

Non cliccare su link non verificati o sospetti che potrebbero sfruttare questa vulnerabilità.

3. Monitoraggio del Traffico di Rete:

Implementare strumenti di monitoraggio per rilevare attività anomale o non autorizzate.

- **Riferimenti Ufficiali:**

[GitHub Advisory: GHSA-67ww-939x-f5pp](#)

CVE-2023-20132: Vulnerabilità di Cross-Site Scripting (XSS) Memorizzato in Cisco Webex Meetings

- **Descrizione:**

Una vulnerabilità nell'interfaccia web di Cisco Webex Meetings potrebbe permettere a un attaccante autenticato e remoto di condurre un attacco XSS memorizzato contro un utente dell'interfaccia.

[Cisco Security Advisory](#)

- **Possibili Conseguenze:**

Un attaccante potrebbe eseguire script arbitrari nel contesto dell'interfaccia web, portando al furto di cookie, credenziali o altre informazioni sensibili.

- **Soluzioni Consigliate:**

1. Aggiornamento del Software:

- Per Webex Meetings: Assicurarsi che il sito Webex sia aggiornato alla versione più recente, poiché gli aggiornamenti vengono applicati automaticamente per i servizi cloud.
- Per Webex Meetings Server (on-premises):
 - Accedere al portale di amministrazione del server.
 - Verificare la disponibilità di aggiornamenti e applicarli secondo le linee guida di Cisco.

2. Validazione dell'Input:

Implementare controlli per garantire che l'input dell'utente sia adeguatamente validato e sanificato.

3. Formazione degli Utenti:

Educare gli utenti a riconoscere e segnalare comportamenti sospetti o link non sicuri.

- **Riferimenti Ufficiali:**

[Cisco Security Advisory: cisco-sa-wbx-sxss-fupl-64uHbcm5](#)

CVE-2023-20180: Vulnerabilità di Cross-Site Request Forgery (CSRF) in Cisco Webex Meetings

- **Descrizione:**

Una vulnerabilità nell'interfaccia web di Cisco Webex Meetings potrebbe consentire a un attaccante

non autenticato e remoto di condurre un attacco CSRF su un sistema vulnerabile.

[GitHub Advisory](#)

- **Possibili Conseguenze:**

Un attaccante potrebbe indurre un utente a eseguire azioni indesiderate, come unirsi a riunioni o programmare sessioni, senza il suo consenso.

- **Soluzioni Consigliate:**

1. **Aggiornamento del Software:**

Assicurarsi che tutti i sistemi e le interfacce Webex siano aggiornati.

2. **Utilizzo di Token Anti-CSRF:**

Implementare token di verifica per tutte le richieste sensibili.

3. **Educazione degli Utenti:**

Educare gli utenti a non cliccare su link sconosciuti o sospetti.

- **Riferimenti Ufficiali:**

[GitHub Advisory: GHSA-q3fh-c732-57w2](#)