

Esercitazione S5L4

In questa esercitazione vado a sfruttare l'intelligenza artificiale (in questo caso chatgpt) per svolgere un'indagine riguardo gli attacchi social engineering, cercando di farmi dare risposte accurate e dettagliate.

Ho eseguito due richieste (prompt) diverse: la prima è rivolta a una richiesta di spiegazione generale riguardo gli attacchi social engineering, qual è l'obiettivo di questi attacchi e un elenco di metodi comuni utilizzati, la seconda invece è una richiesta su come ci si può difendere da questo tipo di attacchi.

Prompt 1:

Spiegami in maniera dettagliata cosa sono gli attacchi social engineering ed elencami le modalità più comuni utilizzate da un attaccante

Risposta:

Gli **attacchi di social engineering** sono tecniche di manipolazione psicologica utilizzate dagli attaccanti per indurre le persone a rivelare informazioni confidenziali o a compiere azioni che compromettano la sicurezza di un sistema o di un'organizzazione. Invece di sfruttare vulnerabilità tecniche, il social engineering sfrutta la tendenza umana a fidarsi e a commettere errori. Gli attaccanti mirano a ingannare le vittime facendo leva su curiosità, paura, urgenza o confusione.

Ecco le modalità più comuni utilizzate negli attacchi di social engineering:

1. Phishing

Il phishing è uno degli attacchi più diffusi e consiste nell'invio di messaggi fraudolenti (solitamente via email) che sembrano provenire da fonti affidabili, come banche, servizi online o aziende conosciute. Gli utenti vengono indotti a cliccare su link o a scaricare allegati dannosi, oppure a fornire dati personali come credenziali di accesso e informazioni bancarie.

2. Spear Phishing

Una variante del phishing, il **spear phishing** è un attacco mirato a una specifica persona o gruppo, spesso all'interno di un'organizzazione. L'attaccante personalizza il messaggio per sembrare autentico e rilevante per il destinatario, aumentando le probabilità di successo. Questi attacchi sono spesso sofisticati e possono includere dettagli specifici sulla vittima, come il nome, la posizione lavorativa o interessi personali.

3. Vishing (Voice Phishing)

Il **vishing** consiste nel fare chiamate telefoniche fraudolente per raccogliere informazioni personali o sensibili. L'attaccante può fingere di essere un rappresentante di un ente governativo, di una banca o di un'azienda, cercando di ottenere informazioni sensibili come password, numeri di conto o dettagli di carte di credito.

4. Smishing (SMS Phishing)

Lo **smishing** è simile al phishing, ma avviene tramite messaggi di testo (SMS). Gli attaccanti inviano messaggi che contengono link a siti malevoli o istruzioni per compiere azioni rischiose,

come rispondere con informazioni riservate. I messaggi di smishing sono spesso progettati per suscitare una reazione rapida, come "Il tuo conto è stato sospeso, clicca qui per riattivarlo."

5. Pretexting

Nel **pretexting**, l'attaccante crea una falsa identità o "pretesto" per ottenere informazioni dalla vittima. L'attaccante può fingersi una persona autorizzata, come un collega, un responsabile IT o un fornitore di servizi, e fare richieste che potrebbero sembrare legittime per raccogliere dati personali o aziendali.

6. Baiting

Il **baiting** sfrutta la curiosità delle persone, proponendo qualcosa di allettante o interessante in cambio di informazioni. Questo tipo di attacco può includere anche la distribuzione di dispositivi infetti (come chiavette USB o CD) lasciati in luoghi pubblici. Se la vittima trova e collega il dispositivo, il malware si installa automaticamente nel sistema.

7. Quid Pro Quo

Con un attacco **quid pro quo**, l'attaccante promette qualcosa in cambio di informazioni o accesso. Ad esempio, può fingersi un tecnico informatico che offre supporto e, una volta ottenuto l'accesso, installare software dannosi o raccogliere informazioni sensibili.

8. Tailgating o Piggybacking

Questo tipo di attacco avviene di persona, in cui l'attaccante si infila in un'area riservata "accodandosi" a una persona autorizzata. Spesso si tratta di un dipendente ignaro che permette inconsapevolmente l'accesso, per esempio, tenendo aperta una porta per una persona senza badge di accesso.

9. Shoulder Surfing

Il **shoulder surfing** è un attacco in cui l'attaccante osserva direttamente la vittima per carpire informazioni sensibili. Questo può accadere in luoghi pubblici, dove l'attaccante osserva di nascosto mentre la vittima digita una password o altri dati riservati.

10. Impersonation (Impersonificazione)

Questo tipo di attacco implica che l'attaccante si presenti come una persona di fiducia, ad esempio un dirigente o un collega. Con questo metodo, cerca di ottenere informazioni riservate o di influenzare comportamenti interni all'azienda.

Prompt 2:

Elencami in modo accurato le modalità di difesa più utili per difendersi da un attacco social engineering

Risposta:

Per difendersi dagli attacchi di social engineering, è fondamentale adottare un approccio che combini educazione, tecnologie di sicurezza e pratiche rigorose. Ecco le modalità di difesa più utili e pratiche:

1. Formazione e Sensibilizzazione del Personale

- **Addestramenti regolari:** Formare regolarmente i dipendenti sui rischi del social engineering, mostrando esempi di attacchi comuni come phishing, vishing e pretexting.
- **Simulazioni di attacco:** Effettuare simulazioni di phishing e altri test per aiutare i dipendenti a riconoscere tentativi di manipolazione in un ambiente controllato.
- **Aggiornamenti periodici:** Informare il personale sulle nuove tattiche di social engineering in modo che possano riconoscere e segnalare attività sospette.

2. Autenticazione Multifattore (MFA)

- **Protezione aggiuntiva per l'accesso:** Utilizzare l'autenticazione multifattore per proteggere l'accesso ai sistemi critici. Anche se un attaccante ottiene le credenziali di accesso, non può accedere ai sistemi senza il secondo fattore (come un codice inviato via SMS o generato da un'app).
- **Protezione specifica per i ruoli sensibili:** Implementare MFA per account con privilegi elevati e dati sensibili, riducendo il rischio di accesso non autorizzato.

3. Procedure di Verifica per le Richieste di Informazioni

- **Doppia verifica per richieste insolite:** Quando qualcuno richiede informazioni sensibili o azioni fuori dall'ordinario (per esempio, tramite email o telefono), richiedere un secondo metodo di verifica, come chiamare la persona richiedente tramite il numero ufficiale dell'azienda.
- **Politica del "Controllo diretto":** Non accettare mai richieste di cambiamento di dati finanziari o di accesso tramite mezzi non ufficiali (es. email non verificate).

4. Politiche Rigorose di Accesso ai Dati e alle Informazioni

- **Limitazione dei privilegi:** Assegnare accesso ai dati solo a chi ne ha bisogno per il proprio ruolo e revocare l'accesso non più necessario.
- **Tracciamento e logging:** Monitorare gli accessi ai sistemi e conservare i log per rilevare eventuali attività sospette o non autorizzate.

5. Controlli di Accesso Fisico e Sicurezza delle Strutture

- **Badge e accessi protetti:** Utilizzare badge di identificazione, tornelli, e sistemi biometrici per limitare l'accesso fisico ai locali riservati solo al personale autorizzato.
- **Policy di sicurezza per ospiti e visitatori:** Assicurarsi che ogni visitatore sia accompagnato e controllato, con badge temporanei o ospite.

6. Tecnologie di Sicurezza Anti-Phishing

- **Filtri anti-phishing per le email:** Implementare filtri di posta elettronica avanzati per rilevare e bloccare le email di phishing o con allegati dannosi.
- **Browser con protezioni integrate:** Usare software di navigazione web che includa strumenti di rilevamento di siti pericolosi o ingannevoli.

7. Politiche di Gestione delle Password

- **Password robuste e uniche:** Richiedere password complesse e non riutilizzabili tra diversi sistemi.
- **Uso di un password manager:** Consigliare (o fornire) l'uso di un gestore di password sicuro per ridurre il rischio di furti di credenziali e migliorare la gestione delle password.

8. Processi e Procedure di Segnalazione delle Attività Sospette

- **Canali di segnalazione dedicati:** Creare un sistema facile e rapido per la segnalazione di attività sospette da parte dei dipendenti, con risposta tempestiva da parte del reparto sicurezza.
- **Feedback e aggiornamenti:** Fornire feedback a chi segnala incidenti per incoraggiare la proattività e aumentare la consapevolezza.

9. Protezione dei Dispositivi e delle Reti

- **Aggiornamenti e patch regolari:** Assicurarsi che i sistemi operativi e il software utilizzato siano aggiornati per prevenire l'uso di vulnerabilità conosciute.
- **Uso della VPN per accessi remoti:** Utilizzare VPN sicure per crittografare le connessioni esterne, proteggendo il traffico dati da intercettazioni.

10. Educazione alla Privacy e alla Riservatezza dei Dati Personali

- **Consapevolezza della condivisione dei dati:** Incoraggiare il personale a essere consapevole dei dati personali che condivide e a evitare di dare informazioni sensibili su piattaforme pubbliche o social media.
- **Dispositivi di protezione fisica:** Usare schermature per laptop in luoghi pubblici e pratiche di "desk clean" per evitare che informazioni sensibili siano visibili a persone non autorizzate.

Sintesi

L'adozione combinata di queste misure rende molto più difficile per un attaccante sfruttare errori umani. La sicurezza contro il social engineering richiede un impegno costante e un aggiornamento delle difese, adattandosi all'evoluzione delle minacce e delle tattiche utilizzate dagli attaccanti.