**Descrizione traccia per il compito**

La traccia del compito da svolgere richiedeva di fornire prompt per chatgpt che ci permettessero di avere una panoramica sull’ingegneria sociale, che ci fornisse informazioni dettagliate sulle varie tecniche più comuni e sui metodi di difesa più efficaci a riguardo.

Sulla base della mia ricerca ho sviluppato la seguente relazione

**Relazione sul Social Engineering**

Il social engineering è una tecnica utilizzata da attaccanti per manipolare le persone affinché rivelino informazioni riservate o compiano azioni che compromettono la sicurezza. Invece di sfruttare vulnerabilità tecniche, si basa sulla psicologia umana.

Tra le tecniche più comuni ci sono:

**1. Phishing**

* **Descrizione**: Si inviano email o messaggi ingannevoli che sembrano provenire da fonti affidabili, chiedendo di fornire informazioni personali o cliccare su link malevoli.
* **Dettagli**: Il sito web è una replica esatta del sito legittimo, progettato per raccogliere nome utente e password. Una volta ottenute, l'attaccante può accedere ai conti della vittima
* **Obiettivo**: Rubare credenziali, dati bancari o installare malware.

**2. Pretexting**

* **Descrizione**: Il truffatore crea una falsa identità o scenario per ottenere informazioni. Può presentarsi come un rappresentante di un'azienda o un'autorità.
* **Dettagli**: Contatta la vittima, spesso usando un tono autoritario, e richiede informazioni personali, come il numero di previdenza sociale o dettagli bancari.
* **Obiettivo**: Ottenere informazioni riservate senza destare sospetti.

**3. Baiting**

* **Descrizione**: Utilizza l'attrazione di un premio o di un vantaggio per indurre la vittima a scaricare malware o fornire dati. Ad esempio, una chiavetta USB infetta lasciata in un luogo pubblico.
* **Obiettivo**: Infiltrare un sistema con malware.

**4. Quizzing**

* **Descrizione**: Viene effettuato un interrogatorio diretto, dove il truffatore si presenta come un addetto al supporto clienti o un rappresentante aziendale, ponendo domande per ottenere informazioni.
* **Obiettivo**: Raccolta di informazioni sensibili come password o dettagli di accesso.

**5. Tailgating**

* **Descrizione**: Il truffatore si fa seguire all'interno di un edificio sicuro da una persona autorizzata, approfittando della buona fede della vittima.
* **Dettagli**: Può approfittare di un momento in cui la porta si apre, come quando un dipendente usa la propria badge per entrare. Una volta dentro, può cercare di accedere a aree sensibili.
* **Obiettivo**: Accedere fisicamente a spazi protetti.

**6. Shoulder Surfing**

* **Descrizione**: Osservare di nascosto qualcuno mentre inserisce dati sensibili, come password o informazioni bancarie.
* **Obiettivo**: Rubare informazioni senza necessità di interazione.

**7. Vishing (Voice Phishing)**

* **Descrizione**: Simile al phishing, ma avviene tramite telefono. Il truffatore chiama la vittima fingendosi un rappresentante di un'azienda.
* **Dettagli**: Utilizza informazioni personali (ottenute da fonti pubbliche o da precedenti violazioni) per guadagnare la fiducia della vittima e chiede conferma di dati sensibili, come numeri di conto o codici di sicurezza.
* **Obiettivo**: Ottenere dati sensibili o indurre la vittima a eseguire azioni specifiche.

**8. Spear Phishing**

* **Descrizione**: Variante del phishing mirata a un individuo o un'organizzazione specifica, con contenuti personalizzati per aumentare le probabilità di successo.
* **Dettagli**: L'email può sembrare provenire da un collega o un superiore, e può contenere richieste urgenti di azioni, come il trasferimento di fondi o la condivisione di documenti riservati.
* **Obiettivo**: Raccogliere informazioni di valore, spesso per attacchi mirati.

**9. Impersonation**

* **Descrizione**: Il truffatore si presenta come un dipendente o un partner di fiducia per ottenere informazioni o accesso a risorse aziendali.
* **Obiettivo**: Sfruttare la fiducia per ottenere dati sensibili.

**10. Scareware**

* **Descrizione**: Truffe che utilizzano la paura, come avvisi di virus o attacchi, per indurre le vittime a scaricare software dannoso o a pagare per servizi inutili.
* **Obiettivo**: Creare panico per indurre la vittima a compiere azioni impulsive.

È importante adottare misure preventive come queste sotto elencate, che se adottate possono significativamente ridurre il rischio di attacchi di ingegneria sociale migliorando la sicurezza dell’azienda.

* **Formazione e Sensibilizzazione** dei dipendenti; Organizzando corsi regolari di formazione per i dipendenti su come riconoscere e reagire a tentativi di social engineering. La consapevolezza è la prima linea di difesa
* **Politiche di Sicurezza Chiare** e procedure di verifica dell’identità (come psw) per la gestione di informazioni sensibili.
* **Controlli di Accesso** e implementazione dell’autenticazione a due fattori per verificarne l’identità.
* **Limitare l'accesso** alle informazioni riservate solo a chi ne ha realmente bisogno, minimizzando così il rischio di esposizione.
* **Simulazioni di Attacco** eseguendo test di phishing simulati per valutare la preparazione dei dipendenti e identificare aree in cui è necessaria una formazione aggiuntiva**.**
* **Implementare misure di sicurezza fisica**, come badge di accesso e monitoraggio delle aree sensibili, per prevenire accessi non autorizzati.
* **Riconoscimento di Segnali di Allerta** come urgenza eccessiva o richieste vaghe di informazioni.
* **Assicurarsi che tutti i sistemi siano aggiornati** per ridurre le vulnerabilità tecniche che potrebbero essere sfruttate.

Utilizzare tecniche simulate di ingegneria sociale per formare i dipendenti può essere molto efficace, purché venga fatto in modo responsabile. Le simulazioni devono essere controllate e possono includere workshop interattivi, feedback immediato e risorse educative. È fondamentale mantenere un ambiente di apprendimento positivo, dove i dipendenti si sentano liberi di esprimere dubbi.

Organizzare questo tipo di simulazioni richiede pianificazione e attenzione ai dettagli. È importante definire obiettivi chiari, pianificare gli scenari imitando situazioni comuni, come email da un fornitore, richieste di aggiornamento delle password o comunicazioni interne, scegliere un software di simulazione, segmentare il pubblico, e informare i leader aziendali. Dopo aver eseguito la simulazione, è necessario analizzare i risultati, fornire feedback e pianificare ulteriori sessioni di formazione, ripetendo le simulazioni regolarmente.

Infine, è fondamentale notare che esistono siti e forum online dove vengono scambiate informazioni relative all'ingegneria sociale, ma parteciparvi è illegale e contro le norme etiche. È importante utilizzare le informazioni solo per scopi difensivi e educativi, come migliorare la sicurezza contro tali attacchi; inoltre è di cruciale importanza educare gli utenti sulla sicurezza, promuovere la verifica delle informazioni e implementare misure di autenticazione forti per ridurre il rischio di cadere in queste trappole.