**S4 L4**

**Prompt per ChatGPT**

**Social Engineering**

-Il prompt che useremo per comunicare con chatGPT è:

Spiega cos'è il social engineering nell'ambito della cybersecurity, includendo una panoramica delle tecniche principali utilizzate dagli attaccanti per manipolare le persone e ottenere informazioni sensibili o accesso a sistemi informatici.

-La risposta che otterremo sarà:

Il social engineering è una tecnica di attacco utilizzata in ambito cybersecurity che si basa sulla manipolazione psicologica delle persone, anziché sull’uso diretto di exploit tecnici, per ottenere informazioni riservate o accesso a sistemi protetti. Gli attaccanti sfruttano la fiducia, la paura, l’avidità o l’ingenuità delle vittime per convincerle a rivelare informazioni o compiere azioni che compromettono la sicurezza dei dati o delle infrastrutture.

Principali tecniche di social engineering:

1. **Phishing**

È una delle tecniche di social engineering più comuni e consiste nell'invio di email, SMS o messaggi istantanei che sembrano provenire da fonti fidate (come banche, aziende, colleghi) e che inducono l’utente a fornire informazioni sensibili o a cliccare su link dannosi. Alcune varianti includono il \*spear phishing\*, un attacco altamente personalizzato rivolto a individui specifici, e il \*whaling\*, che mira a dirigenti aziendali di alto livello.

2. **Pretexting**

In questa tecnica, l’attaccante si costruisce un falso pretesto (o “pretext”) per ottenere informazioni. Può impersonare una figura autorevole come un responsabile delle risorse umane, un addetto IT, o anche un fornitore esterno per indurre la vittima a fornire informazioni sensibili come password, numeri di conto, o dettagli personali.

3. **Baiting**

Il baiting sfrutta la curiosità o l'avidità della vittima. L’attaccante offre qualcosa di desiderabile (ad esempio un file, uno sconto, o un’unità USB apparentemente smarrita) in cambio di un'azione che porta alla compromissione del sistema. Una tipica tecnica di baiting prevede il piazzare chiavette USB infette in luoghi strategici sperando che qualcuno le inserisca nei propri computer, infettandoli.

4. **Quid pro quo**

Con questa tecnica, l'attaccante si finge un operatore di supporto o un esperto IT e offre un aiuto in cambio di informazioni o accessi. Ad esempio, potrebbe chiedere alla vittima di disattivare la protezione antivirus per “risolvere un problema” o indurre a rivelare le proprie credenziali con il pretesto di “aiutare” a recuperare dati persi.

5. **Tailgating (o piggybacking)**

Il tailgating consiste nel seguire una persona autorizzata all'interno di una zona protetta senza avere le proprie credenziali. Spesso l’attaccante si presenta come un dipendente che ha dimenticato il badge o come un fornitore carico di materiali, sfruttando l'empatia delle persone per accedere a zone riservate.

Efficacia e difese contro il social engineering

Il social engineering si basa sulla comprensione della psicologia umana e delle dinamiche aziendali, rendendolo estremamente efficace. Molti attacchi riescono perché le persone tendono a fidarsi o hanno timore di sfidare figure apparentemente autorevoli.

Per difendersi da questi attacchi, è fondamentale:

- Sensibilizzare e formare il personale su come riconoscere e rispondere ai tentativi di social engineering.

- Implementare l’autenticazione a più fattori (MFA) per aggiungere un ulteriore livello di sicurezza.

- Promuovere una cultura aziendale di verifica in cui sia normale chiedere una doppia conferma o chiamare direttamente un fornitore o un superiore per autenticare una richiesta.

- Monitorare e limitare gli accessi fisici e utilizzare badge individuali per evitare l’ingresso non autorizzato.

Queste tecniche di social engineering sono tanto pericolose quanto complesse da individuare, poiché sfruttano una delle vulnerabilità più difficili da correggere: il fattore umano.

Dopo aver ottenuto la risposta, creiamo un altro prompt:

Riusciresti a suggerirmi e spiegarmi strategie e migliori pratiche per difendersi dagli attacchi di social engineering?

La risposta sarà:

Certamente, adottare le giuste strategie e migliori pratiche può fare una grande differenza nel proteggere sia individui che aziende dagli attacchi di social engineering. Ecco alcune delle difese più efficaci:

1. **Formazione e sensibilizzazione del personale**

La formazione continua è uno dei pilastri per difendersi dal social engineering. È essenziale educare i dipendenti a riconoscere i tentativi di manipolazione e le tattiche più comuni (phishing, pretexting, etc.). Le migliori pratiche includono:

-Programmi di formazione periodica: Insegnano ai dipendenti a identificare messaggi sospetti e a evitare di condividere informazioni sensibili.

-Simulazioni di attacco: Email di phishing simulate permettono ai dipendenti di fare pratica in un ambiente sicuro.

-Incentivi per la segnalazione: Premiare chi segnala tentativi di social engineering aiuta a sviluppare una cultura di vigilanza.

2. **Verifica delle identità**

Sospettare e verificare sempre l’identità di chiunque richieda informazioni sensibili, soprattutto se lo fa via email, telefono o in contesti informali.

-Richiesta di conferma da parte di una seconda fonte: Quando si riceve una richiesta sospetta, è utile confermare l'identità della persona tramite un altro canale di comunicazione, come una telefonata a un numero verificato.

-Regole di autenticazione stringenti: Procedure per verificare l’identità del personale che effettua richieste sensibili (ad esempio, i dipendenti devono chiamare il supporto IT direttamente anziché rispondere a email o telefonate inaspettate).

3. **Autenticazione a più fattori (MFA)**

L'MFA rende molto più difficile per un attaccante ottenere l'accesso a sistemi o account con credenziali sottratte attraverso il social engineering. Integrando più livelli di verifica, gli attaccanti non possono accedere anche se ottengono una password o un PIN.

4. **Segregazione delle informazioni**

Minimizzare la quantità di informazioni che ciascun dipendente può accedere in base al principio del "least privilege" (minimo privilegio). Questo riduce il rischio che un attaccante ottenga tutte le informazioni di cui ha bisogno da una singola fonte.

-Separazione dei ruoli e delle informazioni: Gli utenti hanno accesso solo a ciò di cui hanno bisogno per il loro lavoro.

-Divisione dei compiti: Questo metodo limita il rischio che un singolo dipendente possa completare un'azione dannosa, anche se viene manipolato.

5. **Politiche di password sicure**

Password forti e uniche per ogni account riducono l'efficacia del social engineering, soprattutto quando le credenziali vengono rubate.

-Impostazione di criteri di complessità delle password: Richiedere password lunghe, uniche e composte da caratteri alfanumerici e simboli.

-Modifica frequente delle password: L'aggiornamento regolare delle password e l'uso di un gestore di password aiuta a ridurre il rischio.

6. **Monitoraggio dell'attività e risposta rapida agli incidenti**

Un monitoraggio costante delle attività permette di identificare tempestivamente comportamenti sospetti che possono essere associati a un attacco di social engineering.

-Analisi e log degli accessi: Monitorare le attività di accesso per identificare tentativi di accesso insoliti o fuori dal normale orario di lavoro.

-Risposta automatizzata agli incidenti: Procedure e protocolli che scattano in caso di attività sospette possono fermare un attacco prima che causi danni.

7. **Promuovere una cultura della sicurezza**

Creare un ambiente in cui i dipendenti sentano la responsabilità condivisa di mantenere la sicurezza dell'azienda. Questo include anche la libertà di fare domande su comportamenti sospetti senza temere ripercussioni.

-Incentivare la comunicazione: È importante che i dipendenti si sentano a loro agio nel segnalare situazioni dubbie e nel chiedere una verifica delle richieste.

-Procedure per la segnalazione anonima: Offrire canali anonimi per segnalare tentativi di social engineering, riducendo la paura di ritorsioni.

8. **Limitare l'accesso fisico**

Proteggere le aree aziendali critiche impedendo il tailgating (o “passaggio in coda”) e adottando sistemi di accesso sicuri per prevenire intrusioni non autorizzate.

-Badge e accesso biometrico: L’uso di badge con foto o scanner biometrici riduce il rischio che gli estranei accedano a spazi riservati.

-Procedure di accesso per visitatori: Monitorare i visitatori e utilizzare badge temporanei per loro, affinché siano facilmente identificabili.

9. **Esercitazioni periodiche di consapevolezza della sicurezza**

Gli attacchi di social engineering sono in costante evoluzione, quindi è essenziale aggiornare le difese. Esercitazioni regolari e aggiornamenti sulle tecniche emergenti mantengono i dipendenti preparati.

10. **Testare e aggiornare regolarmente le politiche di sicurezza**

Effettuare regolarmente controlli di sicurezza e test di penetrazione per valutare la resilienza delle difese aziendali contro il social engineering e fare aggiornamenti mirati.

Con queste strategie, le persone e le organizzazioni possono ridurre significativamente la probabilità di cadere vittima del social engineering.

**Esplorazione dei CVE tramite ChatGPT**

Prompt:

Potresti fornirmi una lista dei CVE di Windows 10, vorrei anche informazioni dettagliate su alcuni di essi, inclusi i dettagli delle vulnerabilità e le soluzioni consigliate

Risposta:

Ecco una panoramica su alcune vulnerabilità CVE di Windows 10, con esempi specifici e soluzioni consigliate.

1. CVE-2021-34527 - PrintNightmare: Questa vulnerabilità critica nei servizi di stampa di Windows consente a un attaccante di eseguire codice arbitrario sul sistema, ottenendo privilegi di amministratore. La vulnerabilità è causata da un problema nei privilegi di accesso alla stampa. Microsoft ha rilasciato patch per risolvere questa vulnerabilità e ha consigliato di disabilitare il servizio di spooler di stampa su macchine che non ne hanno bisogno.

2. CVE-2020-0796 - SMBGhost: Colpisce il protocollo Server Message Block 3.1.1 e permette l'esecuzione remota di codice, consentendo ad un attaccante di compromettere un sistema Windows 10. Microsoft ha risolto questa vulnerabilità fornendo un aggiornamento di sicurezza, e una delle misure consigliate include la disabilitazione della compressione SMBv3 dove possibile.

3. CVE-2019-9510 - RDP Session Reconnect: Questa vulnerabilità influisce sulle sessioni Remote Desktop Protocol (RDP). Un attaccante può riconnettersi a una sessione RDP bloccata senza ri-autenticarsi, potenzialmente accedendo a una sessione utente non autorizzata. Per mitigare questa vulnerabilità, Microsoft ha suggerito l’implementazione di patch specifiche e l'utilizzo di criteri di sessione più restrittivi.

4. CVE-2018-8174 - Double Kill: Vulnerabilità nel motore di scripting VBScript di Windows che consente l'esecuzione di codice arbitrario, sfruttabile attraverso siti Web compromessi o documenti dannosi. Microsoft ha risolto questo problema con patch e raccomanda di limitare l'uso di VBScript e utilizzare un browser con più protezioni attive contro attacchi di script dannosi.

Puoi trovare dettagli completi e aggiornamenti su ogni vulnerabilità visitando il **NVD di NIST** (https://nvd.nist.gov) o la **Microsoft Security Response Center** (https://msrc.microsoft.com/) che forniscono informazioni e raccomandazioni dettagliate per ogni CVE.