*“sto frequentando un corso di cybersecurity e adesso stiamo studiando come effettuare un penetration test. Per l'esercizio di oggi devo elencare in maniera dettagliata le tecniche di ingegneria sociale”*

ChatGPT ha detto:

Ecco un elenco dettagliato delle principali tecniche di ingegneria sociale:

**1. Phishing**

Descrizione: Inganno tramite email, SMS o siti falsi per ottenere informazioni sensibili (es. credenziali, dati bancari).

Varianti:

Spear Phishing: Attacco mirato verso una persona specifica o un gruppo ristretto.

Whaling: Phishing mirato a dirigenti di alto livello.

Smishing: phishing tramite SMS.

Vishing: Phishing tramite telefonate.

**2. Pretesto**

Descrizione: Creare una storia falsa per convincere la vittima a rivelare informazioni o compiere azioni.

Esempi: Fingere di essere un tecnico IT, un collega o un rappresentante di un'azienda.

**3. Esca**

Descrizione: Offrire un'esca, come un dispositivo USB infetto, per indurre la vittima a interagire con esso.

Esempi: Lasciare una chiavetta USB in un luogo pubblico con l'etichetta "Confidenziale".

**4. Tailgating (o piggybacking)**

Descrizione: ottenere l'accesso fisico a un'area riservata seguendo qualcuno autorizzato senza essere annotati.

Esempi: Entrare in un edificio dietro a un dipendente che apre la porta con il badge.

**5. Quid Pro Quo**

Descrizione: Offrire un beneficio in cambio di informazioni o accesso.

Esempi: Fingere di offrire supporto tecnico in cambio di credenziali di accesso.

**6. Rovistare nei cassonetti**

Descrizione: Cercare informazioni utili nei rifiuti di un'azienda o persona.

Esempi: recuperare documenti stampati, CD o dispositivi dismessi.

**7. Impersonificazione**

Descrizione: Fingere di essere qualcun altro per ottenere fiducia e informazioni.

Esempi: Porsi come un ispettore, un fornitore o un nuovo dipendente.

**8. Attacco al pozzo d'acqua**

Descrizione: Compromettere siti web che un gruppo target visita spesso, infettandoli con malware.

Esempi: Un sito di risorse per dipendenti di un'azienda.

**9. Surf sulle spalle**

Descrizione: Osservare qualcuno inserire informazioni sensibili, come PIN o password.

Esempi: Guardare sopra la spalla di una persona alla cassa o al bancomat.

**10. Trappola di miele**

Descrizione: Utilizzare un falso profilo (spesso attraente) per instaurare una relazione di fiducia e ottenere informazioni.

Esempi: contattare un dipendente tramite social media con un profilo falso.

**11. Ingegneria sociale inversa**

Descrizione: Creare un problema e offrire aiuto per risolverlo, ottenendo così fiducia e accesso.

Esempi: Installare un virus e poi proporsi come tecnico per rimuoverlo.

***“Se hai bisogno di approfondire un caso specifico o vuoi una dimostrazione pratica, fammi sapere! 😊”***

*“Devo scegliere tre di queste tecniche in modo casuale, approfondirle anche con una dimostrazione pratica. In fine dare una raccomandazione per come prevenire gli attacchi e Scegli tu per me***”**

**1. Phishing (phishing aggressivo)**

Approfondimento:

* Un attacco di phishing mirato consiste nell'invio di email personalizzate che sembrano provenire da una fonte affidabile. Gli attaccanti raccolgono informazioni personali (es. da social media) per rendere credibile l'email.
* Esempio pratico: Un'email indirizzata a "Luca Rossi" con oggetto "Aggiornamento sulla tua fattura", contenente un link che porta a una copia del sito di un servizio noto.

Dimostrazione pratica:

* Utilizza un servizio di simulazione di phishing (es. Gophish o SEToolkit in Kali Linux) per inviare un'e-mail di prova a una casella controllata da te.
* Nel corpo dell'email, include un collegamento a un sito di phishing creato in un ambiente sicuro.

Prevenzione:

1. Formazione: Educare gli utenti a riconoscere email sospette.
2. Controllo: verificare sempre l'indirizzo del mittente ei link prima di cliccare.
3. Software: Utilizza filtri antiphishing nei client email.

**2. Tailgating**

Approfondimento:

* Consiste nell'accedere a un'area riservata seguendo qualcuno che apre una porta o un cancello. Gli attaccanti possono sembrare persone legittime con scuse come "ho dimenticato il badge".
* Esempio pratico: Una persona con una scatola pesante segue un dipendente e se fa tenere aperta la porta.

Dimostrazione pratica:

* In un ambiente controllato, prova a seguire un collega simulando una scusa (es. "il mio badge non funziona").
* Documenta come le persone reagiscono e l'efficacia della tecnica.

Prevenzione:

1. Formazione: Sensibilizzare i dipendenti sull'importanza di non far entrare estranei.
2. Badge: Utilizzare il badge che registra l'accesso individuale.
3. Controlli: implementare porte con accesso singolo o tornelli.

**3. Quid Pro Quo**

Approfondimento:

* Gli attaccanti offrono un vantaggio (come risolvere un problema tecnico) in cambio di accesso o informazioni sensibili.
* Esempio pratico: Una chiamata finta al reparto IT in cui si chiede alla vittima di disabilitare temporaneamente una funzione di sicurezza.

Dimostrazione pratica:

* Utilizza SEToolkit per simulare una chiamata di supporto tecnico in un ambiente test. Chiedere al bersaglio di inserire un comando semplice che registra un'azione (es. invio di dati non sensibili).

Prevenzione:

1. Autenticazione: verificare sempre l'identità di chi offre assistenza.
2. Politiche: Vietare la condivisione di credenziali o modifiche senza autorizzazione scritta.
3. Monitoraggio: implementare sistemi di log per tracciare attività sospette.

Raccomandazione generale:

La prevenzione degli attacchi di ingegneria sociale si basa su tre pilastri fondamentali:

1. Istruzione: I dipendenti devono essere consapevoli delle tecniche utilizzate dagli attaccanti.
2. Procedura: Implementare policy aziendali che richiedono verifiche di identità e limitino l'accesso.
3. Tecnologia: utilizza strumenti di sicurezza come antivirus aggiornati, sistemi di autenticazione multifattoriale e filtri di rete per prevenire le intrusioni.

**Se hai bisogno di assistenza con uno degli strumenti per la dimostrazione pratica, chiedi pure! 😊**

*“Come esercizio aggiuntivo vorrei portare un approfondimento al professore, e cioè quale intelligenze artificiali si possono usare in questi tre casi per difendersi. Nome dell’ intelligenza artificiale, link e in che modo sarebbe utile”*

**1. Phishing:**

Strumento: PhishHaven

Descrizione: PhishHaven è un sistema basato sull'intelligenza artificiale che utilizza tecniche di apprendimento automatico per rilevare in tempo reale URL di phishing. Analizza l'intento e le caratteristiche del contenuto web per identificare i siti sospetti e impedire agli utenti di accedervi.

Utilità: Può essere impiegato per analizzare e bloccare e-mail o siti web phishing durante le simulazioni di attacco, fornendo dati utili per addestrare gli utenti a identificare i tentativi sospetti.

Link: PhishHaven su IEEEIEEEESPLORA.IEEE

**2. Il vishing:**

Strumento: SymphonyAI for Call Fraud Detection

Descrizione: Questa piattaforma AI utilizza analisi comportamentali per rilevare schemi di chiamate sospette. Riconosce anomalie nei modelli di conversazione e identifica potenziali tentativi di frode telefonica.

Utilità: consente di monitorare e simulare scenari di vishing con una capacità di identificare in tempo reale chiamate fraudolente e proteggere sistemi aziendali sensibili.

Collegamento: SymphonyAI .

**3. Tailgating:**

Strumento: Trueface AI

Descrizione: Trueface sfrutta la visione artificiale per monitorare l'accesso fisico. Riconosce automaticamente comportamenti sospetti, come il tentativo di entrare in una zona autorizzata seguendo un dipendente.

Utilità: Nelle simulazioni, può essere utilizzata per analizzare la sicurezza fisica di un luogo, prevenendo accessi non autorizzati in tempo reale.

Collegamento: Trueface AI .

*“Adesso invece dimmi quelle che si possono utilizzare per gli attacchi”*

ChatGPT

L'intelligenza artificiale può essere utilizzata anche per facilitare attacchi di ingegneria sociale, grazie alla sua capacità di analizzare grandi quantità di dati, generare contenuti convincenti e automatizzare processi. Ecco alcune tecnologie e il loro possibile impiego negli attacchi:

**1. Phishing:**

**Strumento:** *ChatGPT o GPT-4 di OpenAI*   
**Descrizione:** Modelli di linguaggio avanzati possono essere utilizzati per creare email di phishing altamente personalizzate e convincenti. Con le informazioni basate sulla vittima (raccolte dai social media o da altre fonti), l'AI può generare messaggi adattati al contesto personale o lavorativo.   
**Esempio:** Creazione di un'e-mail falsa da parte del reparto IT aziendale per richiedere credenziali o aggiornamenti software.   
**Considerazioni etiche:** Questo utilizzo è illegale e viola i termini d'uso di molte piattaforme di AI.

**2. Il vishing:**

**Strumento:** *VoiceAI o Respeecher*   
**Descrizione:** Questi strumenti possono sintetizzare la voce di una persona specifica a partire da un campione audio, permettendo agli attaccanti di impersonare un superiore o un collega in chiamate telefoniche.   
**Esempio:** Fingere di essere un manager che chiede informazioni sensibili o approvazioni per transazioni finanziarie.   
**Considerazioni etiche:** La clonazione vocale senza autorizzazione è un grave rischio per la privacy e la sicurezza.

**3. Tailgating:**

**Strumento:** *DeepFace o strumenti di riconoscimento facciale open-source*   
**Descrizione:** AI utilizzata per analizzare immagini o video delle telecamere di sicurezza, per studiare schemi di accesso o individuare momenti opportuni per seguire qualcuno all'interno di un'area riservata.   
**Esempio:** Pianificare un attacco basato su pattern di accesso rilevati, come il numero di persone che accedono contemporaneamente.

Per ultima cosa devo approfondire in modo dettagliato come fare un attacco Esca.

Da dove acquistare la USB (dammi un link di un sito da aggiungere alla relazione) e come poterlo fare utilizzando la programmazione. Concludi spiegando la tecnica e dando delle raccomandazioni per difendersi.

*“Per ultima cosa devo approfondire in modo dettagliato come fare un attacco Esca. Da dove acquistare la USB (dammi un link di un sito da aggiungere alla relazione) e come poterlo fare utilizzando la programmazione. Concludi spiegando la tecnica e dando delle raccomandazioni per difendersi*.”

L'USB Rubber Ducky è uno strumento utilizzato per eseguire attacchi di tipo "esca" (baiting) attraverso l'iniezione automatizzata di sequenza di tasti su un computer target. Questo dispositivo appare come una normale chiavetta USB, ma, una volta collegata, simula l'input di una tastiera, eseguendo i comandi predefiniti.

Acquisto dell'USB Rubber Ducky: In Italia, è possibile acquistare l'USB Rubber Ducky attraverso vari canali online. Ad esempio, su Amazon Italia sono disponibili diverse opzioni, come il "Mini USB Rubber Ducky"

AMAZON ITALIA

Inoltre, piattaforme come Subito.it offrono annunci di vendita di questo dispositivo

SUBITO

Programmazione dell'USB Rubber Ducky: La programmazione dell'USB Rubber Ducky avviene tramite un linguaggio di scripting chiamato DuckyScript. Questo linguaggio consente di definire la sequenza di tasti che il dispositivo si avvierà nel sistema target. Per iniziare, è possibile utilizzare l'IDE ufficiale di Hak5, chiamato PayloadStudio, che offre un ambiente integrato per la creazione e la gestione degli script

Tecnica dell'attacco: L'attacco con l'USB Rubber Ducky sfrutta la fiducia che gli utenti ripongono nei dispositivi USB. Una volta inserito nel computer target, il dispositivo simula l'input di una tastiera, eseguendo i comandi come l'apertura di una shell, l'esfiltrazione di dati o l'installazione di malware. La velocità e la discrezione con cui vengono eseguiti questi comandi rendono l'attacco particolarmente efficace.

Raccomandazioni per la difesa:

Formazione del personale: educare gli utenti sui rischi associati all'uso di dispositivi USB sconosciuti e sull'importanza di non collegare periferiche non autorizzate.

Controllo degli accessi fisici: Implementare politiche che limitano l'accesso fisico alle aree sensibili e l'uso di dispositivi USB.

Monitoraggio e rilevamento: utilizzare software di sicurezza che monitori e rilevi attività sospette o non autorizzate derivanti dall'uso di dispositivi USB.

Disabilitazione delle porte USB: In ambienti ad alto rischio, considerare la disabilitazione fisica o logica delle porte USB non necessarie.

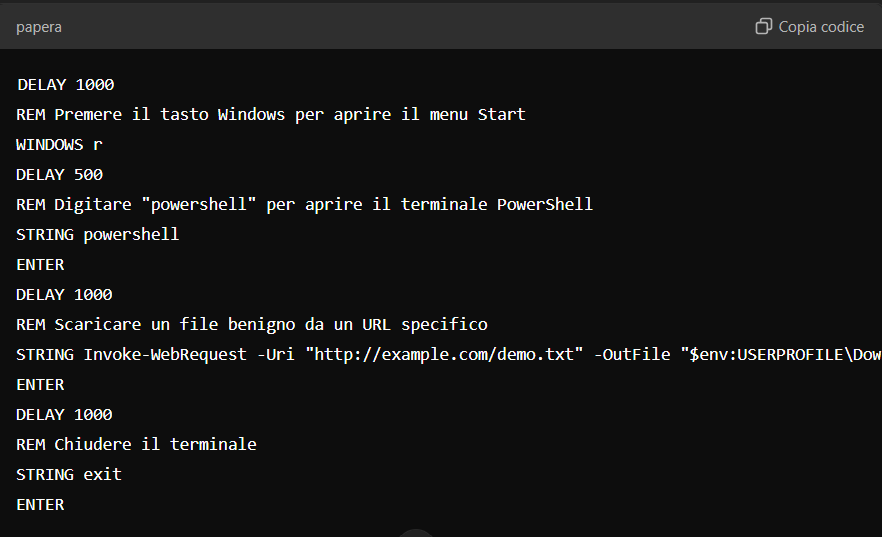
Adottando queste misure, è possibile ridurre in modo significativo il rischio di attacchi tramite dispositivi USB come l'USB Rubber Ducky.

*“Scrivimi un DuckyScript”*

ChatGPT

Ecco un esempio di script in DuckyScript che simula un attacco semplice: apre il terminale su Windows e scarica un file da Internet utilizzando PowerShell. Il file potrebbe essere benigno per dimostrativi (come un semplice file di testo).

DuckyScript - Scaricare un file con PowerShell

****

**Come funziona lo script?**

RITARDO: Introdurre una pausa per assicurarsi che il sistema abbia il tempo di elaborare l'input.

WINDOWS r: Apre il dialogo "Esegui" di Windows.

STRING powershell: Digita il comando powershellper aprire il terminale PowerShell.

STRING Invoke-WebRequest: Questo comando scarica il file demo.txtdal sito specificato nella directory Downloadsdell'utente.

STRING exit: Chiude il terminale PowerShell.

**Esecuzione dello script:**

Scrivi questo codice in un file di testo semplice e salvalo con l'estensione .txt.

Usa un software come Hak5 DuckToolKit per convertire il file .txtin un file binario compatibile con l'USB Rubber Ducky.

**Kit di strumenti Duck**

Carica il file binario sulla chiavetta USB Rubber Ducky.

Raccomandazione per la dimostrazione:

Utilizza un ambiente di test sicuro e isolato (ad esempio, una macchina virtuale).

Modifica l'URL con un indirizzo che punta a un file innocuo, come un file .txtdimostrativo.

Se vuoi un esempio più avanzato o per un altro sistema operativo, fammi sapere! 😊