

PROMPT PER CHATGPT

1)PUNTI CHIAVE

- Prompt Gemini Social Engineering
- Gathering informazioni delle tecniche di attacco/difesa
- Prompt Gemini lista CVE
- Analisi CVE Windowsxp

2)INTRODUZIONE

Nella Cybersecurity, viene implementato l'utilizzo dell'IA sia come aiuto nella prevenzione di attacchi sia strumento per analizzare e sviluppare questi ultimi .

È stato implementato l'uso di un IA per il gathering di informazioni sul social engineering, le tecniche di attacco e difesa.

Usata anche per ottenere una lista di vulnerabilità comuni ed esposizioni (CVE) del sistema operativo Windowsxp

4)PROMPT

3.1) Prompt Social Engineering e tecniche attacco

Sono uno studente di un corso di Cybersecurity, puoi spiegarmi cos'è il social engineering e descrivermi le tecniche più utilizzate dagli attaccanti?

*Prompt prima richiesta

Dalla risposta ho dedotto che:

Il Social Engineering è l'insieme di tecniche di manipolazioni psicologiche utilizzate per manipolare le persone e rivelare informazioni riservate (password, dati bancari, segreti industriali) e sfrutta:

- **Urgenza:** Creare panico per impedire alla vittima di riflettere.
- **Autorità:** Utilizzare il nome di un CEO o di un'alta carica per incutere timore.
- **Fiducia:** Costruire una relazione nel tempo per abbassare le difese.

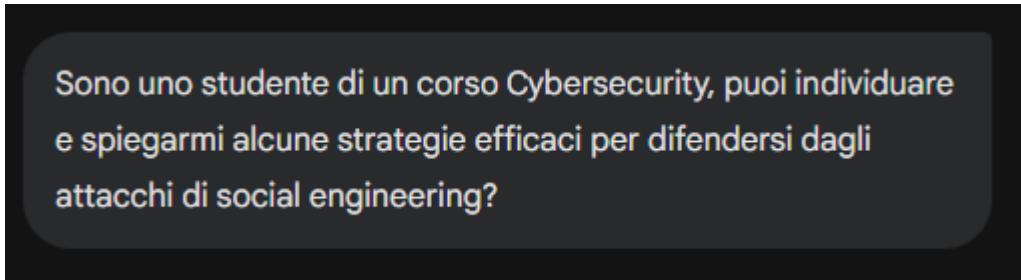
Le tecniche più utilizzate sono:

- **Phishing** ----> Consiste nell'invio di comunicazioni fraudolente che sembrano provenire da fonti affidabili.
- **Spear Phishing** ----> Un attacco mirato a una persona o azienda specifica, con dettagli personalizzati per risultare credibile.
- **Whaling** ----> Phishing rivolto alle cariche più alte (dirigenti, CEO).
- **Smishing & Vishing** ----> Attacchi tramite SMS (Smishing) o chiamate vocali (Vishing).
- **Pretexting** ----> L'attaccante crea uno scenario inventato per portare la vittima a fornire dati.
- **Baiting** ----> Si basa sulla curiosità come lasciare una **chiavetta USB infetta** in un parcheggio aziendale o in una sala d'attesa. Chi la trova, spinto dalla curiosità, la inserisce nel PC aziendale, installando involontariamente un malware.
- **Quid-Quo-Pro** ----> Promette un beneficio in cambio di un'azione.
- **Tailgating** ----> Una tecnica dove l'attaccante segue un dipendente autorizzato all'interno di un'area protetta.

Inoltre, è stato aggiunto anche un esempio reale sul Vishing verso **MGM Resorts** dove un gruppo di hacker ha trovato su **LinkedIn** il nome di un dipendente del reparto IT di MGM. Hanno poi chiamato l'Help Desk dell'azienda fingendo di essere quel dipendente e dichiarando di aver perso l'accesso al proprio account e convinti della messa in scena dell'attaccante, ha resettato le credenziali riuscendo ad avere accesso.

Una volta dentro, hanno installato un ransomware che ha paralizzato il casinò di Las Vegas per giorni. Perdita stimata di circa **100 milioni di dollari**.

3.2) Prompt tecniche difesa agli attacchi



Sono uno studente di un corso Cybersecurity, puoi individuare e spiegarmi alcune strategie efficaci per difendersi dagli attacchi di social engineering?

*Prompt seconda richiesta

Dalla risposta al mio prompt, ho ricavato che le strategie più efficaci verso questi attacchi sono:

- **Hardware MFA** ----> Si usano chiavi fisiche per l'autenticazione. Quando si fa il login, il sito invia una "sfida" alla chiavetta che la firma e la rimanda indietro. Se la firma è corretta si ha accesso al sito.
- **E-mail Security Gateway** ----> Utilizzo di filtri che analizzano e individuano segnali di *Business E-mail Compromise* (BEC), come cambiamenti improvvisi di tono o richieste urgenti di bonifici.
- **Principio del Minimo Privilegio (PoLP)** ----> Se un utente cade vittima di social engineering, i danni devono essere limitati. Se non ha i permessi di admin, l'attaccante non può scalare i privilegi facilmente. Questo secondo il **Role-Based Access Control**

Infine, di grande importanza tra le varie soluzioni è quello della **formazione** dove si allena l'utente con vari esempi e test di phishing .

3.3)PROMPT CVE

Sono uno studente della Cybersecurity,potresti fare una lista dei CVE relativi a Windowsxp? Vorrei anche informazioni dettagliate su alcuni di essi,inclusi i dettagli delle vulnerabilità e la soluzione relative?

**Prompt terza richiesta*

Viene così mostrata una lista di vulnerabilità del sistema operativo windowsxp dove vengono elencate in base alla criticità:

1)CVE-2019-0708: "BlueKeep" Remote Desktop Services (Critico) 9.8

Un attaccante può eseguire diversi codici semplicemente collegandosi alla porta 3389/TCP senza bisogno di username o password.

Una soluzione è l'installazione della patch più recente o disabilitare il Desktop Remoto se non necessario.

2)CVE-2017-0144:" EternalBlue" Protocollo SMBv1 (Critico) 9.3

Sfrutta un bug nel protocollo SMBv1 (Server Message Block) dove l'attaccante invia un pacchetto truccato che manderà in confusione il sistema aprendo così una porta per eseguire comandi con i massimi privilegi

Essendo "wormable", un sistema infetto può scansionare la rete locale e infettare automaticamente altri PC Windows XP con versioni obsolete.

Una soluzione è una patch MS17-010 per Windows XP oppure disabilitare completamente il protocollo SMBv1 obsoleto.

4) CONCLUSIONI

Il report mostra come l'IA sia un'arma a doppio taglio poiché fornisce grande aiuto per difendersi ma allo stesso tempo si comporta come un potente strumento per la fase di attacco semplicemente aggirando i filtri dell'IA.