ESERCIZIO S5 L4

"PROMPT A CHATGPT"

Per comprendere le tecniche di social engineering utilizzo questo prompt a chatgpt: "sono uno studente di cybersecurity, mi spieghi le tecniche si social engineering con esempi pratici e tecnici?"

Attraverso questi input ho capito che ci sono diversi diversi metodi per fare social engineering, vediamoli di seguito:

- Phishing: è un attacco via mail o testuale dove l'attacante utilizza un dominio molto simile all'orginale dove cerca di convincere la vittima a cliccare un link malintenzionato per prelevare passowrd o dati sensibili.
- Spear phishing: è molto simile al phishing solo che è indirizzato ad una persona specifica.
- Whaling: attacco che ha come bersaglio persone a capo di una azienda come un CEO o CFO. Ti fanno credere di essere questi soggetti e cercano di persuaderti per frodi bancarie
- Vishing: In questo caso è una telefonata dove gli hacker impersonificano una persona all'interno dell'azienda e cerca di ottenere chiavi di accesso
- Smishing: è il phishing ma tramite messaggi e whats'app
- Pretexting: gli hacker inventano una storia molto credibile per ottenere informazioni
- Baiting: spesso gli hacker usano una chiavetta usb con all'interno dei virus, sfrutta la curiosità della persona
- Tailgating: gi hacker accedono ad aree riservate con dei badge rubati

Ora che ho capito quali sono le tecniche che usano i red hat per manipolare le persone uso questo prompt su chatgpt per vedere quali sono le tattiche di difesa "spiegami in modo tecnico e con esempi pratici le misure di difesa che si possono adottare per contrastare il social engineering".

Vediamo come ci si può difendere dagli attacchi hacker:

- SPF, DKIM, DMARC per contrastare il phishing e spear phishing:
  SPF blocca i server per alcuni domini
  DKIM crittografia della mail
  DMAR decide cosa fare della mail se non passa
- Secure mail gateway, si analizza URL del mail con static o sandbox
- MFA autenticazione a due fattori, ad esempio usare anche il telfono prima di accedere ad un account
- EDR/XDR è una scatola nera installata su ogni computer e server che analizza i comportamenti anomali. Se ad esempio un utente apre un link che avvia la

powershell facendole compiere azioni sospette, l'edr interviene e blocca il processo. L'XDR è la versione estesa e più potente dell'EDR.

- Difesa da vishing, verificare sempre l'identità chiamando la reale persona
- Zero trust umano significa non dare la massima fiducia a nessuno, verificare sempre.
- Se si trova una usb bisogna sempre mandarla prima all IT
- Campagne all'interno dell'azienda per sensibilizzare e addrestare il personale al social engineering.