Kevin Giuseppe Cerrone

PROGETTO S5/L5

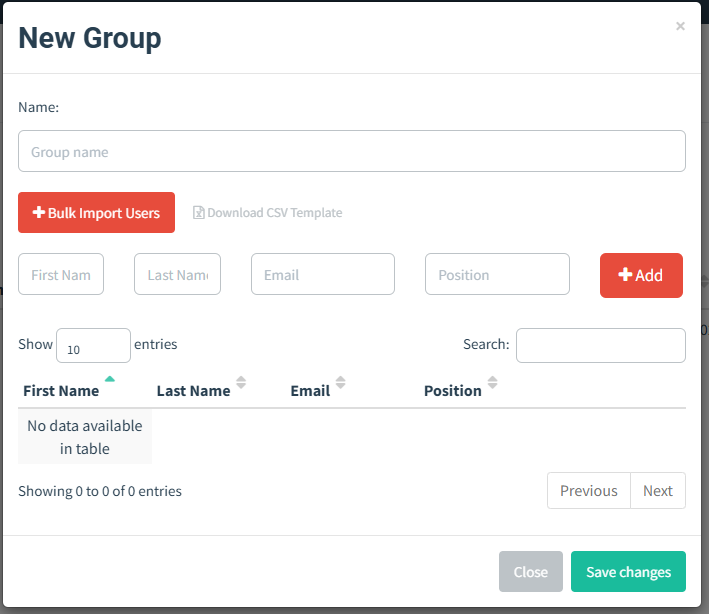
Ingegneria Sociale: Il Phishing

Il phishing è una tecnica di ingegneria sociale in cui i truffatori cercano di ingannare le persone per ottenere informazioni personali come password, numeri di carte di credito e dati bancari. Al giorno d’oggi questa tecnica è una delle più diffuse al mondo e l’unico modo per prevenire questa tipologia di attacchi è tramite la sensibilizzazione e l’istruzione.

Esistono vari tipi di e-mail che potrebbero ingannare gli utenti, dagli avvisi di accesso sospetto, alle e-mail da parte di colleghi e gente conosciuta. Vediamo nello specifico un chiaro esempio:

Immaginiamo ci sia stato un grosso leak di informazioni a danno di un’azienda, i dati finiscono online e chiunque abbia un minimo di conoscenze informatiche riesca a scaricarli. L’obiettivo del truffatore, in questo caso, sarà quello di recuperare gli username e password delle vittime per accedere ai loro servizi bancari. Non importa se l’e-mail non sarà accurata, statisticamente ci sarà sempre una percentuale di persone che rischia di cadere nel tranello e “regalare” i propri dati ai malintenzionati.

Per rendere questo esempio il più realistico possibile, abbiamo utilizzato Gophish per creare un’e-mail di phishing:

Tenendo in considerazione il presunto leak di dati, in questa schermata sarà possibile aggiungere tutti gli indirizzi e-mail delle vittime, permettendo al truffatore di avere a disposizione un consistente numero di persone a cui poter mandare le e-mail.

Una volta creato il gruppo di vittime, si passa alla creazione della vera e propria e-mail. Grazie a ChatGPT abbiamo avuto modo di crearne una, tenendo in considerazione i fattori più importanti, come richieste urgenti, link sospetti ed errori grammaticali. Di seguito un esempio di e-mail phishing:

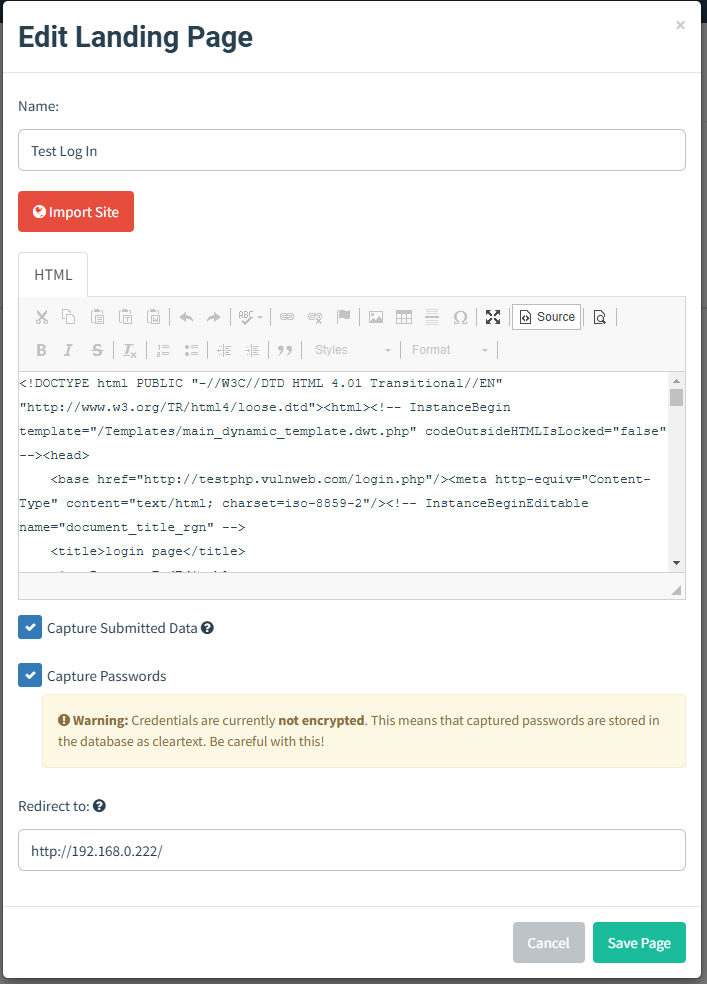
Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente**Elementi sospetti nell’email:**

1. **Tono eccessivamente urgente**: L’uso di maiuscole e di avvisi di chiusura immediata sono segnali di allarme.
2. **Errori grammaticali**: Errori come "*temporaneamenti*", "*informazionni*", "*cordialimenti*" e "*servizzio*" indicano una scarsa professionalità e sono spesso presenti nelle e-mail di phishing.
3. **Minaccia di sanzioni**: Includere sanzioni o altri avvertimenti gravi serve a mettere pressione alla vittima e indurla a cliccare senza riflettere.

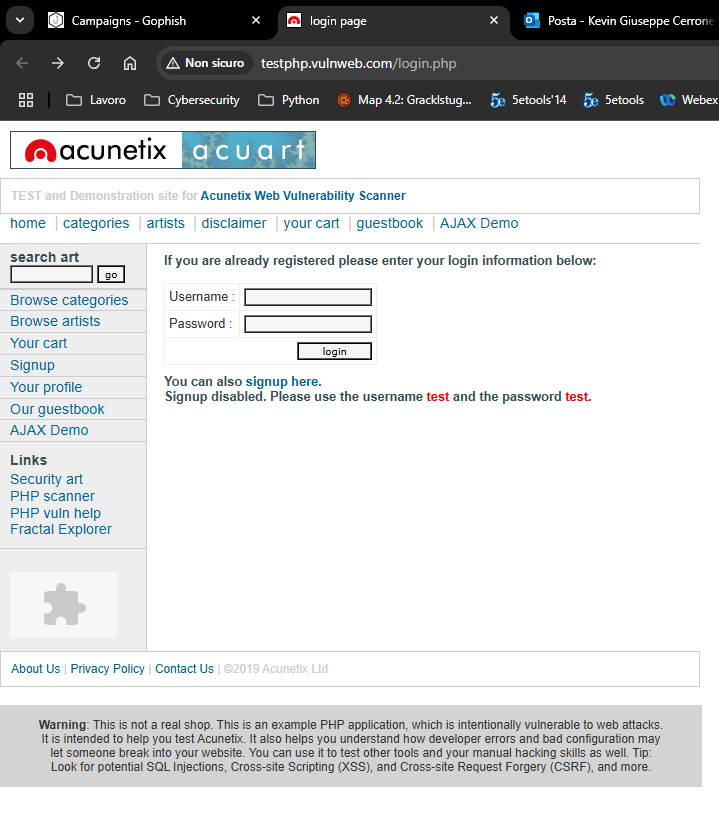
Questi sono segnali che dovrebbero far dubitare dell’autenticità dell’e-mail. In questi casi, è sempre meglio contattare l’istituzione ufficiale senza usare i link forniti.

Il povero malcapitato, però, non sa dell’esistenza dell’e-mail phishing e quindi clicca sul tasto “Verifica il tuo conto”. Cosa accadrà adesso?

La vittima verrà reindirizzata ad una pagina web di creazione del truffatore, con lo scopo di rubare i suoi dati per poi utilizzarli successivamente. Di seguito un esempio:  
  
Tramite l’utilizzo di Gophish o SET sarà possibile copiare un sito web realmente esistente. Usando il primo, è possibile importare interamente la pagina di login di un servizio bancario. La vittima verrà dunque reindirizzata ad un indirizzo ip di nostra creazione dove troverà un sito web identico all’originale.

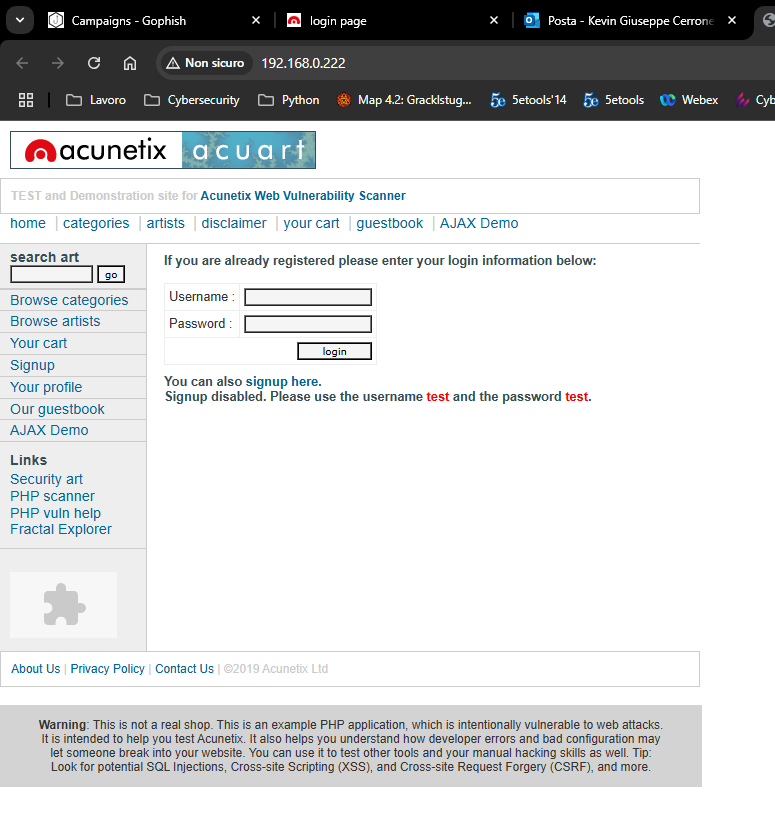
Ecco di seguito il sito web originale, con il sito web di nostra creazione, notate delle differenze?

**SITO WEB ORIGINALE**



Questa è la pagina web originale, lo si può notare dall’url del browser dove è correttamente riportato l’indirizzo, in questo caso: testphp.vulvweb.com/login.php

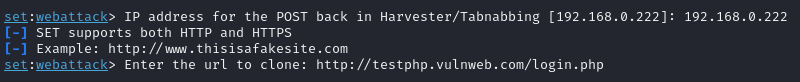
**SITO WEB RICREATO**



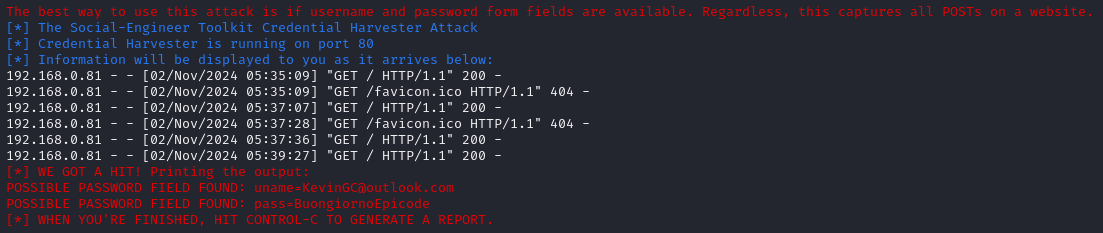
Questo, invece, è il sito web ricreato dal truffatore. Cosa c’è di diverso? Per un occhio inesperto assolutamente ma nulla, ma facendo più attenzione si può notare come l’url sia diverso rispetto al sito precedente. Qui troviamo un indirizzo IP Privato (in questo caso), solo questo dovrebbe bastare per fare scattare i nostri campanelli d’allarme.

Questo sito web è stato creato utilizzando SET. Si tratta di uno strumento di sicurezza e pentesting (penetration testing) progettato per simulare attacchi di ingegneria sociale e mettere alla prova la consapevolezza e la sicurezza degli utenti.

**CREAZIONE SITO CLONATO TRAMITE SET**

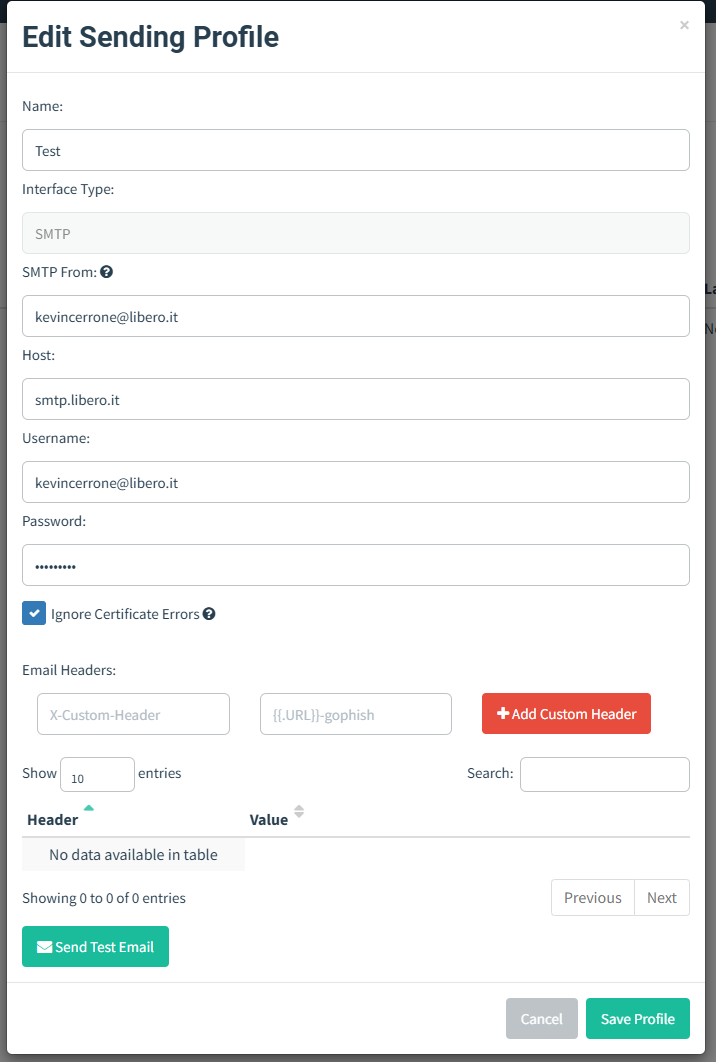


Come da esempio, abbiamo impostato l’indirizzo IP 192.168.0.222 e dando a SET l’url originale del sito web, è stato possibile ricrearne una copia esatta come mostrato precedentemente.

Se adesso il malcapitato dovesse immettere le su informazioni personali sul sito clonato, il truffatore riceverebbe i dati direttamente sul suo schermo tramite una notifica

Possiamo vedere chiaramente in esempio i dati rubati con e-mail “[KevinGC@outlook.com](mailto:KevinGC@outlook.com)” e password “BuongiornoEpicode”

**CREAZIONE DEL PROFILO EMAIL ATTACCANTE**

Ma come è stato possibile l’invio delle e-mail? Tramite gophish è possibile utilizzare un dominio web, che sarà visibile anche alla vittima. In questo caso abbiamo usato il dominio di libero.it e il suo SMTP (Simple Mail Transfer Protocol), creando un’e-mail al solo scopo di inviare i messaggi di phishing alle vittime. Dando quindi a gophish username e password dell’e-mail attaccante, il programma avrà modo di raggiungere la lista di e-mail precedentemente creata.

**CONCLUSIONE**

Come difendersi quindi da questi attacchi? Ci sono vari modi per farlo:  
  
1. Utilizzare domini web sicuri e affidabili come gmail (Google) o Proton che utilizzando protocolli aggiornati.

2. Controllare il contenuto dell’e-mail per scovare errori grammaticali, link sospetti. Nel dubbio, contattare direttamente la propria filiale per richiedere più informazioni.  
3. Controllare nella e-mail la presenza di tecnologie di autenticazione come SPF, DKIM e DMARC.

**SPF** è un sistema di autenticazione che consente di specificare quali server sono autorizzati a inviare e-mail per conto di un dominio.

**DKIM** è un metodo di autenticazione delle e-mail che utilizza una firma digitale per verificare che il contenuto del messaggio non sia stato alterato in transito e che provenga effettivamente dal dominio dichiarato.

**DMARC** è un protocollo che permette ai proprietari di un dominio di specificare come gestire i messaggi che falliscono i controlli SPF e DKIM. È pensato per aiutare a prevenire lo spoofing e fornire rapporti dettagliati sui tentativi di frode.

Questi tre sistemi di autenticazioni sono fondamentali per accertarsi dell’autenticità di un’e-mail, offrendo un livello di protezione completo e resiliente contro il phishing e lo spoofing.