Campagna phishing S5L5

Email di Phishing Personalizzata (Spear Phishing)

Oggetto: Urgente: Il tuo account Twitter è stato compromesso, agisci subito!

Da: supporto@twitter.com

Caro Tomas Bellini,

Ti scriviamo per informarti che il tuo account Twitter è stato recentemente compromesso. Abbiamo rilevato attività sospette nel tuo profilo, e al momento stiamo monitorando l'accesso non autorizzato. Inoltre, abbiamo notato che il tuo account sta condividendo contenuti inappropriati che violano le nostre politiche: materiale pedopornografico.

Poiché ci preoccupiamo per la tua privacy e sicurezza, ti avvisiamo che **tutti i tuoi contatti** stanno già vedendo questi contenuti. È fondamentale che tu intervenga immediatamente per evitare che il tuo account venga definitivamente sospeso e per proteggere la tua reputazione online.

Il tuo account è a rischio e solo tu puoi fermare questa situazione.

Visto che sei in ferie e probabilmente non hai ancora avuto tempo di controllare, vogliamo darti l'opportunità di risolvere rapidamente il problema. Ti consigliamo di agire entro **le prossime 24 ore**, altrimenti l'accesso al tuo account potrebbe essere limitato.

Ecco cosa devi fare per proteggere il tuo account e ripristinarlo immediatamente:

1. Clicca sul link qui sotto per entrare nel tuo account Twitter.
2. Una volta effettuato l'accesso, ti verrà richiesto di cambiare la password e rivedere le attività recenti.
3. Segui le istruzioni per rimuovere qualsiasi contenuto inappropriato dal tuo account e ripristina la sicurezza.

Clicca qui per accedere al tuo account e risolvere il problema

Nota importante: Abbiamo visto che hai due figli, Rosa e Piero, e che sei attualmente in ferie. Ti invitiamo a completare questa operazione rapidamente, così da non preoccuparti di eventuali ripercussioni nei giorni di riposo con la tua famiglia.

Se hai domande o necessiti di assistenza, il nostro team è a tua disposizione 24/7. Non esitare a contattarci.

Grazie per la tua attenzione e collaborazione. La tua sicurezza è la nostra priorità.

Cordiali saluti,

Il team di sicurezza Twitter

Relazione sull'uso di SET per la creazione di un sito di phishing di Twitter

Introduzione

Nel contesto di un'attività educativa e di sensibilizzazione alla cybersicurezza, ho utilizzato il **Social-Engineer Toolkit (SET)** su Kali Linux per simulare un attacco di **phishing**. L'obiettivo di questo esercizio era quello di comprendere le tecniche utilizzate dai criminali informatici per raccogliere informazioni sensibili attraverso l'inganno. In particolare, ho creato un **sito di phishing falso di Twitter**, sfruttando un **template preimpostato** offerto da SET, per raccogliere le credenziali di accesso degli utenti.

Obiettivo

Il fine di questa simulazione era quello di apprendere come i siti di phishing vengano creati e lanciati, per poter identificare e difendersi contro tali attacchi nella vita reale. In questo caso, l'attacco mirava a simulare un **spear phishing** diretto a un singolo individuo, utilizzando informazioni personalizzate (nome, lavoro, familiari) per rendere l'attacco più credibile.

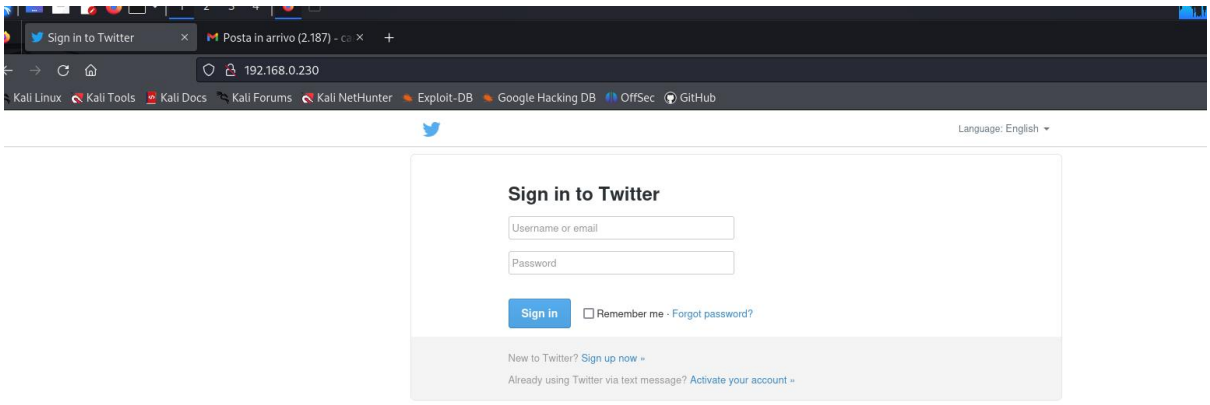
Strumenti Utilizzati

- **Kali Linux**: Il sistema operativo dedicato alla sicurezza informatica, contenente una vasta gamma di strumenti utili per il penetration testing e la simulazione di attacchi.
- **Social-Engineer Toolkit (SET)**: Un potente framework open-source progettato per simulare attacchi di ingegneria sociale. SET fornisce diversi template per creare siti di phishing credibili, ed è stato utilizzato in questo caso per generare una copia falsa della pagina di login di Twitter.
- **Template di phishing di Twitter**: SET offre vari template preimpostati per simulare pagine di login di social media popolari. Per questa simulazione, ho utilizzato il template relativo a Twitter.

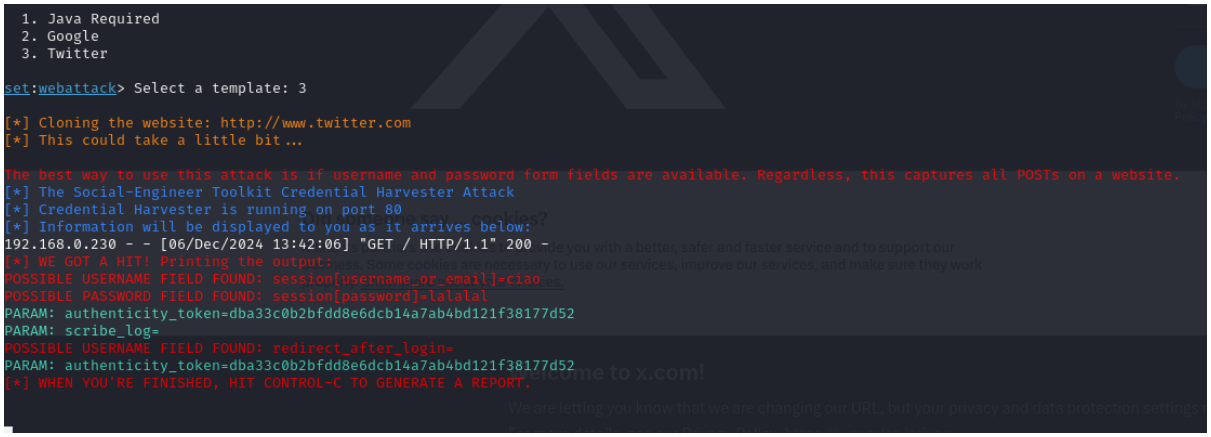
Fasi dell'Attacco

1. **Impostazione dell'ambiente di lavoro**:
    a. Ho avviato Kali Linux, che è preconfigurato con strumenti per il penetration testing.
    Ho lanciato SET attraverso il terminale.

2. **Selezione del tipo di attacco**:
    a. Una volta avviato SET, ho scelto l'opzione **"Spear-Phishing Attack"** per simulare un attacco mirato.
    b. Ho selezionato la **"Website Credibility"** come metodo per attaccare la vittima attraverso un sito web clonato.
3. **Creazione della Landing Page Falsa**:
    a. Ho scelto il template preimpostato relativo a Twitter, che replica la pagina di login.
    b. Ho configurato il sito fasullo in modo da includere un modulo di login che raccoglieva nome utente e password dell'utente.
    c. Ho personalizzato l'URL e configurato il sistema per raccogliere i dati inseriti nella falsa pagina di login.
4. **Configurazione dell'email di phishing**:
    a. Ho creato un'email personalizzata con un messaggio di **phishing** che avvisava la vittima di un problema con il proprio account Twitter, chiedendo di cliccare su un link per "ripristinare" l'accesso.
    b. Il link puntava al sito falso creato tramite SET, progettato per sembrare una vera pagina di login di Twitter.
5. **Invio dell'email e Monitoraggio**:
    a. Ho utilizzato l'email configurata su SET per inviare la simulazione a un indirizzo di test (account Gmail).
    b. Ho monitorato l'attività, verificando se l'utente ha cliccato sul link e inserito le credenziali nel sito fasullo.



-Qui sotto vediamo come il sito rilevi correttamente username e password della vittima.



Ecco una versione della relazione più diretta e senza giustificazioni:

Report sull'uso di Gophish per la simulazione di un attacco di phishing

Introduzione

Durante l'esercizio di simulazione di phishing, ho utilizzato **Gophish** per creare una campagna mirata a un obiettivo specifico. Tuttavia, non sono riuscito a completare correttamente la configurazione e l'esecuzione del processo. Il tentativo di configurare Gophish ha comportato diversi problemi tecnici che non sono riuscito a risolvere. Nonostante i numerosi tentativi, inclusi cambiamenti nelle impostazioni e la disattivazione dell'autenticazione a due fattori per l'account Gmail, non sono riuscito a ottenere il risultato desiderato.

Problemi Riscontrati

1. **Configurazione del Server SMTP**:
    a. Non sono riuscito a configurare correttamente il server SMTP per l'invio delle email di phishing. Le email non venivano inviate correttamente agli obiettivi, nonostante la corretta configurazione dei parametri di rete.
2. **Autenticazione a Due Fattori**:

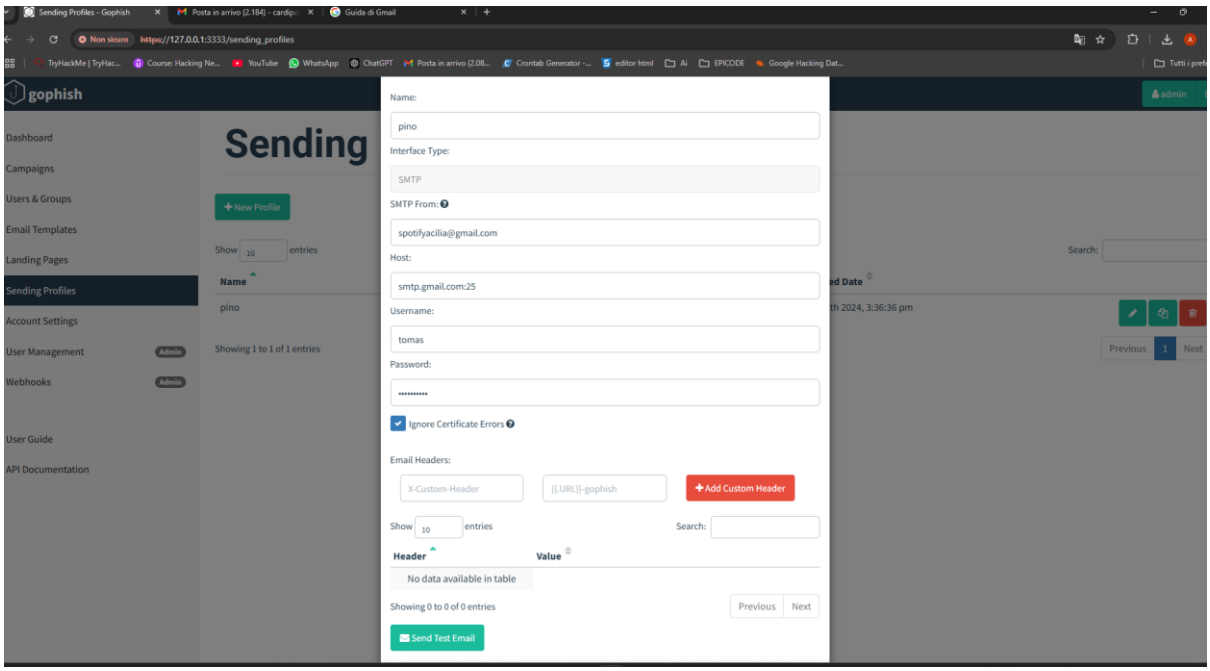
a. Nonostante avessi rimosso l'autenticazione a due fattori sull'account Gmail, il problema persisteva e non sono riuscito a identificare una causa precisa che impedisse l'invio delle email.

3. **Problemi di Rete**:
   a. Durante la configurazione, ci sono stati blocchi di comunicazione tra il server Gophish e i destinatari, che sembravano essere legati alla gestione della rete e alla configurazione dei firewall.

Soluzione Alternativa: Utilizzo di SET

Nonostante i problemi con Gophish, ho deciso di utilizzare **Social-Engineer Toolkit (SET)** per continuare con la simulazione. Questo strumento ha reso il processo di creazione del sito di phishing molto più semplice e rapido, grazie all'uso di un **template preimpostato** che replica il login di Twitter. L'utilizzo di SET mi ha permesso di completare la simulazione senza ulteriori problemi.

1. **Creazione della Pagina di Phishing**:
   a. Con SET, ho potuto generare un sito clonato di Twitter, simile al sito originale. La configurazione è stata rapida e non ha comportato difficoltà significative.
2. **Email di Phishing**:
   a. Una volta configurato il sito di phishing, ho inviato l'email di phishing che indirizzava gli utenti al link falso di login. L'email è stata progettata per sembrare legittima, utilizzando il template creato in precedenza.



Conclusioni

L'uso di Gophish ha evidenziato alcune difficoltà tecniche che non sono riuscito a risolvere, nonostante vari tentativi di configurazione e la rimozione dell'autenticazione a due fattori. Questo ha limitato la possibilità di proseguire con la simulazione utilizzando Gophish.

Tuttavia, l'uso di SET ha permesso di completare la simulazione con successo. La creazione di un sito di phishing e l'invio dell'email sono stati eseguiti senza intoppi, il che dimostra l'efficacia di strumenti alternativi in situazioni in cui si riscontrano difficoltà con Gophish.

Questa esperienza mi ha permesso di comprendere l'importanza di avere più opzioni a disposizione e la flessibilità nell'affrontare problemi tecnici durante l'esecuzione di simulazioni di phishing.