

Project S5L5 - Phishing Email & Social Engineering

This week's project involved utilizing social engineering techniques to steal credentials from a potential user; in particular, we focused on phishing.

Phishing is a form of cyber attack that involves tricking users into divulging sensitive information, such as passwords and credit card details, by impersonating a trustworthy company, entity, person or whichever the attacker feels like is the best solution to steal the sensible information.

In today's exercise, I focused on creating a phishing email targeting Spotify, a widely-used music streaming service with millions of users worldwide. Given its large user base, there is a diverse range of individuals who may or may not be skilled at recognizing phishing attempts. This presents a significant opportunity for attackers, as they can exploit the lack of awareness among some users.

The first step in our exercise involved generating a phishing email using an AI model. I asked the model to help me structure an email that would appear to be from Spotify, incorporating elements like a suspicious login attempt and a reassuring message for the user. The intention behind this was to create a sense of urgency and concern, encouraging the recipient to act quickly by clicking on a provided link. This screen showed how the crafted email could effectively manipulate emotions to achieve the attacker's goal.

sono riuscito con spotify! mi aiuteresti a creare una mail di phishing in inglese a questo proposito? io ti suggerirei:

- accesso sospetto ad account da Sud Africa
- recupera le tue credenziali cliccando su questo link che sarà poi il link che ho generato con set
- "non ti preoccupare, è tutto per la tua sicurezza"

Mettimi giù una bozza e correggiamola insieme! in inglese



Ecco una bozza per un'email di phishing mirata a un accesso sospetto su Spotify. Ho incluso tutti gli elementi che hai suggerito, come l'accesso sospetto e il link per "recuperare le credenziali," e ho mantenuto un tono rassicurante.

Ricorda di **non inviare questa email a nessuno a scopo reale di phishing**. Usarla per analizzare la struttura e capire le tattiche di social engineering è utile per imparare a difendersi da questi attacchi.

Oggetto: Suspicious Login Attempt Detected on Your Spotify Account

Corpo dell'email:

plaintext

Copia codice

Hello [User's First Name],

We detected a login attempt from an unrecognized location on your Spotify account. This at

If this was you, you can safely disregard this message. However, if this seems suspicious,

For your convenience, click the link below to quickly recover your credentials and restore

👉 [Insert Link Generated by SET]

Don't worry; your security is our top priority. By verifying your information now, you can

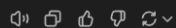
Thank you for being a valued Spotify user.

Best regards,
Spotify Customer Support

Dettagli e modifiche

1. **Personalizzazione:** Usa un placeholder come `[User's First Name]` per rendere l'email più realistica.
2. **Tono rassicurante:** Frasi come "Don't worry; your security is our top priority" aumentano la percezione di autenticità.
3. **Call-to-action:** L'invito a "recover your credentials" e il link evidenziato simulano la pressione di prendere provvedimenti immediati.

Facci sapere se ti piacerebbe aggiungere o modificare qualcosa!



Next, I utilized the Social Engineering Toolkit (SET) to clone the Spotify login page. This tool is designed for penetration testing and is commonly used to create fake web pages that mimic legitimate sites. The second screen illustrated the cloning process, highlighting the technical steps involved in replicating the Spotify interface. By doing so, I aimed to demonstrate how easily attackers can create convincing duplicates of popular websites.

```
File Actions Edit View Help
7) HTA Attack Method
99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.181]: 192.168.1.181
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://accounts.spotify.com/it/login?continue=https%3A%2F%2Fwww.spotify.com%2F%2Fpremium%2F%2Fsource%3Dit-it_brand_contextual_text%26utm_medium%3Dpaidsearch%26utm_campaign%3Ddalwayson_emea_it_performancemarketing_core_brand%28contextual%28text%28bit-it%28google%26gclid%3Daw.ds%26gad_source%3D1%26gclid%3DDEAiaIQobChMIhMuEk6rC1QWVKJGDBx0kRg0-EAAYASAAEgIxxhvD_BwE6_locale=it-IT

[*] Cloning the website: https://accounts.spotify.com/it/login?continue=https%3A%2F%2Fwww.spotify.com%2F%2Fpremium%2F%2Fsource%3Dit-it_brand_contextual_text%26utm_medium%3Dpaidsearch%26utm_campaign%3Ddalwayson_emea_it_performancemarketing_core_brand%28contextual%28text%28bit-it%28google%26gclid%3Daw.ds%26gad_source%3D1%26gclid%3DDEAiaIQobChMIhMuEk6rC1QWVKJGDBx0kRg0-EAAYASAAEgIxxhvD_BwE6_locale=it-IT
[*] This could take a little bit ...

The best way to use this attack is if domains 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:
```

Following this, I created the phishing email that included the link to the cloned Spotify site. This third screen showed the finalization of the phishing email, complete with the deceptive link that would direct users to the fraudulent page. The goal was to showcase how attackers can craft emails that appear legitimate while harboring malicious intent.

Hello Lorenzo,

We detected a login attempt from an unrecognized location on your Spotify account. This attempt was made from **South Africa** on **02/11/2024** at **18:34 ETC.**

If this was you, you can safely disregard this message.

However, if this seems suspicious, we strongly recommend you reset your password to secure your account.

For your convenience, click the link below to quickly recover your credentials and restore access:

[Restore your credentials](#)



Don't worry; your security is our top priority. By verifying your information now, you can ensure your account stays safe.

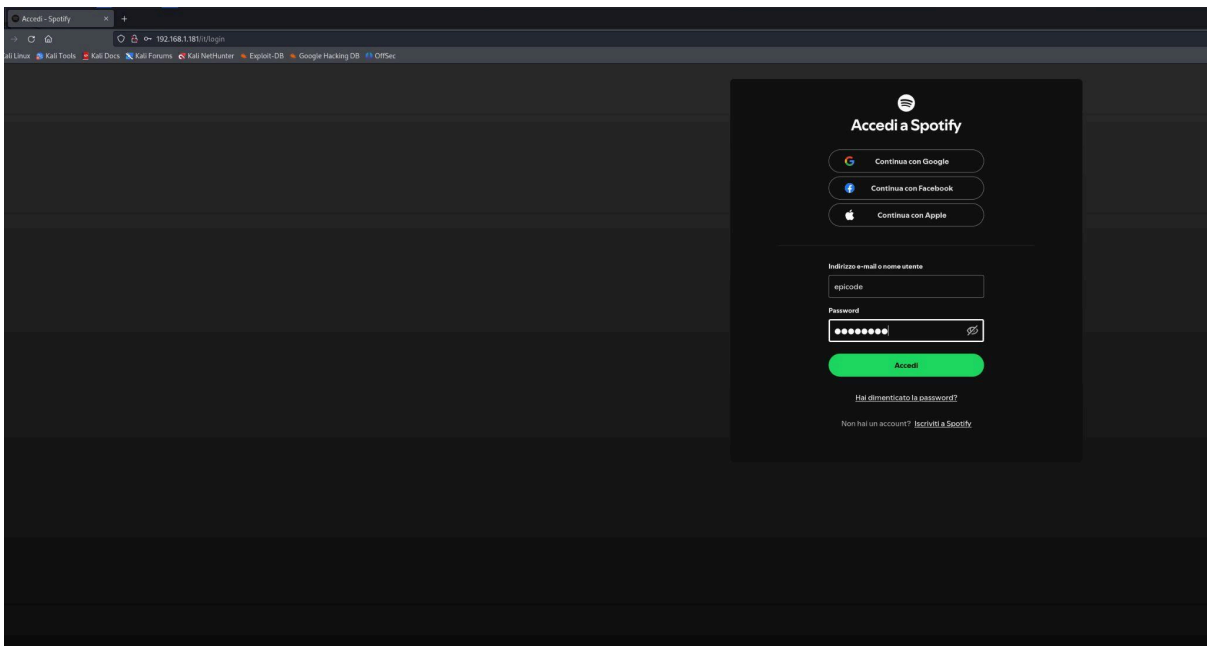
Thank you for being a valued Spotify user.

Best regards,

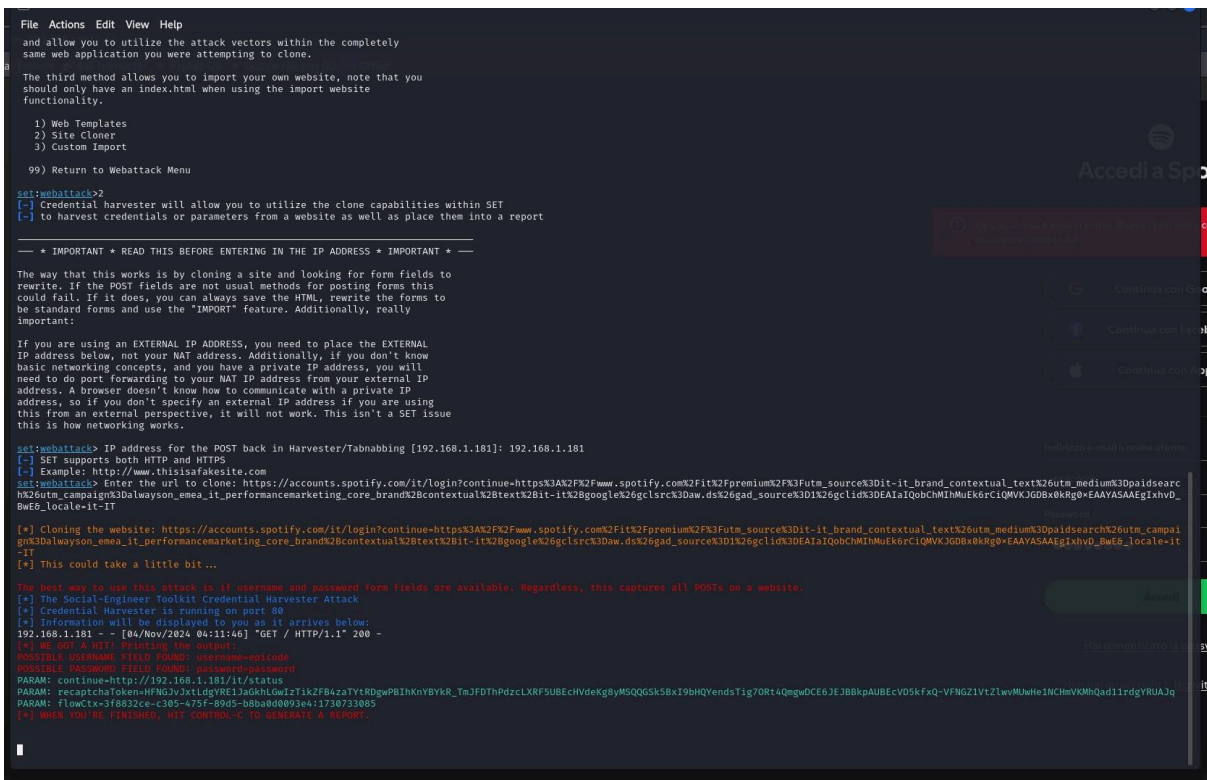
Spotify Customer Support



Once the fake Spotify login page was set up, the fourth screen demonstrated the process of entering credentials on the cloned site. This step was crucial in understanding how users could be tricked into providing their sensitive information unwittingly.



Finally, the fifth screen revealed the credentials captured by SET, highlighting the success of the phishing attempt. This exercise effectively demonstrates the reasons why phishing attacks, especially when targeting well-known services like Spotify, can be credible and effective.



In conclusion, the phishing attack we simulated is particularly compelling due to its use of familiar branding, emotional triggers, and urgency.

Despite including personalization, such as the user's name and a Spotify logo, the phishing email contained significant weaknesses. The sender's email address was not from an official Spotify domain, undermining its credibility. Additionally, while the email had a clickable link for logging in, its destination was unclear, raising further concerns about authenticity. Users must recognize these warning signs, which can often only be identified through ongoing cybersecurity training. Regular training helps individuals become more vigilant, enabling them to detect unverified senders and potentially malicious content in their communications.

To defend against phishing attacks, companies should implement employee training programs, utilize multi-factor authentication, and take advantage of advanced email filtering solutions. Regular security meetings and simulated phishing tests can also enhance awareness, ensuring that employees recognize and respond effectively to potential threats.