Phishing Simulation Report (SET Toolkit)

Objective:

Simulate a phishing attack using the Social Engineering Toolkit (SET) in Kali Linux to demonstrate credential harvesting for awareness training.

Tools Used:

- Kali Linux
- Social Engineering Toolkit (SET)
- Browser (to view cloned phishing page)

Steps Performed:

- 1. Opened SET with: sudo setoolkit
- 2. Chose: 1) Social-Engineering Attacks > 2) Website Attack Vectors > 3) Credential Harvester > 2) Site Cloner
- 3. Entered local IP for POST back.
- 4. Entered 'https://github.com/login' to clone.
- 5. Hosted fake page on local network.
- 6. Shared localhost as phishing link (same network only).
- 7. Collected credentials from terminal logs after interaction.

Result:

- Successfully hosted a cloned phishing page.
- Credential harvesting was functional.
- Demonstrated phishing risk in a simulated, ethical lab environment.

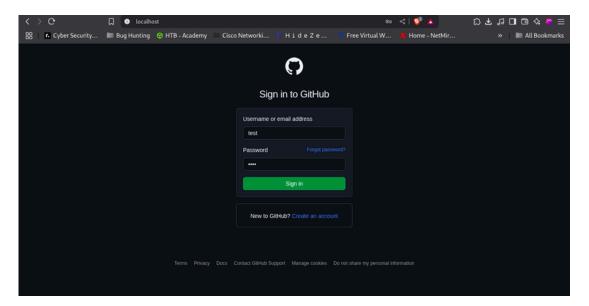
Recommendations:

- Conduct user training on phishing awareness.
- Deploy email filters and web proxies.
- Implement multi-factor authentication (MFA).

Conclusion:

The phishing simulation using SET effectively showcased how easily credentials can be harvested, emphasizing the need for strong user awareness and technical defenses.

Setoolkit Configuration



Cloned Login Page

```
this from an external perspective, it will not work. This isn't a SET issue
this is how networking work.

set'mebatiack> IP address for the POST back in Harvester/Tabnabbing [1]

- SET supports both HTTP and HTTPS
- Example: http://www.thisiasfakesite.com
set:mebatiacko Enter the urt to clone: https://github.com/login

- Coloning the website: https://github.com/login
- This could take a little bit...

The best way to use this attack is if username and passeord form fields are destable, beginning, this captures all POSTS on a website.
- The best way to use this attack is if username and passeord form fields are destable, beginning, this captures all POSTS on a website.
- The best way to use this attack is if username and passeord form fields are destable, beginning, this captures all POSTS on a website.
- The best way to use this attack is if username and passeord form fields are destable, beginning, this captures all POSTS on a website.
- The best way to use this attack is if username and passeord form fields are destable, beginning, this captures all POSTS on a website.
- The best way to use this attack is if username and passeord form fields are destable, beginning to the sound and the second of the passeord form fields are destable, beginning and the destable of the passeord resource and the destable of the passeord passeord resource and the destable of the passeord passeord resource and the passeord passeor
```