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:

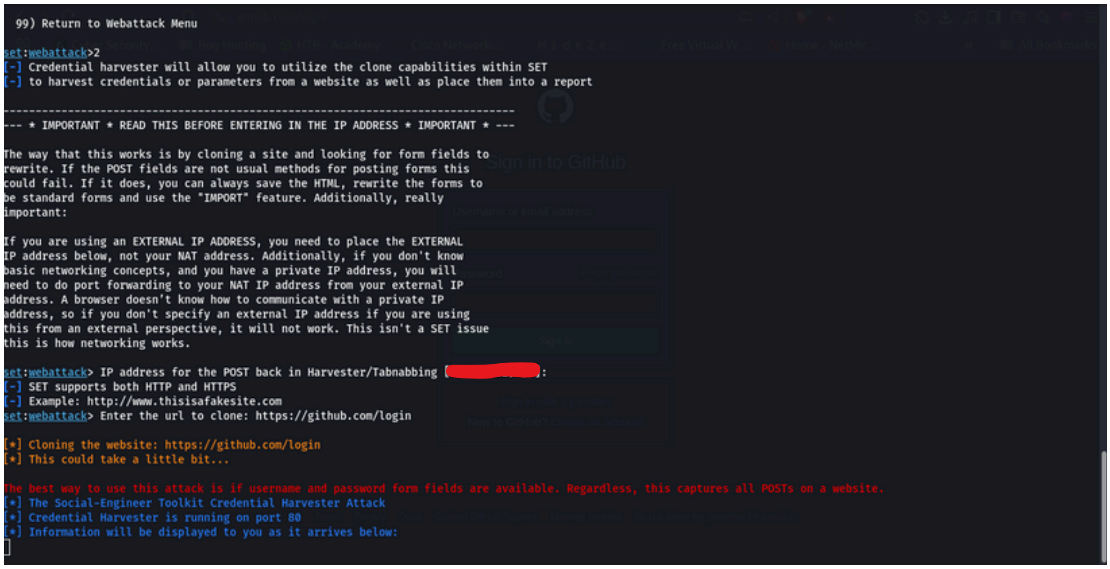
- Successfully hosted a cloned phishing page.
- Credential harvesting was functional.
- Demonstrated phishing risk in a simulated, ethical lab environment.

Recommendations:

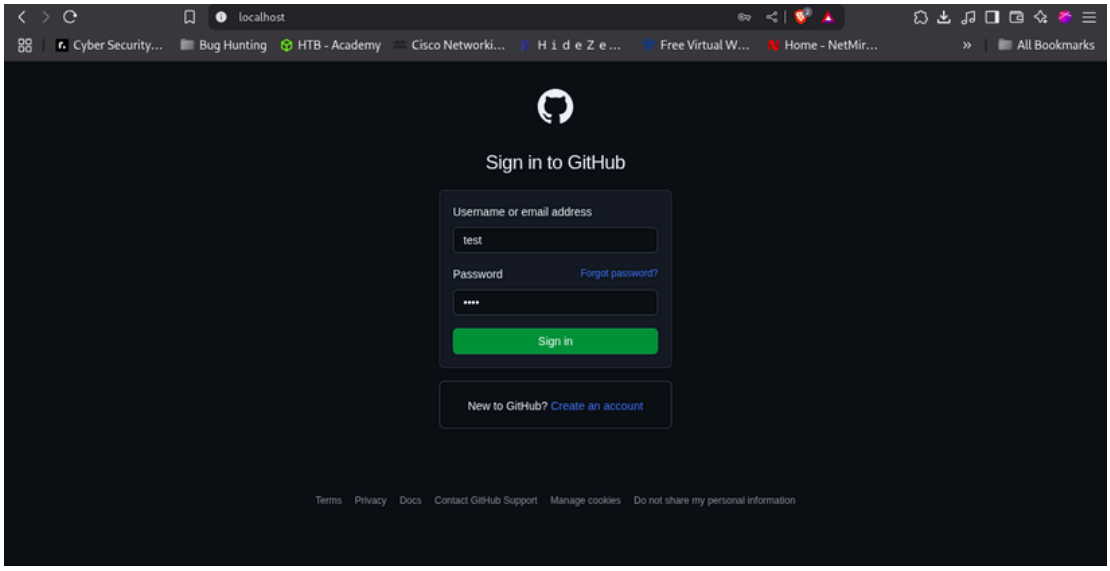
- Conduct user training on phishing awareness.
- Deploy email filters and web proxies.
- Implement multi-factor authentication (MFA).

Conclusion:

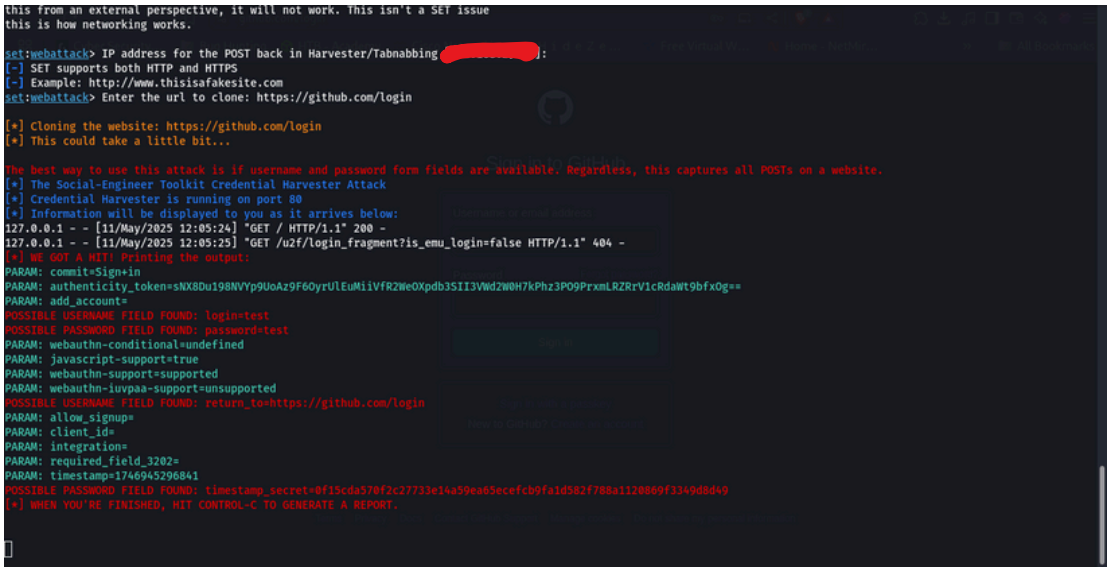
The phishing simulation using SET effectively showcased how easily credentials can be harvested, emphasizing the need for strong user awareness and technical defenses.



Setoolkit Configuration



Cloned Login Page



Credentials Phished