Phishing Simulation Report

Conducted by: [Your Name]

Tool Used: Social Engineering Toolkit (SET)

Platform: Kali Linux (VM)

Date: [Insert Date]

# Objective

To simulate a phishing attack in a controlled environment to understand the tactics used by malicious actors, demonstrate the risk of credential harvesting, and raise awareness about phishing threats within a secure and ethical lab setup.

# Tools & Environment

|  |  |
| --- | --- |
| Component | Description |
| OS | Kali Linux (running in VirtualBox) |
| Tool | SET - Social Engineering Toolkit |
| Target Site | http://testphp.vulnweb.com/login.php (cloned locally for simulation) |
| Network Type | Localhost (192.168.x.x) |
| Simulation Scope | Private lab environment only |

# Methodology

1. Launching SET:  
 sudo setoolkit  
  
2. Attack Vector Selection:  
 - [1] Social-Engineering Attacks  
 - [2] Website Attack Vectors  
 - [3] Credential Harvester Attack Method  
 - [2] Site Cloner  
  
3. Cloning Target Website:  
 - Target: http://testphp.vulnweb.com/login.php  
 - SET cloned the login page locally  
 - Harvested credentials from simulated input  
  
4. Testing the Link:  
 - Hosted page at: http://192.168.1.21 (local IP)  
 - Accessed from another browser/device in the same network  
 - Entered test credentials:  
 - Username: testuser  
 - Password: password123  
  
5. Result Observed in Terminal:  
 [\*] WE GOT A HIT!  
 [\*] Username: bharatgupta@gmail.com  
 [\*] Password: FUTUREINTERN\_CS@

# Simulation Results

|  |  |
| --- | --- |
| Metric | Count |
| Pages Cloned | 1 |
| Credentials Submitted | 1 (Simulated) |
| Phishing Link Accessed | ✅ Successfully accessed on LAN |
| Email Spoofing Sent | ❌ Not included (optional step) |

# Ethical Scope

✅ This simulation was executed entirely within a private virtual lab.  
❌ No real users, emails, or external targets were involved.  
✅ The cloned site was accessed only on the local IP address.

# Key Learnings

- Credential harvesting simulations are powerful tools for security awareness training.  
- Even a simple cloned login page can deceive users if not trained.  
- Ethical hacking must always be confined to permitted environments.

# Recommendations

- Implement email filtering and anti-phishing software  
- Train employees to recognize social engineering tactics  
- Use Multi-Factor Authentication (MFA) to reduce risk  
- Conduct regular phishing simulation exercises with tools like Gophish or SET

# Attachments (Optional)

- Screenshots of terminal  
- Image of cloned page  
- Sample phishing email (if crafted)