# Social Engineering Toolkit (SET) Script Documentation

## Purpose of the Scripts

The Social Engineering Toolkit (SET) is an open-source framework designed for social engineering attacks. The provided scripts automate tasks like launching the SET interface, setting up spear phishing attacks, and configuring credential harvesting attacks. These scripts streamline the process of deploying social engineering techniques, making them accessible and efficient for security assessments.

The first script, Launch SET Interactive Mode, starts SET in interactive mode, allowing users to navigate its menu for various attack vectors. The second script, Automated Spear Phishing Attack, configures and initiates a spear phishing campaign using SET. The third script, Credential Harvester Setup, automates the setup of a credential harvesting attack by cloning a target website.

## Usage Instructions

### General Setup

1. Install the Social Engineering Toolkit by following the instructions from its official GitHub repository:
2. sudo apt install set
3. Ensure Python is installed on your system.
4. Run the scripts as a user with sudo privileges, as SET often requires elevated permissions.

### Script 1: Launch SET Interactive Mode

#### Command:

python launch_set_interactive.py

### Script 2: Automated Spear Phishing Attack

#### Command:

python spear_phishing_attack.py

#### Required Parameters:

- ✓ None. Prompts for required inputs during execution.

## Script 3: Credential Harvester Setup

### Command:

python credential_harvester_setup.py

### Required Parameters:

- ✓ target_url: The URL of the website to clone (e.g., http://example.com).

# Expected Outputs or Results

### Launch SET Interactive Mode

- ✓ Starts the SET console in interactive mode, displaying its main menu for manual navigation and execution of attacks.

### Automated Spear Phishing Attack

- ✓ Configures and launches a spear phishing attack with user inputs, such as the email template and recipient addresses.
- ✓ Displays progress and success messages in the terminal.

### Credential Harvester Setup

- ✓ Sets up a fake website that looks like the target URL.
- ✓ Outputs the location of the cloned site and starts listening for user credentials entered into the fake site.

# Dependencies Needed

- ✓ Social Engineering Toolkit (SET): The core tool used for executing social engineering attacks.
- ✓ Python: Required to run the scripts.
- ✓ Subprocess Module: Used for interacting with SET from the command line.

# Line-by-Line Explanation

## Launch SET Interactive Mode

```
import subprocess
```

- subprocess: Used to run system commands from Python.

```
def launch_set_interactive():
```

- Defines a function to start SET in interactive mode.

```
print("Launching Social Engineering Toolkit...")
subprocess.run(["sudo", "setoolkit"])
```

- Prints a message indicating that SET is starting and executes the setoolkit command with sudo privileges.

## Automated Spear Phishing Attack

```
import subprocess
```

- subprocess: Used to interact with SET commands programmatically.

```
def spear_phishing_attack():
```

- Defines a function to configure and launch a spear phishing attack.

```
commands = [
    "use social-engineering",
    "1",  # Social Engineering Attacks
    "2",  # Website Attack Vectors
    "3",  # Credential Harvester Attack Method
    "1",  # Web Templates
    "http://example.com",  # URL to clone
    "run"
]
subprocess.run(["sudo", "setoolkit"], input="\n".join(commands) + "\n", text=True)
```

- Constructs the SET menu navigation commands to configure the phishing attack.
- Runs the commands within the SET framework.

### Credential Harvester Setup

```
import subprocess
```

- subprocess: Used to run system commands from Python.

```
def credential_harvester_setup(target_url):
```

- Defines a function to set up a credential harvesting attack for a specified target URL.

```
commands = [
    "use social-engineering",
    "1",  # Social Engineering Attacks
    "2",  # Website Attack Vectors
    "3",  # Credential Harvester Attack Method
    "2",  # Site Cloner
    target_url,
    "run"
]
subprocess.run(["sudo", "setoolkit"], input="\n".join(commands) + "\n", text=True)
```

- Constructs and executes the commands to configure a credential harvesting attack by cloning the specified target website.

## Why These Scripts Are Needed ?

The provided scripts simplify the use of the Social Engineering Toolkit by automating repetitive tasks and configurations. The Launch SET Interactive Mode script ensures that users can easily access the full functionality of SET without needing to type commands manually. The Automated Spear Phishing Attack script provides a streamlined way to test phishing campaigns, which are a common vector in real-world attacks. The Credential Harvester Setup script facilitates the creation of realistic-looking phishing pages, enabling organizations to test the effectiveness of their security awareness training and identify weaknesses in their defenses.