1. Install Required Software

Before starting, ensure the necessary software is downloaded and properly installed.

- **Nuclei**: Open-source vulnerability scanner.
  - Download: https://github.com/projectdiscovery/nuclei/releases
- **Metasploitable**: A deliberately vulnerable virtual machine for testing.
  - Download: https://sourceforge.net/projects/metasploitable/
- **VirtualBox** or **VMware**: To host Metasploitable as a virtual machine.
  - VirtualBox: https://www.virtualbox.org/
  - VMware: https://www.vmware.com/

2. Setting Up Metasploitable Virtual Machine

1. **Install and Configure VirtualBox/VMware**:
   - Follow the installation instructions for your chosen virtualization tool.
2. **Import Metasploitable Image**:
   - Open VirtualBox or VMware.
   - Select **"Import Appliance"** or **"Open Virtual Machine"**, then locate the Metasploitable file downloaded.
3. **Start Metasploitable VM**:
   - Launch the virtual machine to run the vulnerable environment.
   - Note down the IP address of the VM (e.g., 192.168.x.x) by logging in with:
     - Username: msfadmin
     - Password: msfadmin
   - Use the ifconfig command to find the IP and make sure they are in NAT network.

3. Install and Set Up Nuclei

1. **Download Nuclei**:
    - Follow the link above to download and extract Nuclei binaries for your operating system.
2. **Add to PATH (Optional)**:
    - Ensure the Nuclei executable is accessible via the terminal/command line by adding it to your system's PATH variable.
3. **Install Templates**:
    - Open a terminal and run:

    ```
    nuclei -update-templates
    ```

    - This downloads the latest vulnerability scanning templates, including CVE-based and custom YAML templates.

4. Create and Use Custom Templates

1. **Write Your YAML Templates**:
    - Navigate to the `nuclei-templates` directory.
    - Create custom templates (e.g., for SQL injection) using this structure:

    ```
    id: custom-sqli
    info:
      name: Custom SQL Injection
    ```

```
  severity: high
  author: yourname
requests:
  - method: GET
    path:
      - "{{BaseURL}}/vulnerable/endpoint?param=1'"
    matchers:
      - type: word
        words:
          - "SQL syntax error"
```

2. **Save Templates**:
   - Save the file as custom-sqli.yaml in the nuclei-templates directory.
3. **Run Scans with Custom Templates**:
   - Use the following command to scan Metasploitable for vulnerabilities:

```
nuclei -u http://<Metasploitable-IP> -t nuclei-templates/custom-sqli.yaml
```

5. Performing Scans on Metasploitable

1. **Run Basic Scans**:
   - Use prebuilt templates for scanning common vulnerabilities:

```
nuclei -u http://<Metasploitable-IP>
```

2. **Specify Templates**:
   - Run specific vulnerability checks, such as for SQL injection or weak authentication:

```
nuclei -u http://<Metasploitable-IP> -t nuclei-templates/<template-name>.yaml
```

3. **Save Scan Results**:

    - Store scan results in a file for review:

    ```
    nuclei -u http://<Metasploitable-IP> -o results.txt
    ```