Introduction to Penetration Testing Tools

Part 1: Installing Kali Linux

Steps to Install Kali Linux:

1. **Download the Kali Linux ISO**
   - Visit the official Kali Linux website and download the appropriate ISO file for your system (Virtual Machine version if using virtualization software).
2. **Set Up Virtualization Software**
   - Install **VMware Workstation Player** or **VirtualBox**.
   - Create a new virtual machine and allocate the following resources:
     - **Memory:** At least 2 GB (4 GB recommended).
     - **Storage:** 20 GB of hard disk space.
     - Attach the Kali Linux ISO as the virtual machine's boot disk.
3. **Install Kali Linux**
   - Start the virtual machine and follow the guided installation process:
     - Select **Graphical Install** for a user-friendly experience.
     - Configure settings like language, keyboard layout, and hostname.
     - Set up a user account and password.
     - Partition the disk and complete the installation.
4. **Update and Configure Kali Linux**
   - After installation, update the system with the following command:

     ```
     sudo apt update && sudo apt upgrade -y
     ```

- Verify the installation of default tools using the **Kali menu**.

Part 2: Exploring Penetration Testing Tools

Tool 1: Burp Suite

1. **Installation:**
    - Burp Suite is pre-installed in Kali Linux. If not, install it using:

      ```
      sudo apt install burpsuite
      ```

2. **Configuration:**
    - Open Burp Suite and set up the **proxy listener** (default is localhost:8080).
    - Configure your browser to use Burp Suite as a proxy.
3. **Basic Exercise:**
    - Use Burp Suite to intercept and analyze HTTP requests.
    - Steps:
        - Open Burp Suite and enable the **Intercept** tab.
        - Navigate to a website in your browser configured with the Burp proxy.
        - Observe the intercepted requests and explore options like modifying headers.

Tool 2: Metasploit Framework

1. **Installation:**
    - Pre-installed in Kali Linux. Update it with:

      ```
      sudo apt update && msfupdate
      ```

2. **Configuration:**
    - Start Metasploit by typing:

```
msfconsole
```

3. **Basic Exercise:**
    - Perform a basic exploit simulation:
        - Search for an exploit using the `search` command, e.g., `search vsftpd`.
        - Use the exploit with `use <exploit-path>`.
        - Set the target using `set RHOST <target-IP>`.
        - Run the exploit using the `exploit` command.

Tool 3: Nmap

1. **Installation:**
    - Pre-installed in Kali Linux. If not, install it with:

    ```
    sudo apt install nmap
    ```

2. **Basic Exercise:**
    - Scan a network to discover devices and open ports:

    ```
    nmap -sS -A <target-IP>
    ```

        - `sS`: Performs a SYN scan.
        - `A`: Enables OS detection and version scanning.
    - Review the scan results, noting open ports and services.

Part 3: Documentation

Tool	Installation Process	Configuration	Basic Exercise
Burp Suite	Pre-installed or `apt install`	Configure proxy settings, enable intercept mode	Intercept and analyze HTTP requests.

Metasploit	Pre-installed or `msfupdate`	Start Metasploit with `msfconsole`	Simulate an exploit with a chosen vulnerability.
Nmap	Pre-installed or `apt install`	No configuration needed. Run directly via CLI.	Scan networks, identify open ports and services.

Hands-On Summary

- The hands-on exercises provided an understanding of reconnaissance and scanning tasks.
- **Burp Suite** enabled us to analyze web traffic effectively.
- **Metasploit** demonstrated how to simulate controlled attacks.
- **Nmap** facilitated network exploration and vulnerability identification.

By mastering these tools, we can build a strong foundation in penetration testing.