# 13.3.9 Mobile Device Hacking Facts

Mobile devices have become a necessity in today's business world. Because mobile devices can be compromised in many ways, it is important that both users and network administrators adhere to security best practices in the use and security management of these devices. Security management includes the installation of apps to protect mobile devices. Network administrators should also conduct penetration testing.

This lesson covers the following topics:

- Mobile security best practices
- Mobile device protection tools
- Penetration testing processes
- Penetration testing strategies
- Penetration testing tools

## Mobile Security Best Practices

Security best practices should be practiced by both users and network administrators. The following table lists some of these best practices.

| Employee Type | Best Practice |
|---|---|
| User | Users should follow these best practices to secure mobile devices:<br>▪ Limit the number of applications on a mobile device.<br>  ▪ Unused apps take up storage space.<br>  ▪ More apps mean more vulnerabilities.<br>  ▪ Updates are more likely to be applied with fewer apps installed.<br>▪ Don’t auto-upload photos to social networks.<br>  ▪ Uploaded photos are a privacy concern.<br>  ▪ Photos have geotags that can be used to track movements.<br>▪ Maintain configuration control and management.<br>  ▪ Identify, document, and control the changes that are made to mobile phone settings and applications.<br>  ▪ Keep the operating system and applications up to date by installing the latest updates.<br>  ▪ Encrypt the storage on the device.<br>▪ Have a plan in case the phone is lost or stolen.<br>  ▪ Use a passcode.<br>  ▪ Enable remote management.<br>  ▪ Set up remote wipe.<br>  ▪ Back up and synch your device often.<br>▪ Don’t root or jailbreak to override the mobile device’s built-in security. |
| Administrator | Administrators should follow these best practices:<br>▪ Publish use policies for mobile devices.<br>  ▪ Publish an acceptable use policy for mobile devices that connect with the network. Write the policy to apply to mobile devices supplied by the organization and bring-your-own devices.<br>  ▪ Specify network data mobile devices can access.<br>  ▪ Publish a policy of cloud usage for mobile apps that connect to cloud resources and cloud data storage.<br>  ▪ Implement a policy that clearly defines the apps that are allowed on mobile devices that connect to the network.<br>▪ Enable antivirus on mobile devices to protect the data in your datacenter.<br>▪ Enforce mobile access gateway authentication and specify a session timeout to close access when the device is inactive for a length of time. |

## Mobile Device Protection Tools

Ensure that mobile devices that connect to the network have security apps installed. Examples of mobile device protection tools available include the following:

- Lookout Personal is a mobile app that provides mobile security, identity protection, and theft prevention.
- Zimperium’s zIPS app is a mobile intrusion prevention system. zIPs:
  - Analyzes the behavior of a mobile device through the operating system’s statistics, memory, CPU, and other parameters.
  - Identifies attacks and gives you the who, what, where, when, and how information of the attack event.
- Bullguard Mobile Security includes antivirus, antitheft, parental control, and mobile security manager features.
- Malwarebytes detects and removes malware and ransomware. It provides real-time protection and anomalous behavior detection, as well as conducting a privacy audit and report of apps that track.

## Penetration Testing Processes

Processes for penetration testing mobile devices include:

| Process | Description |
|---|---|
| Footprinting | Use scanning tools such as nmap to locate mobile devices attached to your network. These tools often return the OS version and type. |
| Scanning | Use software such as Kismet to identify the wireless networks the devices are looking for. |
| Exploitation | Use man-in-the-middle attacks, spoofing, ARP poisoning, and traffic insertion attacks to exploit client-side vulnerabilities. Also, manipulate captured traffic to exploit backend servers. |
| Inspect mobile data | Inspect data areas on the mobile device for sensitive information. Use forensic tools for mobile phones to look for SMS and browser history databases and extract information from these databases. |

## Penetration Testing Strategies

Penetration testing strategies change depending on the operating system an organization uses.

| Type | Strategy |
|---|---|
| Android | A good strategy for penetration testing an Android phone is to follow these steps:<br>1. Attempt to root the Android phone using tools such as Kingo Android Root and TunesGo Root Android Tool.<br>2. Use tools like LOIC and AnDOSid to perform denial-of-services and distributed-denial-of-service attacks.<br>3. Investigate vulnerabilities in the Android browser by checking for a cross-application-scripting error. Hackers use this vulnerability to break down the browser's sandbox using infected JavaScript code.<br>4. Check for unencrypted email passwords and Skype contacts that have been stored in the SQLite database.<br>5. Use the APSET tool to exploit the Android Intents system to gain the user's private information. Android Intents is a messaging system that Android apps use to request functionality from other Android components.<br>6. Use Co Checker and IntentFuzzer to detect capability leaks in the Android device. |
| Android | Follow these steps to penetration test an iPhone:<br>1. Attempt to jailbreak the iPhone using Cydia, Anzhuang, or other jailbreaking tools.<br>2. Use a tool like iPhoneSimFree to unlock the iPhone.<br>3. If the iPhone has a smart cover that both wakes the iPhone and puts it to sleep, try these steps to bypass the password code security:<br>a. Hold the power button until the power off message appears.<br>b. Close the smart cover.<br>c. Wait for the screen to shut down.<br>d. Open the smart cover and press the Cancel button.<br>4. Try to access the iPhone by sending malicious code as a payload using the Metasploit tool.<br>5. Use other Metasploit features to attack the iPhone.<br>6. Try spoofing a Wi-Fi connection by creating a wireless access point with the same name and encryption type as the connection stored in the iPhone.<br>7. Intercept the wireless parameters from the iPhone and use the information to perform man-in-the-middle and SSL stripping attacks.<br>8. Send malicious packets using the Cain and Abel tool. |

## Penetration Testing Tools

Consider adding these mobile penetration tools to your toolkit:

- Hackode is a free Android app that is available on Google Play. The full name of the app is Hackode: Hacker's Toolbox. Hackode:
  - Performs reconnaissance using whois and Google hacking, also referred to as Google dorking.
  - Uses utilities such as ping, traceroute and DNS dig to scan devices.
  - Provides security feed modules.
- The zANTI app is available on Google Play. zANTI:
  - Has more features than Hackode, but to use those features, the app must run on a rooted Android device.
  - Scans a network to identify connected devices. It provides the properties and vulnerabilities of those connected devices.
  - Simulates real-world exploits and mobile attack techniques.
  - Sends email reports about devices and collected data at regular intervals.