EC-Council Licensed Penetration Tester

Methodology: Mobile Devices Penetration Testing

Penetration Tester:			
Organization:			
Date:		**Location:**	

Penetration Testing Android-based Devices

Test 1: Try to root an Android phone

Target Organization	
URL	
Rooting Process in Andriod Phone	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 2: Try to install malicious apps without user's approval

Target Organization	
URL	
Installing Malicious Apps without User's Approval	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3: Perform a DoS attack on Android phone

Target Organization	
URL	
DoS Attack on Andriod Phones	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 4: Check for vulnerabilities in the Android browser

Target Organization	
URL	
Cross-Application-Scripting Present in the Browser	1. 2. 3. 4. 5.
JavaScript Code is Infected to Break Down Web Browser	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 5: Check for vulnerabilities in SQLite

Target Organization	
URL	
How Email Password are Stored as Plain text	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 6: Check for vulnerabilities in intents

Target Organization	
URL	
Obtain the User's Privacy Information by Using Intent in Andriod Phone	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 7: Check for Android Wi-Fi vulnerability

Target Organization	
URL	
Accessing a user's Personal Information through an Unencrypted Wi-Fi Connection	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 8: Use the "Woodpecker" tool to detect capability leaks in Android devices

Target Organization	
URL	
How to Detect Capability Leaks in Android Devices	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Penetration Testing iOS-based Devices

Test 1: Try to Jailbreak the iPhone

Target Organization	
URL	
JailBreaking iPhone	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 2: Try to Unlock the iPhone

Target Organization	
URL	
Remove SIM Restrictions from the iPhone	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3: Try to Activate the Voicemail Button on Your Unlocked iPhone

Target Organization	
URL	
Activate Voicemail on the Unlocked iPhone	1. 2. 3. 4. 5.
Tap the Voicemail button to Enable Customary Voicemail Services	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 4: Try to Bypass the Smart Cover

Target Organization	
URL	
Smart Cover can be Exploit and Bypassing the Protective Shield	1. 2. 3. 4. 5.
Gaining Access to last used Application	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 5: Exploit Siri to Get Unauthorized Access

Target Organization		
URL		
Find Siri is enabled and Locked	☐ Yes	☐ No
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 6: Try to Hack the iPhone Using Metasploit

Target Organization	
URL	
Exploit the Vulnerabilities in iPhone by using Metasploit	1. 2. 3. 4. 5.
Checking the iPhone's web browsing history	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 7: Check for an Access Point with the Same Name and Encryption Type

Target Organization	
URL	
Accessing Malicious Access Points	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 8: Check iOS Device Data Transmission on Wi-Fi Networks

Target Organization	
URL	
Attacking Data Transmission Layers of an iOS Device	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 9: Check Whether the Malformed Data Can Be Sent to the Device

Target Organization	
URL	
Social Engineering Techniques can be used to Track User Activities	1. 2. 3. 4. 5.
Sending the Malicious Code to Access user Personal Information	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 10: Check for Code Signing Vulnerabilities on iOS Devices

Target Organization	
URL	
Executing Arbitrary Code on an iOS Device	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 11: Check Whether Hardware Encryption/Backup Recovery Can Be Done

Target Organization	
URL	
Protecting with Multilayer Security Levels with Encryption keys and Hardware Encryption	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Penetration Testing BlackBerry-based Devices

Test 1: Try Blackjacking on the BlackBerry

Target Organization	
URL	
Blackjacking BlackBerry-based Devices	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 2: Perform a Metaspolit Exploit with Blackjacking

Target Organization	
URL	
Verifying the BBproxy Handshake	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3: Try IDS Evasion on the BlackBerry Enterprise Network

Target Organization	
URL	
Creating an Outbound Network Connection from a BlackBerry	1. 2. 3. 4. 5.
Monitoring and Controlling by the Malicious host	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 4: Perform DNS Spoofing

Target Organization	
URL	
Infecting a Target DNS Server with Trojans	1. 2. 3. 4. 5.
Monitoring and Controlling the DNS Server Communications	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 5: Check for Flaws in the Application Code Signing Process

Target Organization	
URL	
Creating a fake Applications	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 6: Use Trojans to Extract Information

Target Organization	
URL	
Extracting Information by sending Malicious Trojans or Bugs on BlackBerry Devices	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 7: Perform a DoS Attack

Target Organization	
URL	
Basic Protocol transmition of Data between BlackBerry Devices and the BlackBerry Server	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 8: Check for Vulnerabilities in the BlackBerry Browser

Target Organization	
URL	
Executing Malicious Code to retrieve Personal Information	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 9: Check for Flaws in Attachment Services

Target Organization	
URL	
Corrupting the memory on BlackBerry Devices	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 10: Try to Attack by Sending TIFF Image Files

Target Organization	
URL	
Heap Overflow Vulnerability in the BlackBerry	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 11: Search for Password-protected Files in BlackBerry Devices

Target Organization	
URL	
Recovering Password-Protected Files, and Backups from BlackBerry Devices	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Penetration Testing Bluetooth Connections

Test 1: Check Whether the PIN can be Cracked

Target Organization	
URL	
Establishing Communication with other Bluetooth Devices using a Pairing	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 2: Try to Perform a Blueprinting Attack

Target Organization	
URL	
Attacking Bluetooth-Enabled Devices Remotely	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3: Check Whether You Are Able to Extract the SDP Profiles

Target Organization	
URL	
Extracting the Service Discovery Protocol	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 4: Try Pairing Code Attacks

Target Organization	
URL	
Pairing Process of Bluetooth Device by using Eavesdropping	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 5: Try a Man-in-the-Middle Attack

Target Organization	
URL	
Gaining an Access to Link Keys and Unit Keys by Performing Man-in-the-Middle Attack	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 6: Try a Bluejacking Attack

Target Organization	
URL	
Sending Unsolicited Messages to Bluetooth-Enabled Devices	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 7: Try a BTKeylogging Attack

Target Organization	
URL	
Finding out the Fixed PIN code and Bluetooth Device Address	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 8: Try BlueSmacking - The Ping of Death

Target Organization	
URL	
Generating and Sending a Large Data Packets for Attack	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 9: Try a Bluesnarfing Attack

Target Organization	
URL	
Exploiting the Weaknesses Found in a Bluetooth Connection	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 10: Try a BlueBug Attack

Target Organization	
URL	
Exploiting the loopholes in the Bluetooth-Enabled Devices to gain access of the devices	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 11: Try a BlueSpam Attack

Target Organization	
URL	
Intercepting the Connections by Sending Spam Messages	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 12: Try Denial-of-Service Attacks

Target Organization	
URL	
Exchanging Binary Objects Between Devices that relies on OBEX Protocol	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis: