

CORE Impact for Mobile Device Testing

Assess Mobile Device Security Before Attackers Do

With CORE Impact[®] Pro Mobile Device Penetration Testing, you can demonstrate the exploitability of iPhone[®], Android[™] and BlackBerry[®] smart phones using the same attack techniques employed by criminals today.

CORE Impact Mobile Penetration Testing capabilities assess device security and end-user security awareness through the following real-world attack techniques:

Phishing

- Replicate email and text-based phishing attacks
- Determine whether employees would click through to malicious sites and/or install nefarious mobile apps
- Assess security awareness by recording each user's clicks
- Assess device security by launching actual attacks designed to run on or against the target devices

Web Form Impersonation

- Assess data leakage threats by conducting phishing tests seeded with links to web forms
- Capture and record user-entered data, such as usernames and passwords

Fake Wireless Access Points

- Impersonate valid wireless access points
- Gather profile information about connected devices
- Launch appropriate attacks when the device or user requests Internet data from the access point

Wireless Man-in-the-Middle (MITM) Attacks

- Identify and monitor wireless networks with no encryption or WEP-based encryption
- Intercept and relay wireless transmissions between connected devices and the legitimate access point
- Insert attacks that attempt to target connected devices

The CORE Impact Pro Mobile Device Penetration Test

CORE Impact's mobile device penetration test capabilities speed the testing process, automate mundane tasks, and provide a repeatable assessment methodology for measuring mobile device security over time.

1. Attack and Penetration: Exploit devices using real-world techniques

One of the most effective ways for an attacker to take control of a mobile device is by getting the user, or the device itself, to install a malicious application. During phishing tests, you trick the user into clicking on a link and triggering the attack. For Wi-Fi tests, Impact delivers attacks in response to data requests (fake AP attacks) and inserts them into existing traffic (MITM attacks).

Key Benefits

- Identify and prove critical data breach exposures created by mobile devices in your environment
- Evaluate the security of new mobile technologies prior to deployment
- Get actionable data required to mitigate financial, operational and reputational risks
- Assess end-user security awareness of social engineering techniques
- Protect end users from defamation, fraud and blackmail
- Audit and report on mobile device security to executive management and other stakeholders

Assess Mobile IT Security without Sacrificing Device Integrity or Stability

Since 2001, CORE Impact has been designed to test your security posture in the safest and most stable way possible.

- Impact is built in-house by professional researchers, engineers, exploit writers and QA testers
- Mobile attack capabilities are designed to maximize target stability and leave no backdoors that could be exploited at a later time
- Impact exploits are continuously run through rigorous QA tests, using a combination of automated testing processes and close personal inspection
- No new security vulnerabilities are created during testing; Impact simply finds the weak points that already exist in tested devices

Next Steps

CORE Impact Pro allows you to proactively test the security of network systems, web applications, endpoint systems, email users, mobile devices and wireless networks. Learn more by contacting us today to schedule a demonstration.

Attack Delivery

- Email phishing attacks are launched directly from Impact
- SMS text phishing attacks are launched from Impact via an email-to-SMS gateway service
- Wi-Fi attacks are delivered via Impact's integration with the AirPcap[®] TX Wireless Packet Capture Adapter from Riverbed Technology (sold separately)

Device Penetration

Impact's mobile attacks are packaged as applications that attempt to run locally on the mobile device. In addition, some attacks attempt to leverage known vulnerabilities in the device's operating system or built-in components, leveraging those weaknesses to run the application. All Impact attack capabilities are developed and tested in-house, are designed to maximize the target stability and integrity, and are updated as new vulnerabilities emerge and attackers hone their techniques.

2. Evidence Retrieval: Demonstrate the implications of a mobile device breach

With CORE Impact Pro, you not only can demonstrate how mobile devices in your environment can be compromised, but also reveal how attackers can access and manipulate device data.

Extract data

Once you compromise a tested device, Impact Pro enables you to extract data from the device just as an attacker would. Impact enables you to extract the following data types:

- Phone call, SMS and MMS logs
- GPS location
- Contact information

Take snapshots

You can also take and retrieve snapshots using the mobile device's camera, providing additional evidence of the compromise.

3. Reporting: Gain actionable data to address critical exposures

Impact Pro generates the following reports to assist in vulnerability remediation and fulfill security assessment documentation requirements:

- **Mobile Device Reports** record information on all mobile devices accessed during testing
- **Executive Reports** provide a high-level overview of test findings
- **Client-Side Reports** present the results of security awareness assessments
- **Vulnerability Reports** detail vulnerabilities exploited and provide links to remediation information
- **Activity Reports** provide audit trails of all targeted devices and conducted tests
- **Delta Reports** compare the results from tests repeated over time
- **Attack Path Reports** graphically depict the path followed to target and exploit specific devices