

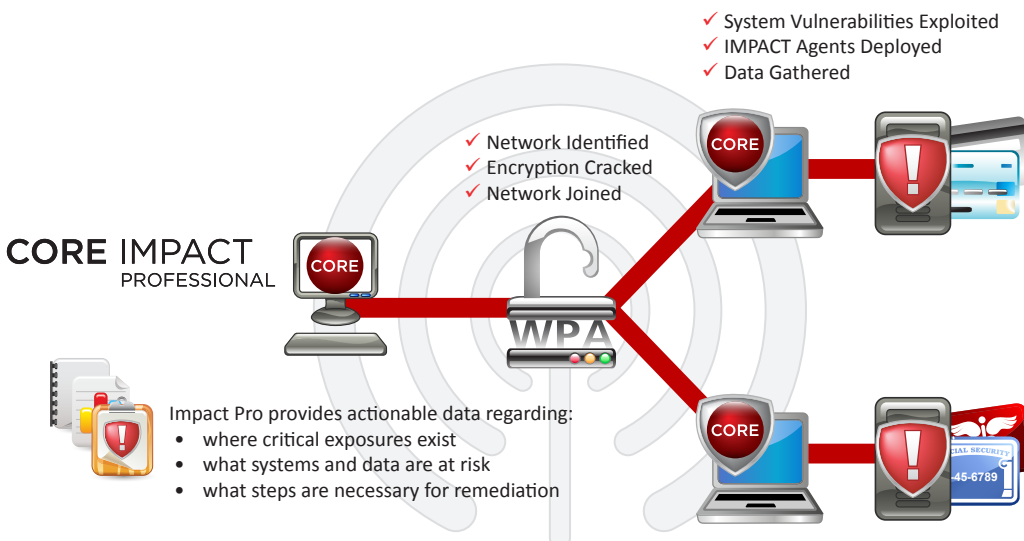
CORE Impact for Wireless Network Testing

Gauge Your Organization's Exposure to Wi-Fi Threats

CORE Impact Pro's wireless penetration testing capabilities enable you to assess your organization's readiness against real-world attacks originating over Wi-Fi networks. With CORE Impact, you proactively replicate the actions of a would-be attacker to reveal exploitable weaknesses in your wireless and backend networks – gaining actionable data at each step for efficient and effective risk mitigation.

Wireless penetration testing capabilities in CORE Impact Pro include:

- Discovery of both known and unauthorized Wi-Fi networks and access points
- Identification of devices interacting with the network
- Information gathering on network strength, security protocols and connected devices
- Attack and penetration of networks encrypted with WEP, WPA-PSK and WPA2-PSK
- Man-in-the-Middle (MITM) attack replication
- Beaconing machine detection
- SSID impersonation
- Automated traffic sniffing for finding streams of sensitive data
- Capabilities for joining cracked networks and testing backend systems
- Comprehensive reporting of wireless testing activities and findings
- Seamless pivoting between wireless, network, web application and endpoint tests, replicating multi-staged attacks that trace chains of vulnerabilities to sensitive backend data



Gain Actionable Information for Improving Wireless Security and Protecting Backend Resources

- Pinpoint exploitable Wi-Fi weaknesses that extend beyond the walls of your organization
- Identify unauthorized networks
- Replicate the steps an attacker would take after gaining entry to the network
- Exploit OS, service and application vulnerabilities in backend system connected to exposed networks
- Identify sensitive data, escalate privileges, and determine the true implications of a breach
- Harvest email addresses from exposed systems for use in CORE Impact phishing tests
- Gain access to backend web applications and pivot to Impact web application testing
- Generate reports for efficient remediation and maintain audit trails for compliance initiatives
- Benchmark and measure changes in your security posture over time

CORE Impact Pro allows you to replicate multistaged attacks that leverage compromised systems to target backend resources, revealing how chains of exploitable vulnerabilities can open paths to mission-critical systems and data.

Wireless use has exploded in business and attackers have found many vulnerable WLANs to exploit.

Enterprises need to make sure their vulnerability assessment processes incorporate WLAN technologies into both continuous monitoring and periodic penetration testing.

- John Pescatore
Distinguished Analyst, Gartner

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.

Wireless Penetration Testing with CORE Impact requires the use of an AirPcap TX Wireless Packet Capture Adapter from CACE Technologies. A discount is available for CORE Impact customers.

Identify Known and Unauthorized Wireless Networks

Many organizations have policies against unauthorized Wi-Fi networks. Impact's discovery capabilities allow users to identify both authorized networks and unauthorized points of access. It then profiles any networks discovered by analyzing signal and packet data to measure network strength, determine security protocols, and identify devices interacting with the network.

Crack WPA, WPA2 and WEP Encryption

CORE Impact Pro determines keys by taking advantage of known vulnerabilities in WEP-secured networks. The solution also assesses networks secured by WPA and WPA2 (using a Pre-Shared Key) via dictionary attacks that leverage information from sniffed authentication attempts.

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

Man-in-The-Middle (MITM) attacks involve attackers discretely intercepting transmissions from one or more Wi-Fi users and then acting as a relay, often inserting their own, malicious content as a way to gain sensitive information. Impact Pro offers a straightforward, wizard-based interface to simulate MITM attacks and illustrate the risk resulting from a Wi-Fi breach.

Detect Beaconsing Machines

Wireless cards on certain operating systems scan for, or beacon, default SSIDs that the machine had previously been connected to and will connect to an access point without the user's involvement. If IMPACT Pro locates any such machine, it will attempt to learn its MAC address and the SSID (network name) for which it is probing.

Impersonate SSIDs

Building off of the ability to detect beaconsing machines, Impact Pro can impersonate a valid access point and attempt to have the machine connect to it. Once a machine is connected to Impact Pro's fake access point, the testing potential broadens considerably and users are able to harvest information from the system, insert exploits into traffic to and from the system, manipulate network traffic, and execute local and network attacks.

Trace Attack Paths to Backend Systems and Data

Only CORE Impact offers true multistaged penetration testing capabilities, allowing users to replicate attacks that can occur after the initial Wi-Fi network compromise. By integrating wireless assessments with web application, network and endpoint testing, Impact reveals and documents paths of exposure to sensitive data residing on backend systems.

Share Actionable Data for Efficient Remediation

CORE Impact Pro generates reports of wireless networks discovered, client-to-access point relationships, and access point profile information. Reports also include information about which networks were tested against attacks, which were successfully compromised, and which weaknesses allowed the compromise.