



Core Impact 2017 R1 Technical Datasheet





Contents

Solution and Vendor Background	3
Deployment Requirements	4
Interface	4
Network Penetration Testing	5
Web Application Penetration Testing	10
Client-Side Penetration Testing	13
Wireless Network Penetration Testing	14
Mobile Device Penetration Testing	15
Reporting	16
Training and Support	18



Solution and Vendor Background

Core Impact is the most comprehensive multi-vector solution for assessing and testing security vulnerabilities throughout your organization. Leveraging commercial-grade exploits, users can take security testing to the next level when assessing and validating security vulnerabilities. Core Impact is a product that is built and supported by Core Security. The current version in the market is Core Impact 2017 R1.

Core Security provides companies with the security insight they need to know who, how, and what is vulnerable in their organization. The company's threat-aware, identity & access, network security, and vulnerability management solutions provide actionable insight and context needed to manage security risks across the enterprise. This shared insight gives customers a comprehensive view of their security posture to make better security remediation decisions. Better insight allows organizations to prioritize their efforts to protect critical assets, take action sooner to mitigate access risk, and react faster if a breach does occur.

Core Impact was introduced into the market in 2002. Since then, Core Impact currently has over 1000 installations with 50 plus employees dedicated to research and development of the solution. Core Impact has always been developed in-house at Core Security by experienced researchers, exploit writers and engineers.

Core Impact is the only solution that develops and tests 100% of all exploits in house. Core Impact also supports running a 3rd party security product's exploits. Core Security's exploit library is put through a rigorous quality assurance process every week by a dedicated team to ensure our products will not have unpredicted or ancillary effects on tested systems, processes or users. These QA specialists operate independently from our threat research and development groups, and their sole responsibility is to examine every exploit and protect our customers from any unanticipated results from their testing work. Prior to adding any new exploits to our products, the code is examined to eliminate or reduce the likelihood of negative interactions between exploits and tested systems. Our QA process also ensures that when customers run Core Impact's post-test clean-up feature, no active exploit code or functionality is left behind and no backdoors are created.

Some of Core Impact's exploits do have the potential to interrupt system processes based on the nature of the attacks they emulate. However, users are specifically prompted to ensure that they understand the implications of their work. Core Security's product engineers have gone to great lengths to make certain that our exploits won't unexpectedly effect processes or interrupt services. Core Security exploits are built to recreate the same "slow and low" conditions that many of today's attacks have adopted to hide from defensive security technologies.

Impact typically receives 10+ new exploits and other security testing modules per month. The product typically receives two major version upgrades per year, which include the addition of major functionality to increase the product's breadth and depth of testing capabilities.



Deployment Requirements

You can run Core Impact on any Windows system with the following minimum specifications:

- Intel Core 2 Duo, 2.8 GHz or faster
- 4GB RAM minimum (8GB RAM recommended)
- 4GB free hard disk space (space requirements increase with the quantity of workspaces)
- A Windows-compatible Ethernet networking card. Core Impact works with wireless network interface cards
- Internet Explorer 9.0 or later
- Screen resolution: 1024 x 768 minimum (1280 x 1024 recommended)

Core Impact is certified on the following platforms: (on physical hardware or VMware based virtualized hardware)

- Windows 7 Ultimate SP1 64bit
- Windows 7 Professional SP1 64 bit

Core Impact is supported on the following platforms:

- Windows 7 Ultimate SP1 64bit
- Windows 8.1 Enterprise 64 bit
- Windows 10 Enterprise 64 bit
- Windows 10 Pro 64 bit
- Windows Server 2008 R2 SP1
- Windows Server 2012
- Windows Server 2012 R2

Core Impact can be installed and running in 30 minutes or less.

Interface

Core Impact offers multiple methods of working with the product for different users:

- **Wizard-driven RPTs**, which automate all steps of the pen testing process
- **Manual capabilities**, allowing users to programmatically interact with specific exploits and other modules for more granular control
- **One-step testing**: “set it and forget it” capabilities for running network, client-side and web application tests including Vulnerability Scanner Validation
- **Automatic, scheduled testing**: run one-step tests on a repeated basis
- **Macros**, allowing users to automate custom testing workflows
- **Module customization**: All modules are written in Python and are user-customizable
- **Module creation**: Users may also write their own Python exploits and other modules, which Core Impact can then integrate into the testing process
- **Teaming**: Core Impact allows for groups to each use their local copies of Core Impact to view the same data and perform actions as a team



Network Penetration Testing

Core Impact uses a variety of techniques to accurately identify and profile target systems within an IP range. This discovery can occur directly from Core Impact or from any machine that has been compromised by Core Impact.

Core Impact's network discovery and port scanning methods include ARP, Fast TCP, Fast SYN, ICMP, mDNS (Bonjour), Passive, CA BrightStor, UPnp, TCP Connect, Nmap OS Stack fingerprinting and more.

Core Impact can import and validate results from many of the leading vulnerability scanners on the market, including:

- Acunetix® Web Security Scanner
- Retina Network Security Scanner
- GFI LANguard™
- HP WebInspect
- IBM Enterprise Scanner®
- IBM Internet Scanner®
- IBM AppScan®
- Beyond Security AVDS
- Portswigger BurpSuite
- McAfee® Vulnerability Manager
- TripWire IP360®
- Rapid7 AppSpider
- Rapid7 Nexpose
- Qualys QualysGuard®
- SAINTscanner®
- Tenable Nessus®
- Tenable Security Center®
- Patchlink VMS
- Trustwave AppScan®
- NMap

Core Impact includes OS, services and application exploits designed to target vulnerabilities on the following platforms:

- AIX
- Linux
- Mac OS X
- OpenBSD
- Sun Solaris
- Windows



Using Core Impact, tests can be conducted to test the structure of IPv6 systems and access the security of IPv6 systems using exploits to expose vulnerabilities.

The Information Gathering step of Core Impact's Network Rapid Penetration Test (RPT) locates and profiles (attempts to get as much information as possible) any assets found on your network. It will then correlate this information to the relevant assets and then present them as potential targets for attack.

Core Impact also has unique functionality around discovering and profiling network devices. This can be done automatically through the Network Information Gathering RPT, or you can identify targets via Core Impact's Passive CDP network discovery module, which listens for broadcasts from Cisco devices. In either case, if Core Impact is able to discern the operating system of a target and confirm it to be a network device, it will attempt to gather additional information:

- Identify and fingerprint devices to determine manufacturer, device model/type, and operating system details
- Determine the inputs on which the device accepts connections or instructions, including SNMP, Telnet, HTTP, etc.
- Discover broadcasting devices

Core Impact's attack modules reveal exposed devices via dictionary attacks that attempt to guess usernames and passwords to gain access to the device – replicating a common technique employed by actual attackers.

If Core Impact is able to gain access to a network device, it will create an Agent¹ with which you can demonstrate risks to the network that occur subsequent to the initial compromise. Since making material changes to a switch or router's configuration can disrupt users and networks, Core Impact can demonstrate a breach without interrupting a device's operation via the following non-aggressive modules:

- **Get Configuration:** This module attempts to retrieve the configuration file of the device and optionally try to crack any passwords that are in use
- **Set Device Name:** With this module, Core Impact can rename the network device. This won't disrupt the operation of the device, but it can be an eye-opening display of its vulnerability to malicious attacks
- **Interface Monitoring:** This module takes advantage of a legitimate monitoring feature included in many switches, enabling the tester to demonstrate how attackers could intercept copies of data packets
- **Access List Piercing:** This module compromises a router's network visibility filtering, allowing the Core Impact user to access networks that were previously off-limits
- **IOS Shell:** This module will open a shell and allow you to interface with the network device
- **Cisco IOS Agent:** This module attempts to create a Telnet connection whereby testers can make changes on the device. The change(s) made in order to achieve this connection are recorded and can then be reverted using the Cisco IOS Agent - Privilege Escalation Clean Up module

¹ This Agent represents the steps of how to breach the device and does not represent code on the target device.



When targeting databases, either when exploiting a vulnerability or by using weak credentials, Core Impact will install a SQL Agent, which allows direct interaction with the target database (called a SQL Shell). Also, these agents support post-exploitation modules aimed at extracting information about the target database schema, users, instances, searching for SSN or credit card numbers, etc.

As of April 2017 Core Impact supports SQL Agent for the following database servers:

- DB2
- MSSQL
- MySQL
- Oracle
- PostgreSQL

As of April 2017, Core Impact includes ~3,800+ exploits, such as remote exploits, local privilege escalation exploits, and denial of service exploits. Because Core Impact exploits support several targets for exploitation (e.g., versions and service packs), the product offers an increased chance of attacks being successful. Combining Core Impact's unique exploit count with the multiple targets supported by our individual exploits, the solution covers 14,000+ unique exploit combinations. The former numbers do not include dynamically generated exploits that Core Impact creates during Web Application Penetration Testing.

Core Impact is updated automatically on a weekly basis via the internet. An offline update option is available as well. Customers typically receive 10+ exploits and other security testing modules per month.

Core Impact's network exploits are written in Python and are customizable by the user. Users can also leverage Core Impact to run their own exploits written in Python. Exploit payloads must have a minimal footprint on tested systems. Core Impact deploys agents into the memory of targeted system, ensuring that your penetration tests are minimally invasive and safe for compromised systems. Agent code is typically smaller than most emails, and no additional application code needs to be deployed on the compromised system.

Every Core Impact agent provides an interface to the compromised system, allowing you to gather additional information, escalate access privileges or attempt to compromise other network resources. The interface is easy to use, providing common access across all target platforms and eliminating the need to write different scripts for each platform. Capabilities include:

- Browse file structures and view file contents on compromised machines
- View rights obtained on compromised machines
- Take screenshots
- Interact with compromised machines via command shells
- Gather passwords and cookies



Unique Syscall Proxying technology enables you to leverage agents to access any system call or Windows API on a compromised system.

Core Impact complements Syscall Proxying with additional functionality to support binary plug-ins and to execute arbitrary binary code on the target system, such as payloads dynamically created in runtime or as part of a customized exploit.

Core Impact supports the following connection methods:

- Connect To Target
- Connect From Target
- Reuse Connection
- HTTP/s Connect From Target
- DNS tunneling

The connection method is defined when the exploit is executed. Agents can also be chained together to reach network resources with limited connectivity.

Payloads deployed by Core Impact perform an authentication check to confirm they are connecting to the copy of Core Impact that deployed them. Core Impact authenticates to the agent ensuring there are no MiTM attacks being leveraged.

All communication between Core Impact and any deployed payload (regardless of communication protocol) are encrypted by default.

With persistent agents, it's simple to maintain contact with a targeted workstation, even if compromised client software is restarted.

As of April 2017, Core Impact includes 210+ Privilege Escalation exploits that can be run locally on compromised systems in an attempt to gain root or SYSTEM access.

Core Impact's patented Syscall Proxying technology enables users to run any module—including all exploits, information gathering, privilege escalation, and pivoting -- through an agent installed on the target machine (or a chain of agents). All remote code execution exploits deploy an agent on the target machine, hence pivoting is guaranteed (some specific Information Gathering modules would require system/root privileges on the agent, and therein lays the importance of Local exploits).

Core Impact currently supports pivoting on the following operating systems:

- AIX
- Linux
- Mac OSX
- OpenBSD
- Sun Solaris
- Windows



Core Impact offers the Remote Network Interface functionality (a.k.a. VPN Pivoting), which enables users to extend the reach of other external tools (such as other security testing applications) to any system compromised during testing – whether that system is the first to be exploited by Core Impact or last in a chain of compromised systems.

- **Windows and Linux support:** Core Impact can establish VPN pivot points on both Windows and Linux targets
- **Run any third-party application through VPN pivots:** Core Impact allows users to leverage VPN tunnels to run any application against compromised systems, for instance:
 - Email client, using credentials during a Core Impact client-side penetration test to access internal email accounts
 - Web browser to view and interact with internal web applications
 - Vulnerability scanner to identify additional threats on the local machine and backend network

Core Impact includes a unique automated Clean-Up wizard to remove the agents that have been installed during testing. Memory resident OS Agents deployed will be automatically uninstalled when Core Impact disconnects from them (either immediately or after their Reconnection Policy ² expires), even without the Clean- Up wizard. Upon closing a workspace, the user is prompted to uninstall the agents and other modules or keep them running. All clean-up activities are logged, providing an audit trail. If an agent loses connection with Core Impact, the agent can attempt to reconnect with Core Impact for a defined period of time before removing itself from the system.

Core Impact supports Reflective DLL Injection and Dynamic Forking in order to upload and execute DLL and EXE files respectively and is included in most of the modules that require file upload on Windows targets.

Core Impact has the capability to attempt to brute-force accounts on target systems to determine if weak or default credentials have been used for each service.

Core Impact supports testing over the following protocols:

- DB2
- FTP
- HTTP
- MSSQL
- MySQL
- Oracle
- POP3
- PostgreSQL
- Rlogin
- RDP
- RTSP
- SMB
- SMTP
- SNMP
- SSH
- Telnet
- VMware Auth/HTTP
- VNC

²Core Impact has the ability to establish a reconnection policy for the agents that are deployed.



For each protocol, Core Impact has a specific set of default and common username and password lists. These lists can be easily augmented with user provided accounts and passwords. Core Impact also provides the ability to use partial (e.g. a username) or complete identities gathered by other modules and include them in the groups of credentials to test.

Core Impact can communicate securely (encrypted with mutual authentication) with a hosted password-cracking service (CloudCypher) and pass any Windows NTLM hashes found to the service. CloudCypher performs a time bounded series of tests to determine if an attacker would be able to determine the plaintext password for the hashes in a reasonable amount of time. The resulting plaintext passwords are then passed back to Core Impact for further reuse during the test.

Core Impact allows testing teams to identify whether a host on their network is a camera and tests for vulnerabilities and authentication weaknesses. If access is achieved, the team can view the camera's video feed, take a still shot of the video feed, or access the camera's administration interface. Testing video cameras can be done using the RPT wizards, or manually using the included modules.

Core Security and ExCraft Labs partner to deliver enhanced SCADA exploits for Core Impact. The SCADA pack targets over 168 exploits in various SCADA systems deployed across many industries. This enhanced pack is updated with about 5 new exploits on average per month. Because ExCraft developed these exploits on the Core Impact platform, they can be leveraged in tandem with all the Core Security developed exploits thus allowing a comprehensive approach to test and validate SCADA systems.

Core Impact has the capability to re-test vulnerabilities found within a workspace for verification. The Remediation Validation functionality takes a workspace as an input, tries to exploit the vulnerabilities found within that workspace, and reports the differences between the original workspace and the new one automatically.

Web Application Penetration Testing

With interactive web crawling, Core Impact captures pages for testing either by providing a URL to be crawled automatically or by manually interacting with the web application. The user can specify the maximum number of pages to process and the maximum depth to crawl, as well as restrict crawling to a specific domain and specify a browser to impersonate.

Core Impact supports the following authentication mechanisms for web crawling:

- Form based
- HTTP Authentication
- SSL Client Authentication (including CAC)
- WS Security (for Web Services)
- RecordLogin(AssistedLogin)/CaptchaSupport

Hosts discovered during network testing may have HTTP servers running, which can be an indicator that they are hosting WebApps. Core Impact can evaluate those hosts and attempt to identify web pages.



Core Impact can import and validate results from many of the leading vulnerability scanners on the market, including:

- Acunetix
- HP WebInspect
- IBM AppScan
- Rapid7 AppSpider
- Qualys Web Application Scanner

Core Impact offers crawling capabilities that enable it to discover and assess dynamic pages that run JavaScript code in the browser.

Core Impact provides testing capabilities that address the following OWASP Top 10 web application vulnerabilities:

A1: Injection

- SQL Injection: Safely identify both traditional and blind SQL injection vulnerabilities and dynamically create and inject SQL queries in an attempt to access the database.
- OS Command Injection: Detects and exploits OS Command Injection weaknesses in web applications and reveals the implications of a breach by taking control of the web server.

A2: Broken Authentication and Session Management

Core Impact will test for known/default credentials at the target systems. Core Impact users can customize the dictionaries used.

A3: Cross-Site Scripting (XSS)

Core Impact's XSS capabilities include Adobe Flash objects crawling, as well.

A4: Insecure Direct Object References

Core Impact uncovers hidden, backup and old pages in applications, and analyzes "robots.txt" files to reveal admin pages and other sensitive URLs.

A5: Security Misconfiguration

Core Impact will run a network vulnerability test to detect weak credentials in the exposed services. It will also test the presence of WebDAV vulnerabilities.

A6: Sensitive Data Exposure

- Insufficient Transport Layer Protection: SSL Strength Module allows testers to flag weak levels of encryption in HTTPS-secured sites.
- Sensitive Information in documents and databases: These two tasks will be carried out trying to find credit card numbers, SSN, etc. at the target application.

A7: Missing Function Level Access Control

Failure to Restrict URL Access: Access admin, backup and old pages via authenticated and unauthenticated sessions.

A8: Cross-Site Request Forgery (CSRF)

Identify CSRF weaknesses in web applications and replicates CSRF attacks to demonstrate exploitability.



A9: Using Known Vulnerable Components

Performs a network vulnerability test against the target trying to exploit network vulnerabilities.

A10: Unvalidated Redirects and Forwards

Identifies applications that redirect and forward without proper validation and demonstrates how an attacker could redirect victims to malicious sites.

To test web applications against both Local and Remote File Inclusion (RFI) attacks on PHP applications, Core Impact dynamically manipulates PHP templates in an attempt to retrieve commands from a remote web server. If successful, the manipulation is recorded as an RFI Agent, which allows interaction with the targeted web application.

Core Impact's Cross-Site Scripting capabilities are able to target dynamic Flash content in addition to static HTML applications.

Four primary web application attack techniques include capabilities for assessing the ramifications of a web app breach:

SQL Injection

Once the web app testing engine gains access to a Microsoft SQL Server, Oracle or DB2 server, Core Impact enables testers to run several modules to replicate the actions of an attacker (depending on the access achieved), including:

- Install a Core Impact OS Agent
- Check for sensitive information (e.g., credit card numbers)
- Get Database Logins
- Get Database Schema
- Open a commandshell
- Open a SQL shell

OS Command Injection

Building on its existing SQL Injection and Blind SQL Injection capabilities, Core Impact can now detect and exploit OS Command Injection weaknesses in web applications. If the application utilizes user-input variables in system-level commands, Core Impact can attempt to change those variables in a way that causes the system to download a Core Impact Agent, giving the security tester control over the system.

Cross-Site Scripting

After identifying a reflected XSS vulnerability, Core Impact enables testers to send an email message and a specially crafted hyperlink that leverages a XSS Agent to determine if it is possible to compromise the end user's system via their web browser. A successful compromise would allow the tester to install an OS Agent on the victim machine and pivot to a network penetration test to assess the security of the backend network.



Remote File Inclusion

A successful RFI exploit will allow testers to install an OS Agent on the web server, open a PHP shell, or open a command shell, giving the tester access to Core Impact's full network penetration testing capabilities.

Core Impact supports detecting SOAP and REST Web Services. The latter is more effective when using the interactive web crawler capabilities. Once the web services are detected, the RPT Attack and Penetrate phase will try to find SQL Injections and OS Command Injection vulnerabilities. Successful attacks will install agents on the target systems. Core Impact also supports the interactive crawling of a mobile application Web Services backend. This is done by configuring a mobile device to use Core Impact as a proxy. During normal usage of the mobile application, Core Impact will harvest the requests being made on the server and use these requests as a baseline to the target specific backend web services.

Core Impact has the capability to re-test vulnerabilities found within a workspace for verification. The Remediation Validation functionality takes a workspace as an input, tries to exploit the vulnerabilities found within that workspace and reports the differences between the original workspace and the new one automatically.

Client-Side Penetration Testing

Email Address Gathering

Core Impact's Client-Side Information Gathering capabilities can automatically harvest email addresses to target from various sources, including:

- Online public records using Google, Yahoo, AltaVista, Bing, Metacrawler, Ask, and About
- Public Internet databases including PGP, DNS, and WHOIS
- Website crawling
- LinkedIn

Users can import a list of addresses to target in CSV or TXT format.

Sensitive Data Gathering


Core Impact includes capabilities for identifying credit card and/or social security numbers exposed by your user community – both on websites and in documents posted online. You can also define custom search patterns to identify other types of sensitive data.

Information Gathering via Web Bugs

Core Impact allows users to insert web bugs during Client-Side Penetration Testing. When the Word document is opened by an email recipient, the web bug connects back to Core Impact and transmits information about the endpoint system and its outbound connectivity.

Core Impact offers testing capabilities across most common applications including:

- Web Browsers (Internet Explorer, Firefox)
- Mail Clients (Incredimail, Outlook Express, Lotus Notes, Thunderbird)
- Image Viewers (Adobe Reader, Apple QuickTime, IrfanView)
- Media Applications (CoolPlayer, MPlayer, Windows Media Player, VLC Media Player, uTorrent)

- 
- IM Applications (MSN Messenger, Yahoo Messenger)
 - WinVNC, WinRAR, WinZip
 - MS Office (Access, Excel, Outlook, Publisher, and Word)
 - PDF Readers

Core Impact agents can be packaged and registered into binary (.exe) files, gzip/zip attachments, Excel files, PDFs and other file types for sending via email. Agents can also be packaged as VBA scripts for embedding as macros into MS Office documents. For USB drives, Core Impact creates a file-resident OS Agent, then writes it to a USB drive and creates an autorun.inf file to allow execution.

Core Impact can host a web server and serve agents as executable attachments and as executable within gzip/zip attachments. The Web Forms Impersonation feature also allows security testers to clone a form from a legitimate website (including graphics and input fields), serve it locally, and then email end-users a link to the false page, simulating a real-world phishing email attack. Core Impact then records and reports how many times the link was clicked and what data (if any) was entered into the spoofed web form.

Core Impact users can assess security awareness among email users without attempting to compromise their systems. This capability tracks and reports on clicks by recipients of Core Impact generated phishing emails without testing for vulnerabilities.

Each client-side exploit can install an agent that enables the user to leverage the compromised endpoint machine as a beachhead from which to launch additional attacks against the backend network using Core Impact's network penetration testing capabilities.

Wireless Network Penetration Testing

The discovery capabilities in Core Impact 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 involved network.

Note: For some particular Wireless Penetration Testing use cases, Core Impact requires the use of an AirPcap TX Wireless Packet Capture Adapter from CACE Technologies. A 15% discount is available for Core customers. In order to create a Fake Access Point using Core Impact, you must use a Pineapple Tetra, Nano or Mark V (<http://www.hak5.org>) wireless network auditing tool.

Core Impact 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.

If connected to a wireless network, Core Impact can attempt to insert itself into an ongoing transmission over that network. Even when not connected to a wireless network, Core Impact can sniff for client requests and attempt to send its own replies.



Core Impact can scan a wireless environment for end-user machines with powered-on wireless NICs. If left at their default configurations, wireless cards on certain operating systems scan, or send probe requests, for default SSIDs that the machine had previously been connected to and will connect to any access point with that name -- without the user's involvement. If Core Impact locates any such machine, it will attempt to learn its MAC address and the SSID (network name) for which it is probing.

Building off of the ability to detect beaconing machines, Core Impact can impersonate a valid access point and attempt to have the machine connect to it. Once a machine is connected to the imposter access point, the testing capabilities broaden considerably and users are able to:

- Fingerprint connected machines
- Attempt infrastructure attacks on the machine
- Attempt to harvest usernames and passwords
- Insert exploits into traffic sent and received by the connected machines
- Manipulate the user's network traffic
- Execute any tests available in the network attack vector


Mobile Device Penetration Testing

Core Impact conducts tests to exploit Android™, iPhone® and BlackBerry® smartphones such as:

- Identifying and proving critical data breach exposures created by mobile devices in your environment
- Evaluating the security of new mobile technologies prior to deployment
- Obtaining actionable data required to mitigate financial, operational, and reputational risks
- Assessing end-user security awareness of social engineering techniques
- Protecting end users from defamation, fraud, and blackmail
- Auditing and reporting on mobile device security to executive management and other stakeholders

Core Impact's Mobile Penetration Testing capabilities use the following real-world attack techniques:

- **Phishing:** Core Impact enables you to send emails and texts that determine whether your organization's employees would fall prey to phishing and spear phishing attacks by clicking through to malicious sites and/or installing nefarious mobile apps. You can assess security awareness by simply recording each user's clicks and stop there – or extend the test to assess device security by either launching actual attacks against their device or tricking them into installing a fake application.
- **Web form impersonation:** Core Impact allows you to assess data leakage threats by conducting phishing tests designed to capture and record user-entered data, such as usernames and passwords.
- **Fake wireless access points:** Core Impact can impersonate valid wireless access points in an attempt to trick users into connecting their devices to them. The software can then gather profile information about the connected devices and launch appropriate attacks when the device or user requests Internet data from the imposter access point.

- 
- **Wireless man-in-the-middle (MiTM) attacks:** Core Impact identifies and monitors wireless networks that have either no encryption or WEP-based encryption and observe any connected devices. The solution can then intercept and relay wireless transmissions between the device and the legitimate access point, while inserting attacks that attempt to target the device.

Core Impact speeds up the testing process, automates mundane tasks, and provides a repeatable assessment methodology for measuring mobile device security over time.

- **Attack and Penetration:** 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 to click on the link thereby triggering the attack.
- **Evidence Retrieval:** Demonstrate how mobile devices in your environment can be compromised, but also reveal how attackers can access and manipulate device data to obtain your organization's intellectual property and potentially defraud, defame or blackmail its end-users.
- **Reporting:** Generates reports to assist in vulnerability remediation and fulfill security assessment documentation requirements

The included Android agent allows a user to interact with the compromised Android device in various ways:

- Shell Access
- Get/SendSMS
- Make a phone call
- Contact CRUD
- Calls loginfo
- Geo-location/line number info
- Upload/download files

Reporting

Core Impact incorporates the following report data and is also able to export the data in XML format for use in centralized security databases:

- **CVE numbers:** Common Vulnerabilities and Exposures (CVE) are unique identifiers for publically known vulnerabilities. Core Impact reports CVE numbers for vulnerabilities that are successfully compromised during testing.
- **CVSS ratings:** The Common Vulnerability Scoring System (CVSS) represents a universal standard for rating the severity of known vulnerabilities. Core Impact includes CVSS ratings for vulnerabilities that are successfully compromised during testing.
- **CPE:** Common Platform Enumeration (CPE) is a structured naming scheme for IT systems, platforms and packages. Core Impact reports the CPE for systems identified and exploited during penetration testing.



Core Impact offers a wide range of customized reports, including:

- **Executive Summary Report** - Offers a high-level, aggregated view of penetration tests, vulnerabilities, and remediation efforts.
- **Attack Graph Report** - Presents a powerful visual representation of how tests are able to exploit individual vulnerabilities and achieve subsequent access to other systems and applications.
- **PCI Vulnerability Validation Report** - The PCI Vulnerability Validation Report provides Payment Card Industry (PCI) Data Security Standard penetration testing results.
- **Network Wellness Report** - This report indicates the amount of testing that was performed and indicates which tests resulted in a vulnerability being found on the selected targets. The Wellness Report details all exploits attempted, not just successful exploits.
- **FISMA Exploited Vulnerabilities Report** - Provides results of penetration testing performed by government entities and other organizations working to remain compliant with the Federal Information Security Management Act of 2002 (FISMA).
- **Delta Report** - Synthesizes a wide range of testing results for an integrated view of vulnerabilities across various assets, including network systems and client systems.
- **Web Application Vulnerability Report** - Comprehensive information about every security flaw that can be successfully exploited during penetration testing, including those available to SQL Injection, Cross-Site Scripting and Remote File Inclusion attacks.
- **Web Application Executive Report** - Summary of every vulnerable web page found during testing and how those problems can be exploited by real-world attackers.
- **Network Host Based Activity Report** - Provides detailed information about all the modules that were against each host, including relevant data that organizations might need to share with auditors reviewing their security programs.
- **Network Report** - This report provides detailed information about hosts found and vulnerabilities successfully exploited by Core Impact during this test could be found in this report. Each one of the reported vulnerabilities was actively exploited in order to obtain control, elevate privileges or obtain information about the vulnerable asset. None of these results are potential; all of them were practically tested as part of this assessment.
- **Network Vulnerability Report** - Provides users with specific details about all the weaknesses successfully exploited during penetration testing and how those flaws can be used by attackers to obtain control of a tested system and establish a beachhead for subsequent activity.
- **Client-Side Penetration Test Report** - Results of assessments performed on endpoints and end users, including social engineering tactics utilized to trigger tests.

- **Client-Side User Report** - Helps organizations understand exactly how well their end users stand up to social engineering attacks involving both e-mail and web-based delivery models, including spear phishing assessments.
- **Wireless Network Report** - Details wireless networks discovered, client-to-access point relationships, and access point profile information. Also includes information about which networks were tested against attacks, which were successfully compromised, and which weaknesses allowed the compromise.

Training and Support

Core Impact customers can achieve Impact Certified Professional (CICP) and Impact Certified Advanced Professional (CICAP) status through optional on-site, instructor-led training programs. Participants receive:

- Recognition as a certified practitioner of commercial-grade penetration testing
- Credits toward maintaining CISSP certificates
- In-depth product training through hand-on tests against lab environments
- Guidance on planning, promoting and reporting on highly targeted penetration tests

Each course spans two days (an optional third day can be added to address specific requirements, etc.) and can be conducted at your location or at Core Security's Roswell office.

Core Security provides phone support Monday – Friday 7:00 AM – 7:00 PM Eastern. Core Security also provides customers with 24x7 access to the Core Customer Community Portal (<https://coresecuritysupport.force.com/>), which includes customer forums, training videos, documentation, experimental modules, a knowledge base, and case management capabilities.

About Core Security Corporation

Core Security provides companies with the security insight they need to know who, how, and what is vulnerable in their organization. The company's threat-aware, identity & access, network security, and vulnerability management solutions provide actionable insight and context needed to manage security risks across the enterprise. This shared insight gives customers a comprehensive view of their security posture to make better security remediation decisions. Better insight allows organizations to prioritize their efforts to protect critical assets, take action sooner to mitigate access risk, and react faster if a breach does occur.

Core Security is headquartered in the USA with offices and operations in South America, Europe, Middle East and Asia. To learn more, contact Core Security at (678) 304-4500 or info@coresecurity.com.

blog.coresecurity.com | p: (678) 304-4500 | info@coresecurity.com | www.coresecurity.com