Datasheet

CORE SECURITY
A HelpSystems Company

# CORE IMPACT

Penetration Security testing throughout your organization

## Product Overview

Backed by 15+ years of leading-edge security research and commercial-grade development, Core Impact allows you to evaluate your security posture using the same techniques employed by today's cyber-criminals.

## Multi-Threat Surface Investigation

Core Impact is the only solution that empowers you to replicate multi-staged attacks that pivot across systems, devices and applications, revealing how chains of exploitable vulnerabilities open paths to your organization's mission-critical systems and assets.

## What-If Attack Analysis

Demonstrate and document the severity of exposures by replicating how an attacker would compromise and interact with vulnerable systems, and revealing at-risk data.

## Commercial-Grade Exploits

Core Impact offers a stable, up-to-date library of commercial-grade exploits and real world testing capabilities. Core Security routinely delivers 10+ new exploits and other updates each month–all professionally built and tested by in-house researchers and developers.

Core Impact simplifies testing for new users and allows advanced users to efficiently execute common tasks. This saves significant time versus manual testing, while providing a consistent, repeatable process for testing infrastructure.

## Benefits of Web Application Testing with Core Impact:

+ Exposed systems due to compromised perimeter defenses
+ What OS and services vulnerabilities pose actual threats to your network
+ How privileges can be escalated on compromised systems
+ What information could be accessed, altered or stolen
+ What systems are vulnerable to denial of service attacks
+ How trust relationships could expose additional systems to local attacks

## Teaming

Multiple security testers have the capability to interact in the same workplace against the same environment across multiple copies of Core Impact. This capability provides a common view of discovered and compromised network targets.

## Reporting

Core Impact offers comprehensive, customizable reporting capabilities.

+ Confirm exploitable vulnerabilities to plan remediation efforts
+ View metrics that illustrate the efficacy of layered defenses
+ Validate compliance with government and industry regulations
+ Remediation validation reporting capabilities

## Excraft SCADA Pack Add-on Product

Core Security partners with ExCraft Labs to deliver additional SCADA and Industrial Control System exploits for Core Impact. The SCADA pack by ExCraft Labs targets over 140 exploits in various SCADA and ICS that are deployed across many industries, on top of the SCADA and ICS exploits already shipped by default in Core Impact. This enhanced pack is updated with about four new exploits on average a month.

## Network Penetration Testing

+ Gather network information and build system profiles
+ Identify and exploit critical OS, device, service, and application vulnerabilities
+ Replicate attacker attempts to access and manipulate data
+ Pause/resume attacks to meet SLA requirements
+ Leverage compromised systems as beachheads to attack other network resources through VPN and proxy pivots
+ Test defensive technologies' ability to identify and stop attacks
+ Impersonate access points to target Wi-Fi enabled systems

## Client-Side Testing of End Users and Endpoints

+ Crawl sites, search engines, etc. for potential target information
+ Sit between tested users and real websites capturing exchange of information
+ Auto-tag users falling for phishing techniques for easy re-testing
+ Leverage a variety of templates or create custom phishing emails
+ Use client-side exploits to test endpoint system security, assess defenses, and pivot to network tests
+ Test security awareness with or without exploiting systems

## Identity-based attacks

+ Discover Windows NTLM hashes and attempt to determine plaintext passwords for those hashes
+ Discover identities: usernames, passwords, Kerberos tickets/ e-keys, and SSH keys
+ Utilize learned identities as part of multi-vector tests
+ Leverage Kerberos identities to launch attacks and find exposures
+ Automatically take control of systems via weak authentication manually or with the rapid penetration test wizard (RPT)
+ Gain persistent access to compromised systems by leveraging identity-based attacks

## Web Application Penetration Testing

+ Identify weaknesses in web applications, web servers and associated databases–with no false positives
+ Test for all OWASP Top Ten 2017 Web application vulnerabilities
+ Dynamically generate exploits that can compromise security weaknesses in custom applications
+ Import and validate results from web vulnerability scanners to confirm exploitability and prioritize remediation
+ Pivot attacks to the web server and backend network
+ Web services testing for web and mobile applications

## Mobile Device Penetration Testing

+ Identify critical exposures posed by mobile devices on your network
+ Evaluate the security of new mobile devices and related web services prior to deployment
+ Access call and text logs, GPS data, and contact entries
+ Embeddable Android Agent for Android devices

## Vulnerability Scan Validation

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

*A vulnerability scanner is not required to use Core Impact

## Surveillance Camera Attacks

+ Testing teams can identify whether a host on their network is a camera and then test it for vulnerabilities
+ Ability to prove camera vulnerabilities by taking a still shot of the video feed, or accessing the camera's administration interface
+ Testing video cameras using can be done manually or with the RPT wizard