Core Impact

Sales One-Sheet

TARGET AUDIENCE
Organizations of all sizes
Security Consultants

Industries
All
Government
Military

Job Titles:
- Penetration Tester
- Cyber Security Analyst
- Security Analyst
- CISO/CSO

SOLUTION OVERVIEW

Core Impact is an easy-to-use penetration testing tool that enables security teams to exploit security weaknesses using the same techniques as cyber criminals.

COMMON PAIN POINTS

- Need to be security compliant with industry regulations like FISMA, GLBA, SOX, HIPPA, PCI-DSS, PII, DFARS, NIST.
- Need to identify security weaknesses before cyber criminals do.
- Challenges prioritizing results from vulnerability scanners.
- Need to conduct pen tests, but lack experience

KEY FEATURES

- **Commercial-Grade Exploits**
  Core Impact offers a stable, up-to-date library of commercial-grade exploits and real-world testing capabilities. Continuously updated.
- **Usability Across Skill Levels**
  Entry level users can quickly get up to speed with intuitive GUI wizards. Expert testers can dive deep with multiple module options.
- **Reporting**
  Comprehensive, customizable reporting capabilities can be used to validate compliance with industry regulations.
- **Replicate Attacks**
  Replicate attacks that pivot across systems, devices, and applications. Verify remediation activities with ease.
- **Teaming**
  Multiple security testers have the capability to interact in the same session, providing a common view of discovered and compromised network targets.

DIFFERENTIATORS

- Stable, up-to-date library of commercial-grade exploits
- Usability across all skill levels
- Robust, customizable reporting
- Competitive, flexible pricing
- Network, Web, SCADA, WiFi and application testing support
- Enterprise level phishing included

SOLUTION USE CASES

- Network penetration testing
- Client-side testing of end users and endpoints
- Identity-based attacks
- Web application pen tests
- Vulnerability scan validation
- Phishing campaigns
- Multi-vector testing

RESOURCES & CONTENT

- Core Impact [DATA SHEET]
- Major Airline Carrier [CASE STUDY]
- Penetration Testing Toolkit [GUIDE]
- 6 Stages of Penetration Testing [BLOG]
- 15 Things Every Customer Should Know About Core Impact [ARTICLE]

QUALIFYING QUESTIONS

- Do you have an in-house penetration testing team today?
  - If they are beginners: Our tool can help elevate their skills
  - If they are red teamers, they will likely find Cobalt Strike valuable
- What tools is your penetration testing team using today?
  - If using vulnerability scanners like Nessus, Core Impact integrates well and can help validate which are truly exploitable and what the attack path would be
  - How quickly can a new member become proficient in the tools that you utilize?
  - Can your pen testers collaborate in the tools they use?
- What platform does their environment sit on? (Win, Linux, Unix, etc.)
- How much time is your team spending on repetitive pen testing tasks like verifying remediations?
- Do you conduct phishing education campaigns?
- Can you test the security of your operating systems as well as your websites / applications with the same tool?
- Does your pen testing team verify the security of your SCADA systems, for example your HVAC controls?
- How do you report on testing activity and show value to management?

Core Impact: Sales Approach and Messaging

Sales Approach

1. Research the company to determine…
   - Compliance needs
   - Critical Data (PCI, PII, PHI, IP, etc.)
   - Critical Systems (Healthcare, SCADA, Financial systems, etc.)
2. Talk to titles related to security, risk, audit, compliance, data governance, etc.
3. Clearly articulate you can offer both:
   - In-house pen testing tool – Core Impact
   - 3rd Party Pen Testing services – Core Security Consulting Services (SCS). They may need this option when….
     a. They have a compliance audit that requires an outside (3rd party) pen test
     b. They need a 3rd party pen test because they do not have the time and resources to do it themselves
     c. They want both for a check and balance to their testing strategy – internal and external pen testing
4. Once the needs are defined, schedule a demo

Average Deal Size

- Low – $15,000 (1 end-user)
- Medium – $30,000 - 60,000 (2-4 end users)
- High – $100,000+ (enterprise teams)

Objection Handling

- We use Metasploit as our pen testing tool. Impact is great but too expensive.
  - Many of our customers license both Core Impact and Metasploit to give them a full library of effective exploits. If budget is a limitation, we now can offer competitive pricing to Metasploit. Would it make sense to give you a demo and a competitive quote?
- We are planning to build a penetration testing team but we do not have the staff to do this currently.
  - Great – would it make sense for us to provide a pen test for you while you are getting your team hired and trained?
  - Impact is a great tool for this as it is the most user-friendly UI of any testing tool on the market. When do you project to hire for this? Does it make sense to show you a demo and how we help new testers get confident on Impact?
- We have used Impact and loved it, but my company cannot afford it
  - We have new pricing options and are very competitively priced

Core Impact vs. Metasploit

CORE SECURITY
A HelpSystems Company

	Metasploit	Core Impact
Pivoting	• Can only pivot by proxies or through VPNs that user has to configure • Does not handle multiple pivots well/pivoting through different operating systems. Is very manual	• Easy and intuitive pivoting workflow (right click and set as source, done) • Is lightweight, only needs to proxy syscalls or API calls on the target, all else is handled by the console • Supports PCAP installation in pivoted scenarios, which enables stealthier info gathering • Ability to tunnel its communications through DNS channels (Metasploit cannot do this) • Supports agentless shells and WMI persistence which allows much stealthier interactions with systems in obtaining persistence
Exploits	• Metasploit Pro total exploits: 1429 • Metasploit has no support for testing SCADA systems	• Core Impact Commercial Grade exploits: 1836 • Core Impact + additional unique exploits from Metasploit Pro: 2163 • Exploits are Commercial grade and are thoroughly tested. • Offer SCADA exploits that can be obtained through ExCraft
Reporting	• Does not allow the same level of customization and the workflow is much more laborious	• Highly customizable reports with the ability to save custom templates for future use • Customization workflow is easy and intuitive, just edit an excel template • Can report across all vectors in one product
Remediation Validation	• Does not have any functionality in this area. The closest is a reply script which does not support movement across vectors nor pivoting	• Allows one click test that allows for the user to check if patching/remediation efforts were successful • Can mimic the exact attack path across multiple vectors that resulted in an exploit previously, thus ensuring that the patch/remediation was success or not
Identity Management		• Offers easy integrations with default and custom ID dictionaries for both initial testing and BruteForce attacks • Supports many more authentication protocols than Metasploit • integrated use cases for identities that have been validated, even Kerberos Tickets/keys • Out of the box integrations with offline password cracking tools

helpsystems

Core Impact Background and Anecdotes

Core Impact Background

- Created by Core Labs in 2001
- Core Labs is a team of highly skilled threat researchers and testers who write exploits for Impact
- Thousands deployments globally
- Experience in all major industries, geographies, and governments (standard Federal tool)
- In-house exploit writers and researchers continuously updating the product every week with new exploits, techniques, and updates

Anecdotes

Large Enterprise Company:

- Saved tremendous time by importing scan results into Core Impact
- Extremely large pen-testing scopes due to importing of scan data ease
- Impact automates base level work allowing this enterprise's security team to focus on harder and unusual targets
- Privilege escalation capabilities also helps this team leverage small compromises that would otherwise have been useless.

Small Financial Company:

- Three person team that handles all IT Infrastructure, security policy, and vulnerability management
- With such a small team, Core Impact helps them automate pen testing allowing them to focus their limited headcount on more strategic projects
- The ability to run macros or modules immediately upon successful deployment of an agent also really helps speed things up
- Now they are able to stay ahead of security audits and make sure that there are no surprises from audit findings