

EXTEND THE REACH OF YOUR SECURITY ASSESSMENTS

Core Security Technologies extends the ability of security professionals to replicate attacks against IT systems by combining the commercial-grade, automated penetration testing capabilities of CORE IMPACT® Pro with the community-built functionality of the Metasploit network penetration testing framework.

How the Integration Works

Using Metasploit in concert with IMPACT Pro gives you the benefits of Core's commercial-grade, automated solution – with its massive library of professionally developed exploits, easy-to-use interface, and in-depth reporting capabilities – combined with the additional network exploitation capabilities of Metasploit. The integration works in two ways:

- Begin testing with CORE IMPACT Pro and insert Metasploit into the process, supplementing IMPACT's resident attack and penetration capabilities and expanding your assessment of the network.
- Begin testing with Metasploit and then bring a compromised system into the IMPACT environment for further assessment and to test other systems on the same network.

Regardless of which approach you take, test results are consolidated into IMPACT reports that provide actionable data about where your organization's critical risks lie and what you can do about them.

Beginning with CORE IMPACT Pro

Under this approach, you launch Metasploit's network exploits in tandem with IMPACT Pro exploits. You begin the assessment using IMPACT Pro's information gathering capabilities to first profile a target network. IMPACT then conveys operating system and service pack details about identified systems to Metasploit. As IMPACT selects and deploys its own exploits, it also leverages Metasploit's db-autopwn feature to launch relevant Metasploit exploits against each targeted system – and the results are subsequently uploaded back into IMPACT Pro. This allows users to view Metasploit testing information within the IMPACT environment, without requiring Metasploit expertise.

Beginning with Metasploit

Under this approach, you bring a system compromised during testing with Metasploit into the IMPACT environment and deploy an IMPACT Pro Agent. The Agent is a patented, syscall proxy payload that allows you to:

- Launch IMPACT Pro's full range of automated penetration testing capabilities from the compromised system.
- Leverage IMPACT's broad selection of commercial-grade exploits, plus extensive pre- and post-exploitation capabilities for in-depth, comprehensive attack replication.
- Pivot penetration tests to other systems, mimicking an attacker's attempts to identify and exploit paths of weakness to backend systems and data.

The Benefits of a Combined Penetration Testing Solution

Whether you're a professional penetration tester or an operational security manager, the integration between IMPACT Pro and Metasploit delivers multiple benefits:

Expanded Exploitation Capabilities

While the majority of network exploits in Metasploit are already available as commercial-grade exploits in IMPACT, supplementing IMPACT's library with those exploits that are unique to Metasploit enables you to assess your organization for an even broader range of exploitable network vulnerabilities.



Capabilities for Penetration Testers

If you're a professional penetration tester accustomed to the Metasploit framework, adding CORE IMPACT Pro enables you to expand the scope and value of your assessments:

- Utilize hundreds of additional, commercial-grade exploits, with 20-30 modules added per month.
- Conduct tests across web applications, endpoints, end users and wireless networks – in addition to network systems.
- Leverage IMPACT's extensive pre- and post-exploitation capabilities to replicate all stages of a real-world attack.
- Document, compare and track test results over time through IMPACT's wide array of professional reports.

Capabilities for Security Managers

IMPACT's integration with Metasploit enables operational security managers to leverage Metasploit's exploit capabilities without requiring Metasploit expertise:

- Launch Metasploit's network exploits from the IMPACT GUI.
- View Metasploit activity and results in the IMPACT interface.
- Include Metasploit results in IMPACT reports.

The Benefits of a Combined Penetration Testing Solution (continued)

End-to-End Attack Replication

To accurately assess risk, a penetration test must reflect all aspects of a potential attack, from gathering information about targets, to exploiting vulnerabilities, to replicating an attacker's interactions with compromised systems. Through the integration, you can initially compromise a system with a Metasploit exploit and then deploy an IMPACT Pro Agent. The IMPACT Agent acts as a conduit not only for launching IMPACT Pro commercial-grade exploits, but also for leveraging IMPACT's broad range of pre- and post-exploitation capabilities.

Comprehensive Testing Across Diverse Infrastructure

The integration supplements IMPACT's network penetration testing capabilities by enabling you to leverage Metasploit exploits to assess the network. In addition to network testing, you can use IMPACT Pro to conduct real-world, multistaged penetration tests across web applications, endpoints, end users and wireless networks.

Actionable, Consolidated Reports

When Metasploit network exploits are used in conjunction with an IMPACT Pro penetration test, those exploits and their ramifications are incorporated into IMPACT reports. IMPACT Pro reports provide actionable data about at-risk systems and applications, exploitable vulnerabilities, and remediation options – as well as security assessment trends over time, delta comparisons of multiple tests, and graphical attack paths depicting chains of exposed IT assets.

Because Metasploit is an independent, community-built, open-source project, Core Security cannot guarantee the safety, reliability or predictability of Metasploit exploits used in conjunction with IMPACT Pro.

Next Steps ...

In addition to offering network penetration testing, CORE IMPACT Pro includes capabilities for testing the security of endpoint systems, web applications, end users and wireless networks. Want to learn more? Contact us today to schedule a demonstration:

Phone: (617) 399-6980

Email: info@coresecurity.com

Headquarters
41 Farnsworth St.
Boston, MA 02210
Ph: (617) 399-6980
Fax: (617) 399-6987
www.coresecurity.com