

CUSTOMER STORY (Cybersecurity)

Security Consulting Firm Increases Efficiency with Automated Pen Tests from Core Impact

Background

With cyber attacks perpetually on the rise and an increasing number of security regulations in effect, independent cybersecurity firms are more important than ever for helping organizations keep their data safe and assisting with adherence to relevant state, federal, and international laws, security frameworks, and industry mandates like PCI DSS, HIPAA, SOX, NIST, and more.

One of the best ways these firms can ensure an organization is effectively protecting their environment and maintaining compliance is by running penetration tests, which help determine an organization's security posture by uncovering and exploiting security weaknesses, demonstrating how an attacker may breach the IT environment.

While cybersecurity firms are staffed with experts, given the high volume of need, they are always seeking ways to increase efficiency and effectiveness.

The Challenge

Compass IT Compliance opened 2010, providing services in IT security, compliance, and risk management services to organizations of all sizes in all industries.

Penetration testing services have become increasingly popular, as they both provide an outside perspective on the status of an organization's security, and can verify compliance when organizations need to provide proof to auditors. With more penetration tests being requested, vigilance about time management is critical.

When completing penetration testing engagements, Compass found that in order to effectively complete all the different tests necessary, they needed to leverage a mix of open source tools alongside their licenses of MetasploitPRO.

As there was no great way to centralize these solutions, switching back and forth between them and manually combining information for reporting was becoming overly time consuming and inefficient.

AT-A-GLANCE



Company
Industry

Compass IT Compliance
Cybersecurity Services

PROBLEMS SOLVED

- Multiple, decentralized solutions
- Time consuming process switching between tools

KEY SOLUTIONS

Core Impact

RESULTS

- Increased efficiency from centralized console
- Can create a more comprehensive picture of a customer's security posture

What Compass wanted was a one stop shop—a tool that had multiple capabilities, as well as the ability to incorporate other tools if need be.

The Solution

Jesse Roberts, VP of Security, had begun the search for a new tool and was reminded of Core Impact after seeing a webcast from Security Weekly on the solution.

"I was impressed with its flexibility," Roberts said. "It has a lot of different options, and really is the centralized tool that we were looking for."

Core Impact allows you to gather information, exploit systems, and generate reports, all in one place. Every phase of the penetration test process can be executed and managed from a single console.

Additionally, Core Impact provides even more centralization by incorporating with and validating vulnerabilities from more than 20 popular scanners, including Burp Suite, Nessus, Qualys, and OpenVAS, which helps to prioritize the greatest risks.

Finally, having integrations with other pen testing tools like Metasploit, PowerShell Empire, and Plextrac can further streamline and increase the breadth of its pen testing program. For example, Compass had previously only been able to complete tests on Wi-Fi networks on site, but with Core Impact's integration with [WiFi Pineapple](#), they have the ability to complete these tests remotely.

The Outcome

Compass only recently deployed Core Impact, but have already been impressed with its capabilities. Roberts has been able to execute both internal and external pen tests that are not only faster, but have better results. "By standardizing tests on one tool, we can provide a more comprehensive picture of an organization's security posture," he noted.

In addition to testing out Core Impact's patented agents, which simplify management of remote host communication, he's also supplemented web application pen tests with Burp Suite scans. Eventually, he hopes to explore Core Impact's client-side test, which includes tailoring and deploying phishing campaign simulations.

Overall, the convenience of a single platform, both in its dynamic toolset and its integrations with other solutions, has enabled Compass to more effectively exploit security weaknesses across any organization, ensuring their customers will be able to keep their data secure and remain compliant.