

CORE IMPACT CUSTOMER SUCCESS STORY

SOLUTION SUMMARY

CUSTOMER TYPE | Major research university

CHALLENGE | Test the network security of 180+ departments and ensure PCI compliance.

SOLUTION | CORE IMPACT, the first comprehensive penetration testing solution for assessing specific information security threats to an organization.

THE COMPANY

Virginia Tech



Founded in 1872, Virginia Tech is a comprehensive, innovative research university with the largest full-time student population in Virginia. With more than 21,500 undergraduate students, about 6,000 graduate students, and more than 2,600 faculty members and researchers, Virginia Tech offers more degree programs and awards more diplomas than any other university in the Commonwealth of Virginia.

THE CHALLENGE

With responsibility for the private information of thousands of students, faculty, staff and alumni, it's no wonder that preventing cybercrime is a top initiative for Virginia Tech. Heading this effort is Randy Marchany, director of Virginia Tech's IT Security Laboratory and the University's assistant IT security officer. Through its IT Security Review Program, the Lab provides comprehensive risk analysis services for over 180 departments. "While our to-do list is long, our overall goal is clear: to prevent the University from experiencing data breaches," said Marchany.

According to Marchany, prioritizing the IT Security Review Program was easy, "We first had to focus on the departments that handle credit card transactions and therefore must comply with the PCI Standard." Established by MasterCard, Visa and other major card providers, the Payment Card Industry (PCI) Data Security Standard holds the University to specific requirements for safeguarding cardholder information.

To help University departments comply with the PCI Standard, Marchany and his team had to perform security tests including vulnerability scans and penetrations tests. Specifically, PCI Requirement 11.3 calls for network penetration testing to be performed "on network infrastructure and applications at least once a year and after any significant infrastructure or application upgrade or modification (e.g., operating system upgrade, sub-network added to the environment, web server added to the environment) ..."

THE SOLUTION

While the PCI Standard requires Virginia Tech to perform penetration testing, Marchany also recognizes its value as part of the University's overall vulnerability management strategy: "We've always done scanning, but we really needed a way to determine if the found vulnerabilities were actually exploitable. We knew that penetration testing could take our security assessments to another level by emulating real-world data breach attempts."

The IT Security Lab first gained experience with penetration testing by using an open-source solution. "While it was free, the open-source application lacked reporting capabilities. This slowed us down, since we had to manually build reports and get them into usable formats for management and technical staff." Marchany and his team therefore decided to look at commercial products and quickly decided on CORE IMPACT.

In addition to the product's tailored reporting capabilities, key reasons for selecting CORE IMPACT included its safe, repeatable testing processes and regular exploit updates. "Overall, IMPACT gave us an automated, industry-standard tool for exploiting the vulnerabilities that expose us to data breaches," said Marchany.

THE RESULT

With CORE IMPACT, Marchany's team could significantly speed the security review process and more efficiently serve the entire University, starting with the 19 departments that process credit card data and require PCI compliance. "The reviews are really like 'pre-audits,' where we work side-by-side with department IT staff to identify security issues before they become problems, such as data breaches or failed PCI audits," stated Marchany.

Making Penetration Testing Integral to the Security Review Process

The IT Security Lab follows a two-week, white-box testing process, which includes replicating threats from internal staff or students with knowledge of the departmental networks – as well as hacking attempts from outside the University. After gathering information about a department's firewall rules, IP addresses and installed programs, testers leverage a comprehensive toolkit of applications for each security review:

- **Local Security Testing**

The tester identifies systems that contain social security numbers and credit card numbers using both custom scripts and a spider application from Cornell University.

- **Vulnerability Scanning**

Using Nessus Vulnerability Scanner and Nmap Security Scanner, the tester assesses the department's IP address space for an overview of all potential security exposures.

- **Automated Network Penetration Testing**

Scan results are imported into CORE IMPACT, which attempts to exploit found vulnerabilities in a deliberate, controlled manner. The tester uses the product to safely demonstrate exploit paths and interact with compromised systems, allowing departmental staff to see exactly how a real-world data breach could unfold – without suffering the consequences of an actual incident.

- **Web Application Testing**

The active review process concludes with an audit of web applications and servers using tools including Nikto, Wikto, WebScarab and Paros.

Speeding and Adding Value to Testing Engagements

With CORE IMPACT, the IT Security Lab team can easily generate reports containing data about targeted networks and hosts, audits of all exploits performed, and details about proven vulnerabilities. The product also offers tailored versions of activity reports, giving IT staff the specific vulnerability information they need to eliminate security exposures, while providing management with concise highlights and test results. "My team can now get their jobs done faster and provide our clients with actionable information, while maintaining a record of all tests for PCI and other compliance needs," stated Marchany.

Staying on Top of Vulnerabilities with Timely, High-Quality Exploits

System administrators at Virginia Tech can rest assured that their networks are tested against the latest threats, since IMPACT is regularly updated with new exploits. "Core Security sends email notifications whenever updates are available. All we need to do is hit a button, and we know that our tests include timely, high-quality exploits," said Marchany. In addition, all IMPACT exploits are designed to work across all relevant operating systems, service packs and attack vectors, ensuring that Virginia Tech can test each vulnerability from multiple angles.

Extending Testing Reach beyond the University Walls

Like many organizations, Virginia Tech uses an external vendor to process credit card transactions, such as tuition payments. The value of automated penetration testing quickly became evident during one security review when it revealed an exploitable vulnerability with the third-party card processing service. "After logging into the service, we were able to launch a remote exploit that identified an outside scripting vulnerability that could potentially jeopardize card data. Needless to say, the vendor immediately corrected the problem and the system was once again secure."

"With CORE IMPACT, we know that security testing at Virginia Tech is about as thorough as it can be," Marchany noted, adding, "This is a very powerful product, so we're sure to lock our pen testing laptop in a safe every night."

The views expressed in this document are solely those of the speaker and do not necessarily reflect the views of Virginia Tech.