NETSPI

NETSPI.COM • 612.465.8880

Security Testing for M&A: Rapid Remediation supported by Resolve™

The Situation

A merger or acquisition can be a high risk process. In some cases, such as through a stock purchase, the acquiring company is legally bound to assume the debts, obligations, and lawsuits of the company being acquired – even if they are not known at the time of sale. What's often forgotten is the IT security risks that the acquiring company assumes as part of the acquisition process. As part of its due diligence process, senior risk managers at a leading software development company wanted to evaluate the network security of a potential acquisition target. Having worked with NetSPI for almost a decade, it called upon its security experts once again.

The Challenge

Providing a detailed report on a company's network security can take some time. Because the due diligence process was already in the final stages, NetSPI had just a few days to build an inspection team, complete a comprehensive array of tests and compile an in-depth report.

The Approach

A six-person security team set about testing two web-based applications as well as conducting external and internal penetration tests using both automated and manual processes. Because of significant time pressure, NetSPI ran all of the tests concurrently.

"For web applications we are looking for vulnerabilities that may exist between a browser and the server and the overall user experience," said Sam Horvath, one of the NetSPI pentesters. "Maybe there's something in the app that provides us with access to sensitive information or maybe we can obtain access to functionality that should be off limits."

Client

A large software developer in the process of acquiring another development company.

Challenge

Test two web-based applications, conduct both external and internal penetration testing as well as provide a detailed vulnerability report – all within just a few days.

Approach

Deploy a six-member test team onsite to run tests concurrently and manage the entire test and reporting process with the NetSPI Resolve™ platform.

Results

NetSPI identified several critical vulnerabilities for its client that could have potentially affected the transaction. Additional due diligence was required and security enhancements were made prior to acquisition.

Industry
Software Development

From a network perspective, the NetSPI team tested the external network for any threats that may allow an external attacker to potentially breach the perimeter from the Internet and access the internal environment. "From the internal network perspective, we assume that a malicious actor is already on the network so we test to find out what they can see, what they can exploit, and if they could escalate their privileges to get access to other areas of the environment," said Horvath.

Had NetSPI relied on a lot of manual processes and spreadsheets – like many companies still do – meeting the tight deadline would have been impossible. Fortunately, it had NetSPI Resolve™. This advanced testing platform automates many processes and effortlessly correlates vulnerability data from all sources, scanners or pentesters, into a single view for the whole organization.

"Once we go through the test checklist in NetSPI Resolve™ and identify what is vulnerable or not vulnerable, we create specific instances describing the vulnerabilities that were discovered and press a couple of buttons to generate a clean, formatted report with verifications," said Horvath. "With Resolve™ it's a quick and simple task to get results turned around quickly."

The Results

Within the first couple of hours of testing, the NetSPI team found several critical vulnerabilities on the network of the software development company that was about to be acquired.

In testing the web applications, NetSPI testers found persistent cross site scripting. In theory, a malicious actor could add their own JavaScript code to the web page to take advantage of this vulnerability. Code could be written to steal a session ID for example, enabling a malicious actor to impersonate the legitimate user for as much time as the session is valid.

NetSPI testers also found a SQL injection vulnerability, which can be used to attack data-driven applications. When a user searches on a website, that query is often turned into a database entry and that query can be manipulated to query for additional data on the database. NetSPI testers were able to breakout of the query that was being sent to the server from the web application and search the database arbitrarily. As a result, over 500,000 records of customer data could be easily accessed.

> Once we go through the test checklist in NetSPI Resolve™ and identify what is vulnerable or not vulnerable, we create specific instances describing the vulnerabilities that were discovered and press a couple of buttons to generate a clean, formatted report with verifications. With Resolve™ it's a quick and simple task to get results turned around quickly.
>
> **Sam Horvath**
>
> *NetSPI Pentester*

During external penetration testing, NetSPI was able to guess a weak domain user password and breach the internal environment through a single factor authentication VPN interface. During the internal penetration test, NetSPI was able to respond to a broadcast protocol request on the internal network, receive authentication data, and capture a hashed version of a domain password. Just a few minutes later, NetSPI was able to crack the password hash and obtain full domain administration rights and gain full control over the entire internal network.

Initial findings were presented to the client within 24 hours resulting in the acquiring company delaying the integration of both IT environments until all vulnerabilities were addressed. Based on NetSPI's findings, the acquired company had to go through a number of additional steps prior to acquisition to ensure its network security was more robust.

Increase Visibility. Reduce Risk.

Transform your security program with NetSPI's comprehensive penetration testing and vulnerability assessment services. Proven to **uncover 2x more critical vulnerabilities** than the top network scanning tools, combined.

Learn more at www.NetSPI.com

About NetSPI

NetSPI is the leader in enterprise security testing and vulnerability management. We are proud to partner with nine of the top 10 U.S. banks, the largest global cloud providers, and many of the Fortune® 500. Our experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces. We uniquely deliver Penetration Testing as a Service (PTaaS) through our Resolve platform. Clients love PTaaS for the simplicity of scoping new engagements, viewing their testing results in real-time, orchestrating remediation, and the ability to perform always-on continuous testing. We find vulnerabilities that others miss and deliver clear, actionable recommendations allowing our customers to find, track, and fix their vulnerabilities faster.

Website
www.NetSPI.com

Email
Info@NetSPI.com

Phone
612.465.8880