NetSPI Testing Highlights Security Flaws for Leading Financial Services Firm

The Situation

The financial services industry typically suffers more data breaches and cyber attacks than any other vertical market. Worse still, the cost associated with those attacks – due to litigation, regulatory fines and lost business – is significantly higher for banks, insurance companies and brokerage firms. Forbes puts the cost at $18 million per firm, per breach, compared to $12 million for firms in other industries. One leading financial services company decided it was time to be proactive and see just how secure its network really was. After evaluating the assessment and testing capabilities of a number of companies, it selected NetSPI.

The Challenge

The financial services firm set quite a challenge for NetSPI: complete internal penetration testing of all internal networks in four days. Beyond allowing physical access to the network, no information would be provided to NetSPI. Acting as malicious insiders that had breached the network perimeter and gained physical access to the internal network, NetSPI consultants were to emulate an Advanced Persistent Threat (APT) and report their findings.

The Approach

NetSPI testers started by passively enumerating hosts on the network they were connected to. In addition, testers ran the SpiderLabs Responder tool to passively listen to broadcast Windows protocols (NBNS/LLMNR). This exposed some interesting information about the hosts on the broadcast network. Once NetSPI had enumerated enough information, specific targets were selected. NetSPI was able to forge NBNS responses to NBNS requests for the WPAD.domain.com host name. The requests for Web Proxy Auto-Discovery Protocol (WPAD) were put on the network by domain computers that were looking for a proxy server to use. As a result, it was possible to force users to authenticate to NetSPI's attacking laptops and capture the network NTLMv2 password hashes for domain user accounts.

Client

A major U.S. financial services company.

Challenge

Complete internal penetration testing of all internal networks within just four days.

Approach

NetSPI conducted an anonymous scenario-based red team attack against the client's internal network. Network- and application-level attacks tested detection and response capabilities as well as identified vulnerabilities and escalation paths.

Results

By showing that full network compromise was possible in a short period of time, NetSPI helped the firm evaluate its ability to identify and respond to an unknown threat agent, increase its detective controls capabilities, and remediate multiple vulnerabilities.

Industry
Financial Services

Once user password hashes were obtained, NetSPI was able to use its GPU-accelerated cracking box to quickly crack the passwords for domain users. It did not take long to obtain the credentials needed to start working up to domain administrator rights.

By coincidence, NetSPI was onsite when the client was working through a Microsoft patch cycle. While patches had been applied to the domain controllers, only half of them had been rebooted – a necessary step for applying this patch. The patch fixed a Kerberos issue that allowed domain users to immediately escalate their privileges to domain administrator on the affected domain controller.

NetSPI was able to use the cracked user credentials with the exploit to gain full control over the domain controller. Even without access to this missing patch, NetSPI could still identify multiple paths that could be used to escalate privileges on the Windows domain. With full access to the domain, NetSPI then dumped the password hashes for all domain users.

With full access to all of the domain password hashes, NetSPI had guaranteed persistence as a domain administrator. Either by passing the hash, or creating long-term Golden Kerberos tickets, NetSPI would have continued domain admin access for the rest of the exercise. Since clear text passwords are easier to use, NetSPI started cracking the password hashes. Within minutes, over 50% of the domain password hashes were cracked, including passwords for several domain admins. NetSPI then started enumerating network shares and targeting sensitive data stores. By identifying shares owned by key employees, NetSPI was able to identify repositories for PCI documentation.

While the financial services company was utilizing strong two-factor authentication methods to access PCI-zone jump hosts, the jump hosts were not fully isolated. By using secondary authentication channels (not-RDP), NetSPI was able to gain a remote shell on the jump hosts. As a result, NetSPI was able to back door the “sticky keys” executable, bypass the two-factor authentication, and gain RDP access to the hosts. NetSPI then had full access to cardholder data and the PCI zone. Additional review of the PCI documentation enabled NetSPI to identify multiple controls that were listed, but not in place. These missing controls resulted in direct access to the PCI environment from the main user network.

NetSPI consultants were to emulate an Advanced Persistent Threat (APT) and report their findings.

The Results

By carefully targeting specific vulnerabilities, NetSPI was able to gain access to internal hosts and escalate privileges to domain admin without detection. After escalating privileges, NetSPI increased the volume of network activity to more aggressively test the detective capabilities of the incident response team. The bottom line: using primarily manual testing techniques, NetSPI was able to show a threat actor with moderate knowledge of common attacks against Windows environments and with access to publicly available tools could gain access to critical assets and sensitive data. Based on the test results, NetSPI was able to help the client evaluate its ability to identify and respond to an unknown threat agent, increase its detective controls capabilities, and remediate multiple vulnerabilities.

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