netSPI Case Study

RISK COMPLIANCE SECURITY

NetSPI Red Team

Four Days Onsite - A Network Red Team Case Study

Red Team: Testing Real-World Defenses

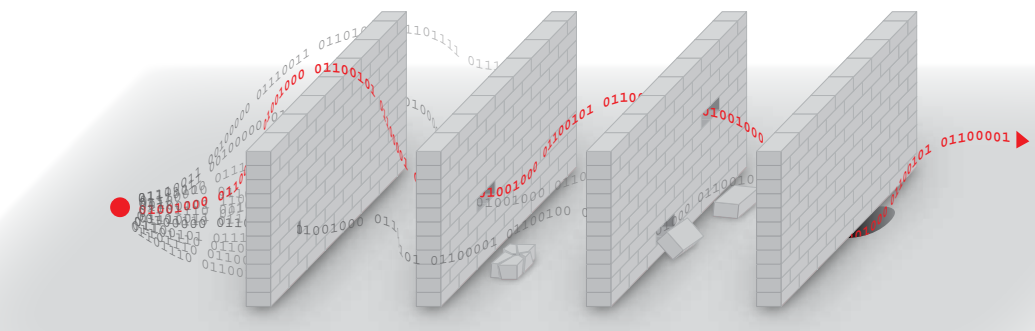
Internal network testing often focuses on three primary strategies—vulnerability assessments, network penetration tests, and red team tests.

- Vulnerability assessments are primarily focused on identifying common vulnerabilities on the server and application layers.
- Network penetration tests focus on a mix of automated and manual vulnerability enumeration, vulnerability exploitation, and escalation of privileges to identify real-world impact. These types of tests are frequently driven by compliance standards (e.g., PCI).
- Red team tests are typically centered on testing critical assets, such as those that drive client revenue and define a client's brand. It is also common to conduct red team tests to assess the response capabilities of the internal incident responders. These exercises often include social engineering such as phishing, phone calls, or attacking physical assets to gain access to network resources.

Emulate an Advanced Persistent Threat (APT)

NetSPI was engaged to complete internal penetration testing of this client's internal networks, while acting as an entity that had breached the perimeter. For this scenario, NetSPI consultants acted as malicious insiders with physical access to the internal network. This saved NetSPI some time, since the testers did not have to gain an initial physical presence in the building. Gaining this access could have been done through social engineering, but testing physical access controls was not in scope for this round of testing.

Red team testing emulates very selective attack behaviors that are relevant to the available technology in the targeted environment. While vulnerabilities and impacts will be identified, red team exercises are not meant as a comprehensive penetration test. For more comprehensive threat emulation, some type of detective controls testing should be done to make sure the incident response team has the ability to detect on the following surfaces: external network, internal network, wireless network, user endpoints, and email.



Client

This NetSPI client is a major financial services company.

Challenge

NetSPI was engaged to do an anonymous scenario-based red team attack against the client's internal network. This project was designed to test the client's detective and response capabilities, identify vulnerabilities and escalation paths, and prove that full network compromise was possible in a short period of time. The entire exercise happened during a four-day period. Vectors of attack were limited to network- and application-level attacks. All phishing and other social engineering attacks were out of scope. Beyond allowing physical access to the network, no information was provided to NetSPI.

Solution

Using primarily manual testing techniques, the NetSPI pentesters enumerated all of the internal network ranges and systematically exploited vulnerabilities to escalate privileges and avoid detection.

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. Using the results of the test, 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.

Hiding in the Shadows

NetSPI testers started by passively enumerating hosts on the network that they were plugged into. This was complemented by running the Responder tool to passively listen to broadcast Windows protocols (NBNS/LLMNR) that exposed some interesting information about the hosts on the broadcast network. Once NetSPI had enumerated enough information about the hosts on the broadcast network, specific targets were selected. NetSPI was able to forge NBNS responses to NBNS requests for the WPAD.domain.com hostname. The requests for WPAD were put on the network by domain computers that were looking for a proxy server to use. This is a common problem seen in Windows networks that are set up to use Web Proxy Auto-Discovery Protocol (WPAD). As a result of this issue, it was possible to force users to authenticate to NetSPI's attacking laptops and capture the network NTLMv2 password hashes for domain user accounts.

Once user password hashes were obtained, NetSPI was able to use its GPU-accelerated cracking box to quickly crack the passwords for domain users. Using this technique, NetSPI was able to get the credentials needed to start working up to domain administrator rights.

Keys to the Kingdom

Call it good timing, but NetSPI was onsite doing testing within the 30-day window of the MS14-068 Microsoft patch being released. This large client organization was working on the patch cycle, so only about half of the domain controllers had been fully patched for the vulnerability. 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 used the cracked user credentials with the exploit to gain full control over the domain controller. Without access to this missing patch, NetSPI still identified multiple paths that could have been used to escalate privileges on the Windows domain. With full access to the domain, NetSPI then dumped the password hashes for all domain users.

This is where things got intriguing. 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 cleartext 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. At this point, NetSPI 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 strong documentation of the PCI environment is a good thing, it also made it easier for NetSPI to go after the PCI hosts. This is a very common tactic for NetSPI to use during penetration tests, as organizations are required to properly document their PCI environments. This company was utilizing strong two-factor authentication methods to access PCI-zone jump hosts, but 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. With a shell on the jump hosts, NetSPI backdoored the "Sticky Keys" executable, thereby allowing NetSPI to 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 allowed 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.

Conclusions

NetSPI set out to take control of the internal network and gain access to business-critical data with only a network connection. NetSPI accomplished that goal within a day, a very short window of time. NetSPI was able to invest the remaining three days emulating common indicators of attack to test the detective control capabilities of the client. In doing so, NetSPI was able to illustrate that 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 that directly contribute to the client's revenue, brand, and the public's trust in the company's ability to protect their sensitive data.

800 Washington Avenue North, Suite 670, Minneapolis, Minnesota 55401
www.netspi.com 612.465.8880 Telephone 888.270.0317 Toll free 612.455.6988 Facsimile