Global Information Assurance Certification Paper

Case Study: Security Assessment at a Small Technology Corporation

Ryan L. Reiber

SANS GSEC Version 2.0
September 10, 2001

Introduction

Our company has developed a Trusted Space for client-server and Web-enabled applications, allowing businesses to safely access and exchange confidential information electronically through the Internet. As we continue to develop products and services on our internal networks, and our suite of Internet Trust Services helps businesses confidently and securely move key business functions online, the security and confidentiality demands must be adequate. Our in-house IT security team, relying heavily on our past experiences and knowledge, performed an *independent* security assessment. Even though the people on the assessment team were all internal employees, the review was able to remain *independent* because of the team's limited knowledge of the internal configuration; the team was made up of recently hired individuals. The assessment included the areas of its ASP, internal network infrastructure, and firewalls.

We conducted the assessment via interviews with individuals responsible for the design and configuration of these components, hands-on investigation, review of supportive procedures, and analysis of relevant documentation. We performed numerous manual and automated security tests employing software tools to validate the control assumptions and identify potential security vulnerabilities. Internet Security Systems' Internet Security Scanner (ISS), Axent's Enterprise Service Manager (ESM), and various other public domain tools were also utilized as part of this review. Procedures performed included a review of the ASP implementation of Extranet technologies, security penetration tests, host vulnerability testing, and an assessment of the general administration and architectural controls surrounding the processing environment for the firewall.

A number of exposures were identified that would allow an outside entity to gain access within our network. Based on the activities performed, there is a potential that our Internal Network could be compromised. Depicted below is a ranking of severity of the areas reviewed, using a color scheme of Red=High Exposures and Green= Low Exposures:

1. **VPN / Remote Access Review** – the review of our proposed VPN solution as well as remote access entry points
2. **External Vulnerability Scans** – the assessment of our Internet connectivity
3. **Firewall / Router Review –** the evaluation of scans ran against the firewall as well as a review of the router

4. **Internal Vulnerability Scans** – the assessment of our company's internal network including scans with both Internet Security Scanner (ISS) and Extended Software Manager (ESM) software tools

5. **ASP Security Review** – the analysis of services offerred by the ASP (Application Service Providor), inlcuding penetration scans and firewall rule set review

In the following pages, I have summarized the approach, findings, and recommendations.

1. VPN / Remote Access Review

The team's objective was to evaluate our company's proposed Virtual Private Networking (VPN) solution to verify there is a secure tunnel between our networks and our ASP.

VPN

Currently, the company is using a dial-in server to enable personnel to connect to the network remotely. In addition, communications with the ASP occur utilizing File Transfer Protocol (FTP) services. However, two VPN solutions have been proposed for future implementation. The first will allow our company's personnel to connect to the internal network via the Internet using Secure Remote with SecurID for increased authentication. The second will enable specific company personnel to transmit one way to our ASP via an encrypted tunnel. Discussions were held concerning the placement of the VPN appliance. It's been the experience of our staff that the VPN should be placed behind the firewall. However, given the requirements of our business and mapping those to the offered solutions with our ASP, this configuration was not a viable solution.

Prior to the implementation of the two VPN solutions, we implemented FTP over SSH (secure shell). We were previously running SSH to connect to our ASP's network to allow our company to FTP through the SSH tunnel. The connection through the SSH link encrypts all stages of establishing the FTP connection and therefore renders an insecure protocol (FTP) more protected.

The encryption of FTP files passing via SSH was validated using the network sniffer SessionWall-3. We did testing, observed and validated the capture of network packets as they were transferred between our company and our ASP.

Remote Access

A remote access assessment and diagnostic activities were conducted to perform a controlled security penetration to assess the overall level of security and identify

exposures associated with the dial-in environment. A listing of analog numbers was obtained from network infrastructure personnel and used as the basis of our test to identify modem connections to the internal network. However, no significant exposures were identified.

2. External Vulnerability Scans

The assessment team's objective was to perform external vulnerability scans to identify external vulnerabilities or threats related to the company's Internet connection. Since our Firewalls/Routers were visible to the Internet, it was extremely important to ensure that only necessary services are allowed or accepted. Having too many services open makes the Firewall/Router too complex to administer and increases security exposure to the internal network.

A number of external scans were performed from the Internet looking for open ports, responsive pings, and known exploits. This review included utilizing both automated software tools (ISS) and common "hacker" techniques that our team gathered. Using ISS, a prevailing security vulnerability scanner that evaluates over 600 known vulnerabilities, we performed a series of tests against the router and FireWall-1 along with the company's visible subnets to identify vulnerabilities as one step of an attack. During the vulnerability tests, a number of vulnerabilities were identified on various machines.

During the time of the assessment, there was no monitoring of the firewall logs for unauthorized access attempts and/or system scans at our organization. During fieldwork, numerous scans were run and went unquestioned by internal network operators unaware of the assessment team's activities. Further discussions with network infrastructure personnel indicated that the firewall logs are too large and cumbersome to review. Following the assessment team's review, a firewall administrator was hired to be in charge of generating and reviewing firewall logs.

3. Firewall / Router Review

The security assessment team's objective was to evaluate the firewall configurations to determine if potential vulnerabilities through external access points exists. The primary purpose of the firewall configuration review was to ensure the external firewall provides adequate front line protection from unauthorized access.

Firewall

The security assessment team evaluated the company's CheckPoint FireWall-1 configuration by reviewing the firewall rule sets and utilizing selected scanning tools to evaluate the specific IP addresses for known vulnerabilities that may exist in the firewall configuration.

Policies and procedures over firewall management at our company did not exist at time of review. This would include administration, change control, and backup procedures

over the CheckPoint Firewall-1. Rule sets should be clearly defined and modifications to the rule sets should follow an approval process based on a risk assessment methodology. It is recommended that each time a rule set is modified, the current copy is placed on file for audit purposes. Furthermore, since we have no backup and recovery procedures for the firewall, it becomes a single point of failure. If the firewall were to go down, our company would lose significant connectivity until the firewall is rebuilt or replaced.

Router

In addition, we reviewed the configuration of the Cisco 2500 router that resides between the Internet and the firewall. The objective for reviewing the Cisco 2500 Router was to determine that the device was performing as our network staff designed and intended it to. Routers, as well as other filtering devices, potentially act as a choke point so the network can determine if certain network traffic should continue or if the network traffic should be denied further access. It is important to review the security settings and configurations of the routers as they control traffic. If these routers were to be compromised, the network traffic could be hindered.

Currently, our internal network architecture is structured with three sub-nets – Demilitarized Zone (DMZ), Development (DEV), and Internal Network - allowing inbound Internet traffic to access the internal network. After a review of industry best practices, we redefined the network architecture so that it is segregated into two logical sub-nets, the DMZ and the internal network. 1 - The DMZ should contain all routable/accessible machines via the Internet. An inventory of the machines accessible from the Internet should be reviewed on a regular basis. Only machines that have undergone system hardening should be located in the DMZ. However, if the information contained on the system is deemed critical it should not be located in the DMZ. 2 - The Internal network should contain all non-routable systems. No inbound traffic should be allowed to the internal network without specific firewall rule sets.

4. Internal Vulnerability Scans

The assessment team's objective was to review the internal security infrastructure to assess the completeness of design against currently known threats and vulnerabilities. For this phase we performed an exhaustive analysis of the security enforced at the operating system level. Unlike external penetration testing, host vulnerability assessments are directed at the operating system.

The automated software tools ESM and ISS were used in this phase of the assessment. The host-based review, utilizing ESM, included an interrogation of selected machines identifying common mis-configurations and general administrative security weaknesses. A number of mis-configurations were identified with rankings from high severity to medium severity to low severity. A number of inactive accounts, shared directories with full access, and logon script access were found to exist on the

system. ISS was utilized to identify vulnerabilities on the internal network systems. The internal scans were compared to the external scans to identify common threads of vulnerabilities.

Given the number of vulnerabilities identified in our assessment, it was recommended that our organization harden the NT operating system. Once a machine has been hardened, security policies can be implemented across the NT platform. In addition, Axent's ESM tool should be used to continuously audit for compliance, not just during instances of security assessments. The ESM tool should be configured to incorporate the baseline and corporate policies and procedures. ESM will perform a variance check on a periodic basis to determine what parameters have changed. For the limited machines that are running Solaris, Axent's ESM tool should be utilized to audit for compliance of established standards.

5. ASP Security Review

The ASP security review included an evaluation of the contract, firewall rule sets, interviews with ASP personnel, and penetration tests to ensure the ASP is incorporating proper security controls. The assessment team's objective was to review the ASP implementation of Extranet technologies (firewall, routers, web servers, etc) and to validate the aforementioned products are configured and have been installed correctly.

Contract

The security team reviewed the signed contract to determine the services provided to our company by the ASP. The escalation procedures and the assignment of severity levels were discussed in detail with the ASP personnel to determine the potential impact on our continued operations. It was agreed upon that the ASP would contact our organization when the severity level approaches the most critical classification (severity 0) to rectify the situation before taking further action. In addition, a clause was identified that allows either our organization or the ASP to terminate the contract with a 60-day notice. Our concern is that the allotted time is not enough and if the ASP were to terminate, it could potentially impact our organization's ability to continue operations within a 60-day timeframe.

Firewall Scans

Scans performed during our review included an assessment of machines located at our organization's ASP. Although our scans did not identify any significant vulnerability associated with the ASP's systems, discussions were held with the ASP personnel regarding the lack of notification of the scans. While the ASP actively logs all network traffic, their classification of an attempted network intrusion is less severe than what our organization's perceived expectations are. It is our recommendation that our

organization provide our ASP with notification standards in the event of port scans (five ports in sequence within five seconds), and "excessive" dropped packets from a specific IP address.

During conversations with the ASP, the possibility of an implementation of an IDS solution was discussed. This would permit real-time monitoring and would have alerted our organization's ASP of the scans we performed, as well as any other entities. Presently, our ASP does not offer an IDS solution. However, to increase the security of the system files, we talked with our ASP about installing TripWire, an active host-based IDS solution. While this would not have alerted our ASP's personnel of our scans, it would have provided assurance that the systems themselves have not been tampered with or compromised.

Firewall Rule Sets

A review of our ASP's firewall rule sets was performed to ensure appropriate firewall rule sets. We also conducted external penetration scans checking for known security vulnerabilities. We found no vulnerabilities.

Secure Communications

Also, through conversations with a number of internal personnel, a concern was identified about secure e-mail to communicate electronically with our ASP. Upon further consideration, our management is considering implementing secure e-mail solution such as Pretty Good Privacy (PGP). Encryption will enable our organization to communicate securely, both internally as well as externally, with our ASP. Messages and files can be encrypted so that only the intended recipient(s) can read them. Digital signatures, which are included in many secure e-mail packages, ensures the authenticity of messages and files. With the passing of the digital signature law, this may become more critical and will enable our organization to more effectively communicate with outside entities.

Next Steps

In this environment, it is important that our organization give appropriate emphasis to technologies and processes that will ensure the security of critical information assets is not being compromised as the company grows in size and complexity. Our internally performed *independent* security assessment recognized the following areas for improvement. The assessment team recommended that our organization give particular emphasis to the following issues:

1. **Continuous Security Assessments** – To protect the internal network, DMZ, and other applications using the Internet Firewall, a vulnerability test and other security assessment activities should be conducted by an objective, qualified information security professional. This would need to be performed each time modifications are made or new hardware/appliance is added to the network security

infrastructure.

2. **Intrusion Detection Systems (IDS)** – IDS systems are becoming industry standard for detecting attempted break-ins and notifying network personnel when break-ins have occurred. Network intrusion monitors are attached to a packet-filtering router or packet sniffer to detect suspicious behavior on a network in real time. IDS's look for signs that a network is being interrogated for attack with a port scanner or that users are falling victim to known traps like .url or .lnk, or that the network is actually under an attack such as through SYN flooding or unauthorized attempts to gain root access. Based on user specifications, these monitors can then record the session and alert the administrator or, in some cases, reset the connection and shun the attack. Although the FW-1 product has some alarming features, it is not an intrusion detection system, such as described above.

3. **Security Incident Response Capability** – Our organization needs to develop an incident response methodology that identifies the appropriate steps that need to be performed when an anomaly occurs. In conjunction, guidelines should be established that provide a clear interpretation of exactly what is our organization's definition of an anomaly. The methodology should be communicated to appropriate network administrator and kept up to date as changes develop.

4. **Cisco 2500 Router Configuration –** The screening router serves as the initial point at which our organization's network is visible to the Internet. It is extremely important to have this device secure from outside entities to ensure availability and security of our Internet connection. During the assessment team's review, we noted the following areas that require immediate attention. (1) The router configuration currently is set not to conduct any authentication techniques. The router should be configured to authenticate users attempting access. This would allow the auditing of individual logon IDs as well. (2) Passwords entered are visible in clear text. The command *service password-encryption* should be entered to enable the password to be encrypted. (3) There is no Access Control List (ACL) in place. The border router should be configured to mirror the firewall rules and allow only ports inbound and outbound that are built into the rulebase on the firewall.

5. **Restructuring of the Network -** Currently, our organization's network architecture is structured with three sub-nets - DMZ, Development (DEV), and Internal Network - allowing inbound Internet traffic that accesses their internal network. Arthur Andersen recommends that the network architecture be restructured so that it is segregated into two logical sub-nets, the DMZ and the internal network (1) The DMZ should have all routable/accessible machines via the Internet, and would include DEV. (2) The LAN should be all non-routable systems. No inbound traffic should be allowed to this network without specific firewall rule sets.

6. **Implementation of Secure E-mail Solution -** During the review, a concern was identified about secure e-mail to communicate electronically with the ASP. Upon

further consideration, it was the team's recommendation that our organization consider implementing public key encryption. This would enable us to communicate securely, both internally as well as externally, with our ASP. Messages and files can be encrypted so that only the intended recipient(s) can read them.

It was noted that because of the nature of the assessment and assessment team's background, all vulnerabilities might not have been addressed. Even if they were addressed at the time of report issuance, there are numerous additional vulnerabilities that have been identified, making our report semi-obsolete. Our final recommendation to the organization was to make this security assessment activity a constant, ongoing activity. People of all job descriptions, at all levels within our organization, must be aware and security conscious. It is everyone's responsibility within our organization to do their part to raise security awareness and enforce security standards.

References

Brooks, Greg. "Nessus – Get on Board". February 15, 2001.
URL: http://www.sans.org/infosecFAQ/audit/nessus2.htm. (June 27, 2001).

Carnegie Mellon University, Using the ps program to examine processes for signs of intrusive activity, March 7, 2000.
URL: http://www.cert.org/security-improvement/implementations/i005.01.html

CERT Incident Note 99-07. Distributed Denial of Service Tools. Nov 18, 1999.
URL: http://www.cert.org/incident_notes/IN-99-07.html

Farmer, Dan and Venema, Wietsa "Improving the Security of your site by breaking into it" Sun Microsystems (11/29/00)
URL: http://www.geocities.com/hackernet_99/breakintoyoursite.htm

Fyodor. "The Art of Port Scanning." September 01, 1997.
URL: http://www.insecure.org/nmap/p51-11.txt. (June 27, 2001).

Hildreth, Sue, "ASP Security: Why Firewalls Are Not Enough",
URL: http://b2b.ebizq.net/asp/hildreth_2.html

Information Security Policies Made Easy, Version 8 Softcover - 775 pp

Nelson, Michael, "Determining Windows 2000 Network Security Strategies",
URL: http://www.microsoft.com/technet/win2000/dguide/chapt-17.asp

Noordergraaf, Alex and Watson, Keith, "Solaris™ Operating Environment Security".

URL: http://www.sun.com/blueprints/0100/security.pdf

Rainbow Technologies, InfoSec Services, Spectria Division. "Security Review Checklist". 1997.
URL: http://www.infosec.spectria.com/articles/check-rvw.htm. (June 30, 2001).

SANS Institute, How To Eliminate The Ten Most Critical Internet Security Threats The Experts' Consensus, v 1.27
URL: http://www.sans.org/topten.htm(Sept 8, 2000)

Watson, Keith and Noordergraaf, Alex, "Solaris™ Operating Environment Network Settings for Security".
URL: http://www.sun.com/blueprints/1200/network-updt1.pdf

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event