Global Information Assurance Certification Paper

Case Study of Hardening a Small Business Network

Andrew Clark
Date Submitted: 02/18/2004
GSEC Practical v1.4b option 2

Abstract:

This is a case study of a small business network that needed to be overhauled to introduce a new web based application and hardened against intrusion and misuse by using the principles of defense-in-depth. The paper will describe the network before the project began and what steps were taken to upgrade and change the network layout. It will then give a high level illustration of some of the concepts that were demonstrated in the GSEC class and compare how they were used to improve the network.

Network Background

Beginning

The organization in this paper is a membership services organization with around fifteen employees on staff, but it has to provide services to a membership of over twenty thousand people that are licensed by the state. One of the main services that this organization provides is making continuing education classes available to its members to meet the state requirements for keeping their license current. A decision was made to introduce a new online registration system for these classes using an in-house web server and database server.

The existing network layout consisted of a dual ISDN connection coming into an Ascend router. The router then went to either a proxy server (Windows NT 4.0 running MS Proxy Server 2.0) that served the internal network of the company, or a web server (Windows NT 4.0 running Internet Information Server 4) that served static web pages. The administrator password for the router had been forgotten, so we could not easily alter its configuration. Behind the proxy server was the internal network that had the staff workstations and the internal servers.

During

In order to support the web traffic, the organization decided to replace the existing ISDN with 4 channels from a T1 that served the telephone system, and also have a DSL line brought in for redundancy. The internal network was also going to be reconfigured and updated to increase security.

A Cisco 1720 router was purchased to combine the two data pipes and bring them into the network. It was configured to perform Network Address Translation on both of the IP address ranges from the data pipes, and to bring them into the 172.16.x.x range on the inside network interface. The Cisco also used access control lists to analyze inbound network traffic preliminarily.

From the Cisco, the inbound network traffic went into a Netscreen 25 Firewall appliance for further inspection and another round of NAT. The Netscreen has 3 network interfaces – Trusted, Untrusted, and DMZ. The Untrusted interface received the data from the inside network interface of the Cisco. From there, the Netscreen would analyze the packet, and route it to the appropriate interface (Trusted or DMZ) or drop it if it did not match an “allow” rule for a specific port or IP address.

The DMZ interface was used for a web server that only had static information and was updated infrequently, and for a mail server that was used primarily for listservs.

The Trusted interface on the Netscreen went to a hub that had the web and database servers for the new application attached to it, as well as the external interface of a server that has Microsoft Internet Security and Acceleration Server 2000 running on it. The internal interface of the ISA server machine led to the switches that connected all of the internal workstations, file servers, and Exchange server.

The internal network was updated from a collection of Windows 95 and 98 clients connected to Windows NT 4 and Novell servers to Windows 2000 workstations connecting to a Windows 2000 Active Directory Domain. The email server was updated from a POP3 mailbox server (SLMail) to Exchange 5.5 for the better messaging and collaboration services it provides. Ultimately this was upgraded to Exchange 2000 for Active Directory integration.

See appendix A for a network diagram of the new layout.

Comparison of Concepts

Physical Security

The physical security of the network was actually slightly worsened during the change in the network layout. The main server room that houses all of the servers and switches for the network is centrally located in the building, and the door is locked when the IT staff is not onsite. Originally, the ISDN lines terminated in the server room, and the Ascend router was also in there. When the T1 and DSL lines were brought into the building, they were terminated in the telephone equipment room at the rear of the building, which is not locked and doubles as a small storage room for cleaning supplies.

This means that the DSL modem and Cisco 1720 router are both in an unsecured area of the building. This risk was deemed acceptable, in part because the office is small enough so that all of the staff members know each other. The front office personnel were advised to alert the IT staff if someone comes in and claims to be there to work on any of the equipment.

To further control access to the network, we performed an audit of all workstations in the building to make sure that there are no unauthorized modems, wireless network cards, or other communications devices that might allow someone to bypass the firewall. We also disconnected the network jacks in the public areas of our building (classroom, boardroom, and reception area) from the switches that serve the internal network.

From time to time, there are requests for internet access to be provided to an instructor who is using our classroom or for a meeting that is occurring in the building. To provide this access, we placed an 802.11b wireless router outside of our Netscreen Firewall, but inside the Cisco router. This places anyone who uses this router outside of our primary network firewall. For additional security, and to prevent anyone from stealing our bandwidth, the router is left unplugged unless specifically requested, then it is again disabled after the meeting or class is over. The wireless router utilizes WEP encryption and is set to not broadcast its SSID.

Perimeter Network Security

The network perimeter was originally guarded by the Ascend router that fed into the web server or the Proxy server that served the internal network. This router was essentially unconfigurable because the admin password had been forgotten. The new design takes into account the principles of "defense-in-depth" and adds an extra layer of firewalling and traffic analysis, as well as a more robust firewall device.

The Cisco router uses the firewall commands and extended access lists (as illustrated in the Cisco IOS Security Configuration Guide) that are available in the IOS 12.1 to allow only the required ports through for inbound traffic, and use stateful inspection on the traffic for the appropriate protocols. It then performs a round of NAT on these inbound requests, translating the traffic to IP addresses in the 172.16.x.x range that the Netscreen expects.

The Netscreen 25 also performs port blocking and stateful inspection, allowing only the necessary ports through on a specified IP address. Some of these ip addresses are mapped to the DMZ interface on the Netscreen, and translated to the 10.0.0.x IP address range, and some are mapped to the Trusted interface and translated into the 192.168.0.x IP address range.

The 192.168.0.x IP address range contains the web and database server for the new registration software, as well as the external interface of the ISA server. The ISA server performs NAT from the 192.168.0.x range to the 192.168.128.x range, which includes the internal network file servers, workstations, and the Exchange server (which is published through the ISA server and mapped through the Netscreen and Cisco to a public IP address).

To prevent unauthorized access attempts, we have set the Cisco to only be configurable from the console. In practice, we have never needed to telnet in and configure it from the outside world, and we decided that the inconvenience in having to go to the telephone equipment room with a laptop was worth it for the increased security it affords us. The Netscreen firewall was similarly configured, except that it is accessible via a web interface, but only to traffic coming from its Trusted network interface.

Disaster Recovery

The disaster recovery procedures have essentially stayed the same for the internal parts of the two versions of the networks. A limited amount of downtime was deemed acceptable for any of the servers on the internal network and web and database server that power the registration software. A seven tape changer was installed both on a file server in the internal network and on the database server behind the Netscreen appliance to perform nightly full backups of all of the primary servers on the network. The nightly and weekly backup tapes are stored in a fireproof vault on the premises, and the monthly backup tapes are stored in a safe deposit box off-site.

Duplicate hardware was purchased for both the primary application web server and database server so that in case of an extreme hardware failure we could just restore a backup to the exact same hardware configuration for a minimum of downtime.

One of the things that changed during the course of changing the network is that there is now a central repository for network information. We have assembled a "Big Book of Network Stuff" that contains network diagrams, printouts of the router configurations, information on the hardware and software of each server, and details notes that contain information that may be pertinent during a time of crisis. This information will also come in handy in getting a new IT staff person or outside consultant up to speed on the network design. It also contains printouts and electronic copies of the complete router configurations, as well as a copy of any necessary floppy disks (Emergency Recovery Disks, floppies with generated passwords on them, etc.). There was nothing like this in place with the old network configuration.

Authentication and Access Control in the Internal Network

One of the best things that was done was the implementation of a stricter password policy. There was essentially no password policy in place originally, and passwords such as "12345" or a user's last name were commonplace. There was also no requirement to change a password at a set interval.

This was changed as the Active Directory Domain was set up. We used group policy to implement a stronger password policy that passwords had to be at least 6 characters long, contain at least one number and a mixture of upper- and lower-case letters. The passwords could not contain any part of a user's name, and had to be changed at regular intervals. An account lockout policy was also implemented where if a user failed to successfully login 3 times the account was locked out.

We used groups to give people their appropriate permissions and for ease of administration. People in the "accounting" group had access to certain network shares that they needed for their accounting software, and people in the "membership" group had separate access to other files that they needed. Everyone had access to his or her own private "Home" directory on the network.

The adoption of the Windows 2000 Professional workstations also allowed us to restrict what the users were able to do with their desktop computers. Most users were assigned "Restricted User" status at their desktop computers so that they could not install programs or change registry settings without the assistance of the IT staff. This helped to keep unauthorized programs off of the computers and network. The Windows 2000 workstations are also more easily configured from a central location with the user of Group Policy.

Incident Handling

There was and still is no written policy about incident handling, but the course materials have given us a better understanding about what to do in the case of an incident. There are two IT staff people, and either one could be the primary incident handler, depending on when the incident occurred and how it was discovered. The intrusion detection systems on the new network should help in discovering and alerting us to an incident

First, we now know that we need to preserve any files that could be thought of as evidence, including logfiles, in the case of an incident. We also need to find out what the root cause of the incident was, so that we can fix that weakness – whether it was a bad firewall configuration, a weak password, or a personnel or training issue.

Once we have identified an event as an incident and fixed the immediate problem (possibly isolating the effected system), we know that we should reevaluate our configuration. We should see what the root vulnerability that allowed this to happen was, as well as reexamine all of the contributing factors – if any unnecessary services are running, if our password policy is strong enough, if our firewall configurations are restrictive enough.

After the root cause has been fixed and the system cleansed or restored from a good backup, we would then test and put the machine back into the production environment.

Email/Web Security

The former email server was SLMail sitting on the server at the perimeter of the network that had Proxy server on it as well. When we moved to Exchange server and ISA server, the Exchange server moved inside the network, and was published through the ISA server, instead of being directly exposed. We also

adopted the “Outlook Web Access” (OWA) functionality of Exchange 2000 server and published that through the ISA server.

OWA allows us to access our email remotely via a web browser in a form that mimics the functionality of the Outlook client that we use in the office. This is done over an SSL connection so that logins and emails are encrypted. This was implemented to encourage staff to move away from unsecured POP3 and IMAP sessions for checking their email. Also, this tends to keep the emails in the mailbox on the server so that we can be sure to back them up. The POP3 clients would often be configured to remove the messages from the server, making them unavailable to the person while they were in the office, and unrecoverable if something happened to the client that they were downloaded to.

Since the OWA component is a web service, the URLScan tool from Microsoft was installed both on the web server and the ISA server that it was published through to try to prevent any exploits via a malformed url request. The URLScan Tool is installed on all exposed web servers to help prevent these types of exploits

Intrusion Detection

To track what traffic was going into and coming out of our network, we decided to go with a mixture of host-based and network based intrusion detection systems.

For the host based intrusion detection, we used the SiteProtector clients and console from Internet Security Systems. We installed the clients on the two primary systems we were concerned about – the database and web server for the registration software. We installed the clients onto the servers and set up a new machine for the console. The console is set to email alerts to the IT staff, and it is manually checked in the morning and evening on workdays.

For network based intrusion detection, we chose to use Snort. We configured two Snort machines, one behind the Trusted interface of the Netscreen and one outside the Untrusted interface. Both are attached to the network via a receive only cable. The logs for both machines are monitored daily for suspicious activity. One of the drawbacks to the Snort machines is the necessity to manually download and apply new rules.

To help detect any incursions into the internal network, the intrusion detection built in to ISA server was activated and configured to modify the IT staff via email alerts in case any attempts are detected. The system logs for all of the servers are set to log failed authorization attempts.

Virus Scanning/Malware

In the old network configuration, the servers had outdated virus scanning software, and the clients had desktop virus software that had to be updated individually. The newer configuration had newer software that was easier to keep up to date, as well as outside email scanning.

Norton AntiVirus Corporate Edition was chosen because of it's ability to be centrally managed. The client software was installed and configured to be managed by the Symantec Management software that was installed on one of the file servers on the internal network. This file server was configured to look for virus updates via Symantec's Live Update twice a week, then distribute those updates to the clients. Full system scans on any of the clients can also be performed from the management software. The clients are configured to scan all floppy disks inserted and all files as they are accessed using it's "Realtime System Scan" option.

Norton AntiVirus for Microsoft Exchange (NAVMSE) was installed on the Exchange server to scan incoming mail and everyone's mailboxes for viruses. NAVMSE was also configured to disallow certain attachment types that commonly carry viruses (.exe, .cmd, .vbs, .bat, etc.). NAVMSE was also set up to check for updates twice a week via the Live Update software. As an additional security measure against email viruses, we subscribed to a spam/virus filtering service from MailProtector.biz.

To monitor malware on the inside of the network trying to communicate out, we look to the ISA logs. Since ISA is the sole link from the internal network to the outside world, we monitor the ISA logs and reports for any deviations from the baseline traffic or requests.

General Windows Security

Using Group Policy, we can alter the security settings for all computers within the domain from a central point. These settings include certain behaviors for the computers that can have an impact on security, including startup and shutdown behaviors. We have used Group Policy to alter the default settings of Internet Explorer, change the settings for the local event logs, and made minor modifications to make the workstations more secure. We can also use Group Policy to implement scripts for users.

Patch/Update Management

As new security vulnerabilities and their fixes are announced, it is important to stay up to date with critical patches and hotfixes. This is accomplished in many ways.

For our servers, we periodically run Microsoft's Baseline Security Analyzer (MBSA) on them to check them for missing hotfixes and service packs for not only the operating system, but the server applications such as Exchange and SQL Server that run on them. This had previously been accomplished by using the "hfnetcheck" tool, but MBSA makes the task much easier. We then download, test, and apply the latest patches as necessary.

To keep up with patches and service packs for the desktop machines, we have installed a Software Update Server in the internal network. This server will automatically query Microsoft for new updates once per week. As it downloads new updates, it will present them to the administrator for approval. Once the updates are approved, they are sent to the clients via their automatic updates software (configured through Group Policy to look to the SUS machine). We will also occasionally use MBSA to scan individual machines to make sure that the updates are being applied appropriately.

Some additional tools in keeping up with patch management are subscriptions to various Security Focus mailing lists (including BugTraq) and the Microsoft Security Notification Service. These mailing lists should help to make us aware of any newly issued patches that are critical to the safety of our computing environment, even before they would normally be discovered using the Baseline Security Analyzer or downloaded via Software Update Services.

Remote Management of Servers

The previous version of the network had no way to remotely administer the servers, and this was a requirement for the new network layout. After looking into both VPNs and Terminal Services to remotely access the servers or the network, we found a product from Belkin called the Remote IP Console. It is a black box solution that suited our needs perfectly. It was essentially a web based terminal server, but the terminal window was actually a duplication of what we would see off of our KVM switch in our server room.

This solution was good for us in many ways. The Remote IP Console did not require any clients or extra services to be run on the servers, so there was no overhead. It would run in any Java capable web browser. It would use a secure communications channel because it could be run over SSL. It would also allow us to remotely get to the BIOS settings of the servers, if needed.

Since this was such a powerful tool, we protected it by generating a very strong password and changing it often. In keeping with the principle of defense in depth, we also make sure to lock the screens of the servers that the Remote IP console can see, so that if someone did manage to get control of the console, they would still have to know the passwords for the servers.

Penetration Testing

In order to validate our security in place at this point, we approached management and received permission and funding to conduct a penetration test. We contracted with an outside firm (Red Bull Technologies) to test our network, with the specific goal of compromising our web and/or database server to the point where they had database access. The results were very positive, and the primary flaw that they found was that the default password was left on our DSL modem by our ISP. This led to a denial of service, but once the flaw was discovered, the password was quickly changed to a much stronger one. After an aggregate 60 hours of testing, they were unable to breach the network perimeter or compromise the web or database servers.

Aftermath

While we have taken steps to make our network more secure, we recognize that a secure network is a "moving target" and that we must consistently work to stay informed of new threats to our organization's security, both internal and external. One of the most dangerous concepts is that "we don't know what we don't know", and this is what we must avoid. It is only through continuing education about security and related issues, constant monitoring of the network for "incidents", and a constant re-evaluation of the state of our systems that we can keep our network and systems as secure as possible.

References

”Cisco IOS Security Configuration Guide, Release 12.1” Cisco Systems 15 September 2002. URL:http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt3/index.htm (12 January 2004)

“Microsoft ISA Server 2000 – Configuring and Securing Microsoft Exchange 2000 Server and Clients” Microsoft Corporation 2001. URL: http://www.microsoft.com/isaserver/techinfo/deployment/ISAandExchange.asp (8 October 2003)

Gross, Chad. “How to Configure Outlook Web Access (OWA) to use Secure Socket Layer (SSL) on Microsoft Small Business Server 2000”. URL: http://www.sbs2000.info/sbs2000/How_do_I_configure_OWA_with_SSL.aspx (October 2003)

“How to use URLScan” Microsoft Corporation URL:http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secmod/html/secmod114.asp (1 December 2003)

Bull, John. “Snort’s Place in a Windows 2000 Environment” 15 April 2002. URL: http://www.snort.org/docs/snort-win2k.htm (September 2003)

“White Paper: Microsoft Baseline Security Analyzer V1.2”. Microsoft Corporation. January 2004. URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/mbsawp.asp (28 January 2004)

“Software Update Services Deployment White Paper”. Microsoft Corporation. January 2003. URL: http://download.microsoft.com/download/c/d/8/cd8ac959-37a8-4e5b-860a-465b179984af/SUS_Deployguide_sp1.doc (October 2003)

Appendix A. Diagram of the New Network Design