Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Securing the Gold through Better Network Design: A Case Study

I was also given the responsibility of assessing, designing and implementing a network design that would allow us to offer more services to the customer base and to the field service personnel. Management wanted to deploy a web-based service for the customers to enable them to access their account information and the company was in need of a network overhaul. Upon initial evaluation, I found no firewall protection for the network. The domain controller and mail server were exposed to the Internet and therefore vulnerab...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn More

Securing the Gold through Better Network Design: A Case Study

Todd Sheppard
GIAC Security Essentials Certification (GSEC)
Practical V1.4b option 2
June 2003

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract

I work for a small, privately owned company that specializes in marketing and servicing office equipment. I was hired to introduce new technologies to the sales force in order to enhance the solutions-based selling approach. I was also given the responsibility of assessing, designing and implementing a network design that would allow us to offer more services to the customer base and to the field service personnel. Management wanted to deploy a web-based service for the customers to enable them to access their account information and the company was in need of a network overhaul.

Upon initial evaluation, I found no firewall protection for the network. The domain controller and mail server were exposed to the Internet and therefore vulnerable and the company's database management system was not well secured. I felt that setting up the additional services in the existing infrastructure was not wise and presented my assessment to management. It was decided that a new network design should be implemented that would allow the company to offer additional services to the customers while providing for the security requirements. The new design was based on the Defense in Depth strategy. [1]

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Before Network Redesign
(Before Network Redesign diagram, page 15)

Main Office
Desktop operating systems consisted of Windows95, Windows98, and Windows NT4 workstation.
There were two servers at the site, one running Windows NT4 and the other SCO UNIX OpenServer 5.
The Windows NT4 server was the domain controller. It was configured to run Exchange, Proxy and Virtual Private Network (VPN). It also functioned as the data backup server for all Windows-based systems. Having all these services running on a single computer provides little security to an organization.
The SCO UNIX server was the company's management system. It controlled all finance, inventory, payroll, dispatch and marketing research functions. No update patches had been applied. The default installation had been used to install the Operating System (OS) leaving many unnecessary daemons running.
Physical network hardware consisted of three 10bT hubs cascaded together to create one physical network. Hubs are open to sniffing all traffic.
All traffic to and from the Internet was managed by the Proxy and ISDN Network Address Translation (NAT)/Router.
Service Packs and updates were not current.

Protocols
TCP/IP was the main protocol utilized. Occasionally IPX/SPX and Appletalk occurred when testing was done on the office equipment.
Outbound Internet communication required an MSProxy client. This made updating the SCO UNIX computer difficult.
Inbound Internet communication was controlled by an ISDN router that allowed all protocols and ports access to the MSProxy server which forwarded the packets to the internal network. Packet Filtering was enabled on the proxy.
Ports allowed by the proxy were:

> Inbound only: ICMP Source-Quench, ICMP Timeout and ICMP unreachable.
> Outbound only: all ICMP was allowed.
> Allowed both directions: PPTP, TCP ports 1021, 119, 20, 21, 389, 82, 49152 – 65535, POP3, SMTP and all UDP ports.

Ftp, port 21 can be very insecure. Many Trojans use ports 49152 – 65535. There was no reason for POP3. Reconnaissance can be done through UDP ports.
Administrative communication with the router was accomplished via telnet. Telnet communicates in plain text and is easily sniffed.
All communication inside the private network with the SCO box was through telnet. Passwords could easily be sniffed with a tool like TCPdump.

Passwords/Logon/Logoff
Root access to the SCO UNIX server was controlled by a dictionary based word. Dictionary based passwords do not take long to break.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Root access via telnet was allowed. Root access should never be allowed from a network connection. Telnet transmits in plain text.
The Windows domain password was 9 alphanumeric characters. More complexity is necessary for a domain password.
Users were required to create a five character level of complexity in their password assignments. There were no restrictions on the number of times they could reuse the same password. Five character passwords are trivial to brute force crack. Reusing passwords is as bad as no passwords.
The password for the ISDN router was same as the Windows domain Administrator password. Router passwords and domain passwords should never be the same.
Systems were not set to log off after a designated time period. Administrators forgetting to log off create holes in the defense.
Any user could reboot all computers.
The last user to logoff a computer was displayed. Last user should never be displayed.
There were no logon banners. Notifying a person that they are about to break the law will prevent some people from attempting to log on.

Event Logging
None. There are no records left as forensic evidence.

Network Policy
No defined policy for usage, conduct or IT procedure. No one knows what is not acceptable.

Firewall
None. Connections coming into the organization are not controlled.

Data Backup
The SCO server had a malfunctioning tape backup system. Disaster recovery could be a problem.
The Windows NT4 server also had a tape backup system.
All documents created on the Windows workstations were saved by default to the Windows NT4 server.
Backups for both systems were conducted nightly, with an offsite backup being done on the weekends.
Tapes were rotated on a weekly basis. Tapes should be rotated on a monthly basis for longer recovery of good information if corrupt backups start to happen.

Physical security
The servers and networking equipment were housed in a 4ft X 4ft closet.
There were no access restrictions to the closet or servers.
All external drives were active.
There was no fire suppression system. The closest fire extinguisher was at the other end of the building, at least 150 ft away.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The IT department had offices upstairs. The only person who could readily observe the networking closet was the receptionist. The receptionist was not aware that the server systems were off limits to general users, guests and non-IT staff.

Remote Office
The remote office used Windows98 in a peer-to-peer environment.
A dialup ISDN Router controlled Internet access.
A VPN tunnel, which was very unstable, achieved remote access to the main office's internal network.
No local authentication was necessary to utilize local resources.
No inbound connections were allowed through the router.

Network Redesign
(Network Redesign diagram, page 16)

After assessing the current network structure, numerous areas for improvement and redesign were identified. The structure of the new network was planned, including new services to be instituted and old services to be eliminated. Then a framework network policy addressing the setup of new computers, servers, baseline security, and testing measures was designed. After putting together a plan of action, physical changes were begun. This permitted the addition of a firewall which enhanced the level of security and facilitated the implementation of the redesign plan and service enhancement. After the firewall implementation, the Demilitarized Zone (DMZ) was created and changes to the physical network infrastructure were begun. The process continued by removing the proxy and VPN connections and deploying dedicated servers into the DMZ to facilitate Internet Information Server (IIS) and email services. All computer systems were brought up to the baseline network policy. The redesign of the network rooms and IT offices was initiated. Upon completion, a comprehensive network policy and procedure manual was written.

<u>Specific issues addressed throughout the process</u>
Router.
Firewalls.
DMZ.
Infrastructure.
Domain control.
Email.
IIS 5.0.
Domain Name Service (DNS).
Passwords and Logon screens.
Systems consolidation.
Event Logging.
Protocols.
SCO UNIX.
Tape backup systems.
Server room redesign.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Remote office upgrade.
Network Usage Policy and IT procedure.

Additional services added
Outlook Web Access – OWA.
Web to Host interface.
Customer account detail display web interface.
Intrusion Detection System – IDS.

Router
Secure router to console access only. For physical security the router is locked in a closet.

Firewalls
One of the first goals was to place a firewall into the system. After considering several commercial firewall vendors I settled on the idea of creating a firewall utilizing Linux and Netfilter/iptables. [2] Several of the commercial vendors I considered were using the iptables or ipchains infrastructure, so I felt that the technology was suitable for securing the network. Several vendors had prettier GUI's for managing the firewall and many offered extended service contracts but one of the driving factors was the amount of money the company could spend. I assessed the level of bandwidth necessary to handle the Internet loads. The bandwidth requirements were not such that we needed extremely high throughput. Cost, usability and the ability to customize the firewall to the environment made Linux iptables the logical choice. The opportunity to learn a new technology also played into this decision.

I gave careful consideration to which technology to use under Linux for creating the firewall. I read everything I could get my hands on about iptables and ipchains, setting up and writing connection rules and the best way to protect and log information about inbound and outbound connections. I chose iptables over ipchains because iptables is capable of connection tracking, [2] making it much easier to write rules when setting up the firewall. I started with a base script written by Stephen A. Zarkos [3] and customized it into a script that would work for this installation. I found the packet filtering capability quite robust and it was not difficult to learn to write the rules to do exactly what I needed them to do. I also took advantage of IP Masquerade, the Network Address Translation (NAT) capability built into Linux. [4]

After choosing the technology, I looked at the different Linux OS distributions on the market. Considering the advantages and disadvantages of the different distributions, I decided to utilize Redhat 9 as the distribution for the firewall. The next task was securing the minimal base installation of Redhat 9. I read many different publications on securing and hardening Linux and decided to use Bastille Linux [5] to be certain I hadn't overlooked anything in the setup. The Linux box was stripped of all unnecessary services and any non-essential software was also removed.

Access to the firewall is now accomplished via Secure Shell (SSH) or a console plugged into the machine. Passwords must now meet a complexity level of at least 21 characters

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

in a combination of upper and lower case letters (dictionary words not permitted), numbers, and symbols. Root access is given only at the console. Users who have access are automatically logged off the firewall within 2 minutes if no activity is detected at the console or the SSH connection. Sendmail has been removed as a daemon and now runs as a cron job every 15 seconds. Tripwire was installed and configured to send me an alert if the machine is compromised. Logwatch also runs each night and sends me a report of all activity that has occurred during the day. All log reports are parsed and stored in other long-term storage facilities. SSH session connections may only be made from the corporate network and only from specified ip addresses. The immutable attribute is set on all password related files, including configuration files that should not change. [6] All non-essential users and groups have been removed from the system. All references to non-essential services have been removed. External drives may only be mounted by root.

Physical access has been restricted to the firewalls via lock and key. The passwords for the firewalls have been written down and are kept in sealed envelopes in a safe. Access to the safe is issued to three people in the organization.

Connections into, through and out of the firewall are strictly controlled. The default policy for iptables is to deny access to input, throughput and output. All connections must be explicitly allowed. This creates some overhead when writing rules but is manageable for a small or medium network. Most incoming ports are blocked from allowing new connections. New connections must originate from within the network with very few exceptions. This does not prevent a determined hacker from gaining access but it does deter the casual script kiddie. There are several ports requiring access to the DMZ in order for the Internet facing servers to do their jobs. I specifically allowed port 25 for email, port 80 for general web traffic to web server one, port 443 for https traffic to web server two and port 1912 for Persona's session setup to web server two. All inbound connections on the allowed ports are NATed to a particular server, thereby denying direct access to any other resources in the DMZ or corporate network. All known Trojan ports are blocked from inbound or outbound communication. Egress filtering is also enabled to make sure traffic is coming from appropriate sources inside and out.

I used a very similar setup for the internal firewall except it is triple homed to handle the additional subnet from the second Ethernet cards on web server two and the email server. I used Stephen Zarkos' "rc.firewall.iptables.multi" [7] script and modified it to this installation. Inbound communication to the corporate network is restricted to the third interface on the internal firewall. That interface is further restricted to the IP address assigned to web server two's second interface and the email server's second interface. Ports from those interfaces are filtered to DNS port 53, TCP port 22 for SSH, TCP port 7005 for customer account interface, TCP ports 135, 138, 4410, 4411, 5500, UDP port 137 and Echo for Outlook Web Access. Spoofing the web server's IP Address from the Internet is not a concern because the Internet firewall blocks inbound traffic containing private IP space addresses as the originating address. As an added protection all inbound new traffic is disallowed by interface two on the internal firewall.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

DMZ
The DMZ was created by adding a second, triple homed, firewall in front of the corporate network to isolate the Internet facing servers in the DMZ. The external firewall protects the DMZ and allows only connections to the Web and email servers. The internal firewall protects the corporate network from the DMZ. The DMZ was created with two things in mind. It needed to secure all Internet facing servers as much as possible and insulate the internal network from direct Internet access. Web servers and email have classically been targets for crackers and remain so. Placing them in the DMZ insulates our corporate network from direct attack.

The physical DMZ consists of two private address subnets. All inbound traffic from the Internet to the web or email servers is filtered and NATed through the Internet firewall. All communication to any resource inside the corporate network is restricted to the second interface of the web or email server. The connections are filtered, NATed and restricted to the two private IP and MAC addresses. The communication from these interface cards is further restricted to specific ports. All servers in the DMZ have dual network interfaces with IP forwarding disabled.

Infrastructure
It was decided to change the network infrastructure from hubs to switches. This enhances security but does not make it foolproof. Tools such as dsniff are quite effective at circumventing the protections provided by utilizing a switched network. Hubs are still used at critical junctions in the network by the IDS system enabling the sensors to sniff traffic. Consideration for future enhancements would include locking each node to a specific MAC address. At the present time we do not have a need for that level of security.

Domain Control
Patches and updates were applied to the domain controller utilizing the Windows installer v2.0 for Windows NT4. [8] The domain controller was moved inside the internal network to secure the user lists from crackers. A domain controller should never be run on an Internet facing server because tools such as L0pht are very adept at getting domain information from a Windows NT4 domain controller. It also violates the Defense in Depth strategy [1] because a cracker only has to penetrate one layer of the security model before gaining full access to all network resources. I think Domain controllers should be dedicated machines due to the overhead imposed on them and to help secure the user database.

Email
Email needed to be serviced by a dedicated SMTP server inside the DMZ. A couple of email servers were considered and it was decided that Sendmail would be the best choice due the wide support available on the Internet. Sendmail transfers email to the Exchange server inside the internal firewall. The specific details of this setup are readily available in other papers written and published on the Internet. I used an excellent paper by Jason McLellan, “A Secure Sendmail based DMZ for the Corporate Email Environment” to configure and secure Sendmail. [9]

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

IIS 5.0
A web server was critical to the services the company needed to incorporate for those accessing data from the Internet. Two web servers were placed in the DMZ. Web server one was setup as a forwarding server and general use server with no connections to the corporate network. Outlook Web Access, Persona and the customer account management were setup on web server two. Web server two has been configured with dual network interface cards. IP forwarding is disabled across the interfaces. I started by securing and patching Windows 2000 Server. I then installed IIS 5.0, secured and patched it. Two excellent resources I used while securing IIS 5.0 are:

> William E. Walker IV. "Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0" [10]
> Michael Howard. "Secure Internet Information Services 5 Checklist" [11]

I then decided to install and utilize Secure Sockets Layer (SSL) for the web sites because passwords are required to access the sites. Due to the cost of an Authorized SSL root Certificate, I decided to create my own using the instructions by Heath Stewart called "Setting up SSL for your Servers and Email". [12] Connections to the site are coming from employees or specific customers, so using a self-generated certificate does not pose a major problem. As funds become available, I will try to get an authorized root certificate. Search bots are disallowed from crawling our sites and posting the info or links found there.

DNS
The company utilizes a DNS server set to forward requests to the Internet DNS servers. Computers inside the corporate network are set to request DNS from this server first in order to maintain access to corporate and DMZ resources. Internet DNS is not allowed to transfer information out of the corporate zone.

Passwords and Logon Screens
Passwords must now be 7 characters long and meet a certain complexity level, including characters, symbols and numbers. [13] It was decided that passwords must be changed every 45 days and all computers have a default logon screen. Domain and server passwords must meet a much higher level of complexity than general user logons and must also be factors of 7 characters. [13] Router Passwords are no longer the same as Domain passwords and must be at least 21 characters long. All Router and Domain passwords are kept under lock and key in separate sealed envelopes.

Systems consolidation
It was decided to migrate the workstations to Windows 2000 Pro and servers to Windows 2000 Server. There is still one Windows NT4 server, the domain controller; however it will be upgraded shortly. A SCO Openserver 5 UNIX machine is maintained along with seven Red Hat Linux-based devices. Migrating the workstations to one OS was the primary goal because they seem to produce the greatest number of help desk calls. I also like the ability to automatically update the Windows 2000 Pro and Server computers through the update service. The SCO UNIX, Windows NT4 and all Linux computers are

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

updated manually at least once per week or when a critical update notice is sent to me from the Red Hat Network.

Event Logging
All transactions and interactions with computer systems are now logged locally and held for at least 30 days. A future enhancement will be a central syslog server and a Windows central logging server.

Protocols
The network utilizes the TCP/IP suite of protocols. SSH is used for all transactions in which telnet was previously used. SSL is used for all connections that require passwords on the web sites. IPX/SPX and Appletalk are no longer allowed on the corporate network.

SCO UNIX
The SCO UNIX server hosts the company's management system. It had not been updated since initial installation. The first priority was to install OS level patches to bring the server up to an acceptable standard. I used the patches that SCO recommends and are applicable to the system. [14] All non-essential daemons were turned off and removed. SSH was installed and all telnet sessions are now disallowed. We also brought it up to the new standard of password protection and activated some additional logging to allow us to see what was going on with the system. Thankfully, the system had not been compromised. The system runs much faster, now that unnecessary services no longer start by default.

Tape backup systems.
Tape backup was fixed on the SCO UNIX computer and extended to a monthly tape rotation to decrease the number of times a tape is recycled. All backups are full backups because not enough new data is generated each day to justify incremental backups. This will make it very easy to restore the systems should a disaster occur.

All Windows servers are backed up to a central tape backup system. A monthly tape rotation is also in effect for all Windows systems.

Weekly backups of all server systems are taken offsite for catastrophic disaster recovery.

Server room redesign
Redesign of the network room and IT department meant building new offices next to the server room and closing the server room off from the main entrance. Physical access to the server room now requires a person to enter the IT department and pass through a locked door.

Remote office upgrade.
The remote office was upgraded to a cable modem connection for Internet access. A Linksys router/firewall was installed. All inbound traffic is disallowed by the firewall. The network is peer-to-peer. All the operating systems were upgraded to Windows 2000 Pro, patched and locked down.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Network Usage Policy and IT procedure
An overall network policy was written and implemented. I recommended the idea of a human firewall [15] and it was implemented along with training procedures for all employees. The idea of the human firewall is that people are the weakest link in protecting company's network and computing assets. If employees can be taught how to create good passwords, follow good security processes and be accountable, the company's risk exposure can be reduced. IT policy and procedure was written for daily activities, incident response and disaster recovery. Acceptable use policies have also been formalized.

Along with addressing the internal infrastructure issues, several new services were implemented to offset the removal of the unstable VPN circuit. Descriptions of the added services follow.

Outlook Web Access – OWA
My mind reeled at the prospect of instituting a technology as full of holes as this one. Changing the entire organization to Suse's Openexchange server was considered. It has not been ruled out for future improvements. In the end, cost of migration and user familiarity won out. The company was already invested and trained in Microsoft's Exchange product. Now the question was, how do I "secure" this technology? After reading many different approaches, I settled on the recommendation by Jacek Nowicki in "MS Exchange Mail Access Based on Outlook Web Access." [16] I decided to use the dual network interface card approach as it gave the widest separation of functions I could get using this technology. This creates additional holes in the internal firewall but it is a risk the company is willing to live with for now.

Web to Host site - Persona
Rumba and Persona were considered for this function. Both were acceptable solutions. More assistance was received from Persona and the configuration was not difficult. It also created its own secured tunnel during use. This site also uses SSL and dual network interface cards to help segment and secure the communication with the internal network.

Customer account interface.
This is one of the least likely products to get my vote, but was necessary to institute as a service to the customers. The software allows a customer to retrieve and display information about their account, place service calls and order products via the web. It is the only software that will interface with the management database. The one positive thing about it is it only displays information about the customer's installed equipment. It will not allow manipulation of any critical data. SSL and dual network cards help secure and segment information requests from the corporate network.

IDS
The last technology installed was necessary to make sure connections getting in were not malicious in nature. I considered several commercial IDS systems and came to the conclusion again that I could better spend the company's money utilizing an open source

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

system and absorb the initial learning curve costs. I decided after reading several articles about the strengths and weaknesses of IDS that I would deploy a Snort based distributed network sensor system. [17] It would consist of four sensors, one on the outside of the firewall, two in the DMZ, and one inside the private network. These sensors are all tied to a main SQL database that captures the events as they happen and pages me if something negative starts to happen. The system runs on an independent physical network, so even if someone gets into the system it will be very difficult for him or her to cause damage to the corporate network. Future plans include the ability to dynamically shutdown connections that are occurring, but for now intrusion detection was in the financial and time budget.

Designing the distributed IDS was an interesting challenge in itself. As I stated before, I decided to utilize open source products due to their cost and availability and also because I enjoy the challenge to learn new things. I decided to use Red Hat 9 as the Linux distribution of choice because of my familiarity with the distribution. Hardware is very inexpensive and flexible when building a Linux based IDS. All sensors and the administrative station are equipped with dual network interface cards. All machines are configured with BIOS and boot loader passwords. Passwords at both levels were different. The downside to this configuration is, if a sensor goes offline it must be restarted with an administrator standing over it. Bastille Linux [5] is run on all machines to ensure that I did not forget anything.

The main database server consists of Linux Redhat 9 with all appropriate errata installed. Passwords are set to meet the minimum level of 21 characters. When configuring the Snort distributed sensor system I used the "Snort Installation Manual" by Steven J Scott. [17] The machine is configured with MySQL, Apache, ACID, Tripwire, SSH, SSL, logwatch, TCP wrappers, iptables, and Sendmail. I checked to see what ports are listening and trace back the listening ports to their services and shut them off if not absolutely necessary. The services installed perform the following functions. MySQL is the database where the captured info from the sensors is deposited. Apache is necessary in order to run ACID for trend analysis and setting up page alerts. Apache was secured as much as possible. I used the article "Securing Apache: Step-by-Step" by Artur Maj [18] to help with securing the service. I then activated only the technologies I needed for ACID support. Tripwire logs all changes in the system and keeps me apprised of the state of the system. SSH is in place to allow me to remotely administer the sensor database server. SSL is used to allow me to browse the ACID data display in a secure manner. I require logins to access any web pages on this machine and encrypting the data stream prevents someone on the network from using webspy to replicate the web data stream for viewing on their computer. I followed many of the suggestions given by Heath Stewart in "Setting up SSL for your Servers and Email" [12] and Richard Sigle's paper "Building a Secure RedHat Apache Server HOWTO" [19] when setting up SSL on this machine. Logwatch is configured to send me any unusual occurrences that happen in the log files. TCP wrappers tells the system who can and cannot attach to the particular service being offered without having to communicate with the originating host. [20] Iptables allows me to control what can or cannot access the sensor database computer. Sendmail is necessary

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

to email reports, alerts, etc. to me for further processing. Sendmail on the database server runs in daemon mode so it can receive alerts from the sensors and forward them to me.

Sensors are configured very similarly with the addition of Snort. Snort is the sensor software. It processes all network traffic and based on the signatures it is provided, logs anomalies to the database server. Sendmail is not run in daemon mode because it is not receiving any connections from the network; it is only sending information to me via the database server. I set it to run as a cron job every 60 seconds.

The sensors are configured with two network interface cards; one is for sniffing, left in promiscuous mode and attached to the network being sniffed. The patch cable attaching the sensor network interface to the regular network has been specially modified for reception only. [21] It is not allowed to transmit and there is no IP address assigned to it. The other network interface communicates on the isolated network with the database server. I could have designed a system that utilized the existing network but I felt that having a separate network for the sensor array leaves fewer holes in the system for penetration. As you can see the design allows me to watch over the network section by section. It alerts me to pending attacks by listening to the outside network. It lets me know when to isolate the internal network should someone break into the DMZ and it assists with forensic evidence of the attack and how it was carried out for later analysis.

Testing
After configuring each piece of the system, a variety of tools were used to engage and test for holes in each component before placing it into production. Nmap was utilized to see if any ports were listening or could be detected that I did not intend. Super Scanner was also employed to see if alerts were being transmitted. All systems were also stress tested to make sure they would hold up under different levels of input and processing.

Redesign Accomplishments

The new network design creates a more secure, multilayered approach to defending the gold. Starting with the packet filtering implementation at the firewalls, we have reduced the number of potential attacks on the DMZ and severely limited access to the corporate network. Creating the DMZ with private IP space places a buffer zone in front of the internal network and introduces a second layer of defense for the critical systems. Securing all Internet facing servers in the DMZ has further reduced the potential for successful attack. Allowing communication to the corporate network from specific network interface cards further reduces our exposure.

Having virus and spam protection on the email server has reduced the potential for malicious behavior. NATing and filtering packets at the firewalls makes attacking the internal network very difficult. On the internal firewall, disallowing Internet IP space from creating new connections to the internal network reduces the exposure further as does disallowing private IP space from traversing the Internet firewall. Implementing SSL for the web servers reduces the chance that someone will be able to get the passwords by sniffing the connections. Keeping logs of activity assists in determining

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

what is happening at the host level as well as leaving a forensics trail. Filtering all known Trojan and worm propagating ports at both firewalls for inbound and outbound connections again reduces the exposure to malicious software. As a result, the company remains a good citizen to the rest of the Internet. Virus protection at the desktop has reduced the chances of infecting other machines on the network should a virus or Trojan get through the defense perimeter. Implementing switches and SSH has further reduced the ability of an internal attacker from gaining access to critical infrastructure components.

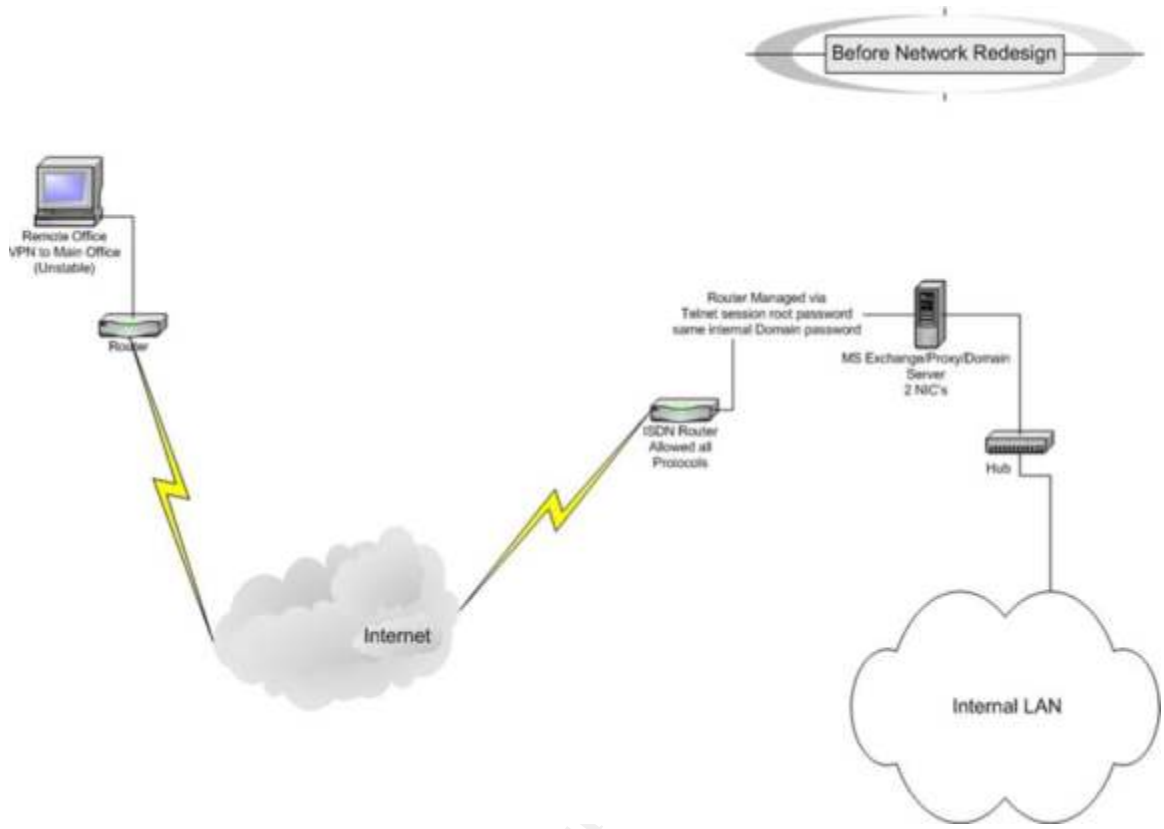
The distributed IDS assists in logging and analyzing all activity that is out of the norm. Attacks are detected starting from the outside and if they succeed, the internal network can be secured. The attack can then be observed to see what techniques are used to move through the layers of defense. This allows an understanding of what parts of the defense are not working correctly. It also gives advanced warning so the internal network can be fully secured if necessary.

The network policies help us understand what to do in the case of an emergency. It helps IT understand their areas of responsibility and it gives a contingency plan if one of the administrators is not available to handle a situation. The human firewall concept brings one more very important piece of the puzzle together as users are better trained and understand their roles and responsibilities when it comes to network resources. [15] Adherence to the human firewall policy is reflected in all employees' quarterly reviews.

Conclusion

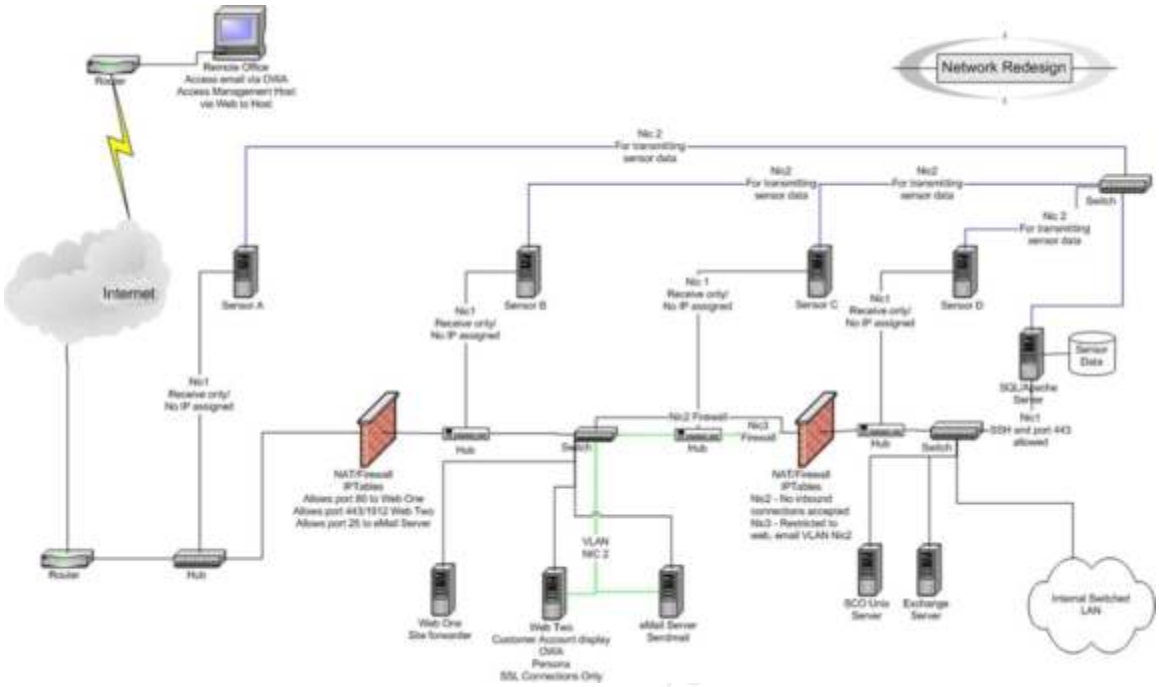
Security is a process. I do not think that all issues with this network have been formulated and addressed in their entirety. However, the network is much more secured than when I arrived. I mentioned several future enhancements within this paper, such as setting up a syslog server, instituting an Active Directory domain, having central logging for all systems, setting up host-based reporting to the IDS and implementing an intrusion prevention system. As with all things, time and money will see these things come. I have helped enhance the network security and I have contributed significantly to the Defense in Depth strategy [1] for this organization. There has been some cost but it has been nominal in comparison to the gold it protects.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



© SANS Institute 2003, Au

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

1. National Security Agency. "Defense in Depth." 10 June 2003. <http://www.nsa.gov/snac/support/guides/sd-1.pdf>

2. Russell, Paul. "Documentation" 28 May 2003. <http://www.netfilter.org/documentation/>

3. Zarkos, Stephen. "rc.firewall.iptables.dual." 28 May 2003. <http://www.sentry.net/~obsid/IPTables/rc.scripts.dir/current/rc.firewall.iptables.dual>

4. Ranch, David. "Linux IP Masquerade HOWTO." 28 May 2003. <http://www.linuxdocs.org/HOWTOs/IP-Masquerade-HOWTO.html>

5. Beale, Jay & Lasser, Jon "Bastille Linux." 10 June 2003. <http://www.bastille-linux.org/>

6. Galitz, Geoff. "Rootkits: Hiding a Successful System Compromise." 28 May 2003. <http://www.iwar.org.uk/comsec/resources/root-berkeley/rootkit.htm>

7. Zarkos, Stephan. "rc.firewall.iptables.multi" 28 May 2003. <http://www.sentry.net/~obsid/IPTables/rc.scripts.dir/current/rc.firewall.iptables.multi>

8. Microsoft. "Windows Installer 2.0 Redistributable for Windows NT 4.0 and 2000." 10 June 2003. <http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=4B6140F9-2D36-4977-8FA1-6F8A0F5DCA8F>

9. McLellan, Jason "A Secure Sendmail based DMZ for the Corporate Email Enivironment." 11 June 2003. <http://www.giac.org/practical/GSEC/Jason_McLellan_GSEC.pdf>

10. Walker, William E. IV. "Guide to The Secure Configuration and Administration of Microsoft Internet Information Services 5.0." 12 June 2003. <http://nsa2.www.conxion.com/win2k/guides/w2k-14.pdf>

11. Howard, Michael. "Secure Internet Information Services 5 Checklist" 12 June 2003. <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/iis/iis5/tips/iis5chk.asp>

12. Stewart, Heath. "Setting up SSL for your Servers and Email." 12 June 2003. <http://www.devhood.com/tutorials/tutorial_details.aspx?tutorial_id=209>

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

13. Microsoft TechNet. "Creating Strong Passwords." 12 June 2003. <http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/winxppro/proddocs/windows_password_tips.asp>

14. SCO. "OpenServer 5.0.7 Supplements." 12 June 2003. <http://www.caldera.com/support/update/download/osr507list.html>

15. The Human Firewall Council. "Blueprint for Building a Human Firewall." 13 June 2003. <http://www.humanfirewall.com/issues.htm#blueprint>

16. Nowicki, Jacek. "MS Exchange Mail Access System Based on Outlook Web Access." 13 June 2003. <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/exchange/exchange55/plan/ekmgem.asp>

17. Scott, Steven J. "Snort Installation Manual" 10 June 2003. <http://www.snort.org/docs/snort-rh7-mysql-ACID-1-5.pdf>

18. Maj, Artur. "Securing Apache: Step-by-Step" 10 June 2003. <http://www.securityfocus.com/printable/infocus/1694>

19. Sigle, Richard. "Building a Secure RedHat Apache Server HOWTO." 10 June 2003. <http://en.tldp.org/HOWTO/SSL-RedHat-HOWTO.html>

20. Red Hat, Inc. "Red Hat Linux Reference Guide." 10 June 2003. <http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/ch-tcpwrappers.html>

21. Freeman, Wayne. "Installing Snort, MySQL and ACID in an Enterprise Environment with a Centralized Logging Console and Distributed Sensors." 10 June 2003. <http://www.inetsecurity.info/downloads/papers/Snort_FreeBSD_dist.pdf>

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**