Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Small Business Security
Migrating to and Securing the Low Budget Office Network
Kolly Mars
4/10/02

With the ever-increasing popularity of Digital Subscriber Lines and Cable internet service the small business owner is inviting cyber criminals in ever increasing numbers. A new frontier is opening with ever expanding boundaries and the businessperson who takes advantage of this is, for the most part, completely ignorant of the potential threat that he unleashes.

This paper will attempt to expose the weaknesses of the small business local area network and give several methods of closing the frontier. The topics covered will be: development of a workable security policy, deployment of anti-virus software and the centralization of virus definitions, choosing a network operating system and secure deployment of it, choosing and deploying a firewall, and how an off site network manager can efficiently manage the whole kit and kaboodle.

Scope

First I would like to better define the scope of the small business for which this paper will be focused. Although the security impact of an unsecured network is quite large in the medium sized business, that size business generally has more capital to hire a full time or contract based computer security company. Perhaps the contractor that wires the office and procures and installs the network is also taking care of network security for that size business. But, the small to very small business owner probably has built her computer network on her own, or possibly with the help of a friend or employee. The simple fact is that with the barest amount of reading anyone can put together a Local Area Network. The computers are talking to each other and they have a connection to the Internet. No thought is given to the security of the network because after all it was an insurance agent who installed the network!

When you drive down the street of your town and you see the small to very small insurance company, or the small travel agency, how many do you see? The fact is that they add up to a very significant number of potential security problems. When you walk in to these offices to book travel, or to set up a new insurance policy for your car or home do you think about how secure the information is that you give them? Do the owners of the business itself think about how secure that information is? Do they know that they should be thinking about those things?

This paper will be from the point of view of the security consultant. This security consultant has just been hired to look over and secure a network for a small insurance company. Although this could be any small company I have chosen an insurance company because of the type of information (Social Security Numbers, Vehicle

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Identification Numbers, Bank Account Numbers etc.) that those companies deal with. The first task is the security assessment.

The first thing to be determined is the Network structure. By this I mean determining the Network Operating System, means and type of internet connection, hardness of servers and clients. It is essential to answer these questions before attempting to harden a network.

In this paper I will assume that we are dealing with a small independent insurance company with an existing Windows98 peer to peer network. Of course, the example could be any type of business with any type of networking environment. After performing a review of the network the following infrastructure was discovered. The office has ADSL internet access. All computers are connected through a 100Mbps hub. The ADSL router is using NAT to connect the clients to the internet. Two modems are connected to on of the computers, one for Symantec PCAnywhere dial in access, and the other is the legacy internet connection which is no longer used. The Internet service provider has given the office five static IP addresses, but currently the office is using DHCP provided by the ADSL router.

There are five steps in the process of going from a wide-open network to a secure office environment. They are:

1. Perform a Vulnerability Assessment and introduce a security policy
2. Harden the Server(s)
3. Harden the Clients
4. Isolate the Network
5. Change the mindset of the Office Personnel

Vulnerability Assessment

Based on the state of the Local Area Network (LAN) as described above it is not difficult to imagine the outcome of the vulnerability assessment. However, just looking over the network operating systems is probably not going into enough depth to form a realistic assessment. Several tools can be used to assess the vulnerabilities of a LAN and no one tool can be considered as the end all be all of vulnerability assessment. For example, several independent comparisons of Vulnerability Assessment Scanners have been published, and while some are better than others, no one scanner detects all vulnerabilities. Having said that, three methods were chosen to determine overall network vulnerability for this type of network. The first is a password cracker to determine what, if any, passwords are on the network. Second, is a network vulnerability scanner such as Nessus Security Scanner or Axent Technologies NetRecon. It should be added here that more than one vulnerability scanner is recommended since no one seems to accurately detect all vulnerabilities. Third, is a good virus scanner such as McAffee Virus Shield or Norton Anti-Virus.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

After performing the vulnerability assessment the following discrepancies were found:

- No password authentication was necessary to access the server's resources. This did not surprise me since the "server" was a Windows98 machine. Overall password strength was extremely weak with some workstations having no password at all. I could access the entire LAN by entering my name as a username and giving a null password.
- The ADSL router requires a password to authenticate itself to the ADSL provider. I found that this password was never changed from the default, and was left at 123456.
- The server was sharing the entire hard drive.
- Norton Anti-Virus was installed on the server and all clients, but the virus definition subscription had long since run out and was not renewed. Each user had become so used to seeing and canceling the warning message that it became second nature.

These discrepancies in the network were catalogued and put into a report. At this point, although much has been done, we have only a good working knowledge of the state of the network.

Since, in this scenario, we have been hired to secure this network, we are assuming that the office manager is prepared to spend some amount of money to bring the network to a secure level.

Server Hardening

Server hardening being the next step, a decision needs to be made. Obviously Windows 98 is not a preferred server. The server needed to be upgraded to a more secure network operating system. The question was which OS? After researching the applications required Linux was chosen. This choice was made for several reasons including robustness, configurability, out-of-the-box security, and last but definitely not least cost. The Linux server was built with RedHat Linux 7.2. A custom install was performed and the following services were deemed to be essential:

- Samba (smbd,nmbd)
- Ssh
- X window system
- Sendmail

At this point this server is designated as a Network File Server and was not installed with any services that would normally reside in the DMZ.

Hardening a server, especially the main file and application server begins with physical security. In most small offices the server is not or sometimes cannot be located in a locked room. There are, however, some things that can be done to overcome this problem. For this server the following was done:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Plug and Play disabled in BIOS
- System BIOS was password protected
- Grub Boot Loader was password protected
- Ctrl+Alt+Del was disabled
- Only root was allowed to log in from the system console.

After the physical security issues are address it is a good idea to ensure that only the ports that you need are listening. Using tcpdump or nmap can do this. The services that can be turned off should be removed by turning the corresponding services off in all run levels, or by editing /etc/services. It should be said here that after these recommended changes are made to the system the port checker of choice is rum on the system again to ensure that the changes were made correctly.

Hey, now we're getting somewhere! Let's review, the server is behind a router, which is using NAT, the server has been made physically secure, only the ports that we need to have open are open, and password restrictions and aging have been set. You may think that this is security deep enough to prevent all but the most diligent hacker. You may even be right, but with just a few more security measures implemented the server would be several times more secure.

Next, access to the remaining ports and services needs to be controlled, and some preventative tools need to be implemented. Controlling access to service can be done using TCP Wrappers and IPTables. Both of these are packet filter tools and can be used to limit access to ports based on several different parameters. RedHat 7.2 is distributed with IPChains as the default firewall but in this example the IPChains module was removed and the IPTables module was installed.
TCP wrappers was configured to allow only local machines access to the services listed above, and IP Tables was configured to allow access only from the local network addresses and no others. Samba was configured as a Primary Domain Controller and domain level authentication was implemented. Password encryption for Samba was enabled.

Now that we have a clean system we can install some intrusion detection tools. As usual there are several to choose from. Two server based detection tools were chosen. The first is Tripwire. Tripwire is distributed with RedHat 7.2 and after some configuration is an extremely valuable tool for detecting if important files have been removed, changed, or added. Although Tripwire does not prevent intrusion it does detect file tampering. The second tool implemented is PortSentry. PortSentry is a port scan detector that has the ability to act immediately to block intrusive scans from any host. Both of these tools have the ability to email the log files to an administrator. Another very important step is subscription to the RedHat Network. RedHat Linux as with several other operating systems are discovering and patching new security issues on almost a weekly basis. By subscribing to the RedHat network using a utility call rhn_register and up2date, the root user will be notified by email of any security patches

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

and errata fixes to that particular server. When rhn_register is run a list of installed software is sent to RedHat so that no unnecessary packages will be sent to your system. This makes it extremely easy to patch the server.

Next the operational software needs to be loaded onto the server. A fresh load is recommended with any available patches that the manufacturer might have. In reviewing the process of hardening our server we have secured the server on several different levels beginning with physical security and ending with port security. You can see now that for a hacker to get through the levels of security that have been implemented on the server they would have some real work to do. Having said that doesn't mean that the job is over, and this is a point that needs to be made to the office manager. The appropriate patches need to be made to keep up with current vulnerabilities, and log files need to be checked. After all it doesn't do too much good to have all these tools running if no one ever looks at them. But, the system is secure enough to be placed in an operational status, and all this without having to purchase any software besides RedHat 7.2. Not bad. Now we make two backup tapes, one "certified system" to be saved in case we need to start again, and one for operational backup purposes.

We have now hardened the server from external attacks, but almost 50% of all attacks come from inside the LAN either from disgruntled workers or non-compliance with the office security policy (assuming that the office has a written policy). So how do we keep the clients from killing the server?

Implementing Security Policy

The perception is that writing, implementing, and enforcing security policy is a mountain that no sane person would attempt to climb. The difficulty of writing security policy alone leaves one with their jaw dropped wondering how to start, let alone how to possibly cover everything that needs to be covered. Lucky for us there are several other more qualified people who have already written several security policies. The SANS Institute has a very fine set of templates that can be downloaded and modified to fit almost any size organization free of charge. By utilizing these templates security policy can be reduced from a mountain to a really big hill.

Enforcing security policy is a challenge that is not easy. The first and most important step is to make the office manager understand the importance of the policy. Once the office manager is on board the person enforcing the policy has the implied authority necessary to make the policy more that just a series of documents.

With this knowledge we can implement a security policy. Security policy templates, downloaded from the SANS Security Policy Project, can be modified to suit almost any office no matter how small (or large). Although this office does not need all of the templates the following templates were modified for use in this office:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Acceptable Use Policy
- Anti-Virus Guidelines
- Audit Policy
- Dial-In Access Policy
- Information Sensitivity Policy
- Password Policy
- Risk Assessment Policy
- Router Security Policy
- Server Security Policy

One the policy statement has been written and agreed to by the office manager, it should be signed by all employees and the office manager's signature should be at the top of the list. Having a policy in place is great but the system administrator needs to have the authority to ensure that the policy is enforced. The system administrator needs to have the written permission of the office manager to assess the security of the network by use of whatever tools necessary. Without written permission, the network administrator is reduced to an intrusive snoop.

Introducing the office security policy to the staff should be done before the clients are hardened and certified. If the workstation's users don't know that they have or need to comply with an established security policy, the workstations will not remain secure.

Hardening the Clients

In our example LAN we have Windows 98 clients. The ability that a network administrator has to harden this particular operating system is fairly limited, and a recommendation should be made to upgrade the existing clients to Windows 2000/XP Professional. This sometimes is not possible due to the monetary constraints of the office manager. Perhaps upgrading a select number of machines per month can make that burden easier to carry. Whether the clients get upgraded or not they need to be modified significantly from the initial load of the OS.

Of course, the first step is a good virus scanner. In our case we have a virus scanner installed on all the workstations, but the virus definitions have not been updated for who knows how long. It is important that new virus definitions be downloaded and installed and all client hard disks be scanned before connecting to the new server. Remember, we are still in the process of certifying the clients and connecting to a certified server without certifying the client first defeats the whole purpose of certification. After the virus scanners are updated/upgraded, we run a full system scan on all files of the hard drive fixing errors as they occur. Also, the active system scan should be enabled, and the virus definition update should be set to download and install with no user intervention. This setting allows the virus definitions to remain updated without giving the user the ability to hit 'cancel' or 'remind me again in 1 day(s)'.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Next, we run Windows Update loading and installing all security patches and hotfixes. This is extremely easy to do, but requires (usually) several reboots of the machine. At this point all the files should be of the latest release and should be virus free. Some network and registry settings are now required.

For the most secure Windows 98 system 'File and Print Sharing' should be disabled. This being a small office it is possible that one or more of the clients is sharing its printer or some files. This should be strongly discouraged and all files shared by a client should be migrated to the server. Printers can be served directly from a print server connected to the network at a reasonable cost.

One of the biggest security problems with Windows 9x/ME is that when a user logs into the LAN with an incorrect password they just get a message telling them that they might not be able to gain access to some network resources. The user in question still has access to that computer's hard drive and the user may even have internet access. Modifying the registry can restrict this problem. The key is: HKEY_LOCAL_MACHINE\Network\Logon "MustBeValidated dword" = "01". With this enabled if a wrong username or password is given the user will be returned to the logon screen.

Other recommendations are to invoke a warning message that must be confirmed before the logon screen appears by adding two keys to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Winlogon which are "LegalNoticeCaption"="Warning Message" and "LegalNoticeText"="Some text which is in accordance with the new security policy". While this change does not limit physical access to the client it does spell out the conditions of legal use of the system.

Although Windows 98/ME can be made somewhat more secure, the best option is still to upgrade to Windows XP Professional. Windows XP had been predicted to be the least secure version of Windows yet. These predictions turned out (so far) to be greatly exaggerated. Windows XP has a multitude of security enhancements when compared to Windows 98/ME. The seemingly significant threat of Microsoft opening raw sockets turns out to be less of a threat if the user is not given administrative rights to their computer in the XP Professional environment. That, coupled with the embedded firewall called Internet Connection Firewall (when set properly) makes XP an excellent choice for the workstation.

No operating system however is completely secure out of the box, and Windows XP is no different. There are some steps that should be taken to further harden Windows XP.

- Users of the computer should only have user accounts on the local computer. Windows XP differs from Windows 9x/ME in that users can have different levels of authority. This makes it easier for the administrator to limit the authority of a user. The local user permissions can differ from the permissions that the same

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

user has on the network. However, by default the system is built with an administrator account. This is a local account and this account has the permission to do pretty much everything. This leads to the second item.

- Secure the Administrator account with a good password. The administrator has authority to do pretty much anything to the system, so it stands to reason that we wouldn't want a user to have access to that account because of a trivial password on that account.
- Disable the Guest Account. This prohibits users from logging on to the system from across the network.
- Disable any unnecessary services.
- Patch, patch, patch. Microsoft has a web-based tool called Personal Security Advisor, which scans a computer and recommends patches to enhance the security of that particular system. This service is designed mostly for workstations, and is a very good tool. This used in association with the Microsoft Update Center on a regular basis can keep your system in tiptop shape. Microsoft also issues security notices through its Security Notification Service. These bulletins are issued whenever a security issue arises and recommends the hot-fix to be applied.
- Set up account lockout policy. Account lockout is a feature in which the administrator determines how many failed attempts before the account locks that user out. The administrator can set this policy to be locked forever (until administrator unlocks) or for a certain amount of time. This is a useful tool to protect an account from someone attempting a brute force attack.

Now that the workstations have been verified free of viruses, and have been hardened according to the steps above and in accordance with the new security policy they can be certified. New Emergency Repair Disks and backup tapes should be created and stored in a safe location.

Loose Ends

As I'm sure you noticed there is a significant loose end dangling out there in space. When I set up my initial network I said that PCAnywhere was running on the server. That little detail to this point has not been re-addressed until now.

Since we have rebuilt the server, we have a spare machine. It is this machine that will be used as the PCAnywhere computer. It does not need a monitor, as it will be for remote access only. In accordance with our new security policy any authorized contractor can, with proper authorization, dial in to this computer to access network applications. Also in accordance with security policy the password for that user will be changed after every remote logon to PCAnywhere requiring the remote user to re-request a new password. Of course the latest version of PCAnywhere was used and all patches installed.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Conclusions

Obviously in the example network chosen much more money could have been spent to harden the entire network. This network was not rebuilt from the ground up (although the server certainly was) as it could have been. The small to very small businessperson, by necessity, must weigh very carefully the cost putting his computers on the web versus the benefits. Of course every business has to do this but the business that I have detailed here requires a more significant percentage of his profits to complete the task with the care that is needed. So, although I haven't recommended some of the higher cost operating system and hardware, I have put forward a very secure and operationally viable networking environment that will be maintainable into the future.

Also, the network used in the example could be any number of different configurations. The size and environment of the initial network is of less importance than the finished network environment. The tools used to harden the existing network, and the methods used to enable the office manager and network administrator to enforce good security policy make the difference in the finished environment.

References

Vulnerability Assessment Scanners
www.networkcomputing.com/1201/1201f1b1.html

Security: The Never Ending Story
www.zdnet.com/devhead/series/articles/0,4413,2631000,00.html

Linux Security How-To
www.linuxdoc.org/HOWTO/Security-HOWTO.html

For Securing Your Linux System
www.its.uiowa.edu/cio/itsecurity/bestprac/linux.htm

The Biggest Threat to Your Network Security (It Isn't What You Think)
www.zdnet.com/anchordesk/story/story%5F1959.html

Windows XP: Is It Safe?
www.computerworld.com/cwi/story/0,,NAV47_STO64909,00.html

The SANS Security Policy Project
www.sans.org/newlook/resources/policies/policies.htm

Microsoft Windows 98 Resource Kit
Microsoft Press

© SANS Institute 2000 - 2002, Author retains full rights.

Windows NT/2000/XP Hardening
ist.uwaterloo.ca/security/howto/2002-03-15/

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.