Global Information Assurance Certification Paper

SANS SECURITY ESSENTIALS PRACTICAL ASSIGNMENT
VERSION 1.4

OPTION 2 – CASE STUDY IN INFORMATION SECURITY

BY DYANN RENE BRADBURY

FIRST STEPS TO SERVER SECURITY

Option 2 – Case Study in Information Security was chosen because the assignment requires one to demonstrate how you solved a real-world problem or addressed an issue relative to Information Security. This document describes the first steps I took to ensure security on all corporate servers.

You have just been given the task of ensuring all corporate servers are secure. They are Windows NT4.0 and Windows 2000 Servers and are located at remote locations through out the United States. You know nothing about these servers and have been told there are more than one hundred of them. There are few policies and procedures written for corporate servers, no documentation exists on any of these servers and you do not know what service pack level the servers are at. You do not know if any updates have been applied to the servers either. Where do you start?

This document will provide the reader with the first steps that one should consider taking to ensure server security. This document will cover inventory, updates, anti-virus, documentation, consideration's for dealing with remote locations and basic server tasks.

State of Servers at Beginning of Project:
As stated above, you know nothing about these servers, no documentation exists, few policies and procedures have been written and you do not know what service pack level the servers are at or if any updates have been applied to the servers.

Steps Taken During Project:

Inventory:
The first step is to inventory all servers. You must find out the operating system version, what service packs, hot fixes and patches (for the remainder of this document, the word updates will be used in place of service packs, hot fixes and patches) have been applied. Is SQL, IIS, Exchange or Internet Explorer installed on these servers and if so, what updates have been applied to each of these services. You must also know what updates need to be applied to the operating system, SQL, IIS, Exchange and Internet Explorer.

To manually inventory the servers is time consuming. Purchase software that will do it for you. The software should also have the capability of pushing out updates to these servers as well as have reporting features. You should be able to print a report that lists all servers and what updates have been applied to these servers.

From personal experience, I have found the best way to inventory all servers is through software. There are some products on the market today that will do just that. Before testing software one must write down a list of criteria that the software should meet. First and foremost, I wanted software that would query servers without having to install an agent on each server, identify what software updates were needed, what updates had been applied, service pack level and operating system version and the capability of pushing out updates to all or just selected servers, scheduling capabilities and reporting features. Secondly, I wanted the software to list policy settings, services, hardware specs and file and share level permissions. I tested ntquery, ntver, whotfixcheck, dumpsec, Ecora and UpdateExpert.

Ntquery listed what hot fixes had been applied, service pack level, operating system version, system type, installed date, #of processors, last local logon, total memory, available memory and CPU speed. It lacked in reporting features and the ability to push out updates.

Ntver listed what hot fixes had been applied, service pack level and operating system version. It lacked in reporting features and the ability to push out updates.

Whotfixcheck listed what hotfixes needed to be applied but it also fell short in reporting features and the ability to push out updates.

Dumpsec is a good tool for listing group membership, rights on shares and files and account policies. It did not meet the other criteria.

Ecora is a wonderful product. This piece of software has inventory features that are out of this world. If you need software that will list file and share permissions, services that are running, installed applications, hardware (bios, physical and logical disk drives and network adapters), local policies, installed protocols, process that are running along with a host of other features. Ecora is the product. If Ecora would have had the capability of listing what updates had been applied and what updates need to be applied, along with the capability of pushing out these updates, Ecora would have been purchased.

(1) Update Expert by St. Bernard best fit the needs of our corporation. The most critical task at hand is to ensure that all servers are up to date with the latest updates. UpdateExpert met the first criteria. UpdateExpert searches the network and identifies all servers and workstations with Microsoft Windows

NT/2000/XP, Terminal Server, IIS, SQL Server, Exchange, Internet Explorer, Media Player, NetMeeting, Windows Media Services, Office and Outlook without having to install an agent on each server. Queries these systems to report the status of updates. Updates "Live" with the latest service packs and hotfixes so you don't have to do the research or find the downloads. Distributes and installs remotely all updates according to your requirements and validates installations. Policy management is enforced by designating "required" updates. Conformance report displays non-compliant machines. I am able to set policies, one of what updates need to be installed on NT4.0 servers and another of what needs to be installed on Windows 2000 servers. Before a new Windows 2000 server is put into production, I run the policy that I setup for Windows 2000 servers against this server and UpdateExpert applies all updates that I have defined in this policy. I have set separate policies for servers that are just domain controllers, SQL server, IIS servers or those that run a combination of services. I am able to produce reports that list what updates have been applied to each server with date and time stamp as well as conformance reports that list what servers do not meet the policies I have defined. Although UpdateExpert did not meet all criteria, it did however meet the first and most critical criteria.

After taking inventory of the servers you find that they are all at different service pack levels, some hot fixes and patches have not been applied and you have versions 7.0 and 2000 of SQL and versions 4.0 and 5.0 of IIS running on several of the servers. You also find versions 4.0 up to 6.0 of Internet Explorer installed on the servers. You do not have Exchange installed on any server.

Backups and ERD:
The next step is to ensure successful backups are being done on each server. You will then need to make an Emergency Repair Disk (ERD) for each server. These steps are necessary, as we will be applying service packs, hot fixes and patches to the servers. Recovery of a server will go more smoothly if you have an ERD and a good backup.

Documentation:
Before you go any further, start to document every thing that you do. I would suggest creating a database that contains the following information. Server name, operating system version, service pack level, IP address, physical location, time zone, remote site manager name and number, servers primary function, is it a BDC, PDC, member server, DNS, DHCP or WINS server. Date server was put into production, vendor contact and contract information for hardware and software installed on the server. BIOS version. Serial number, model number and asset tag number of hardware. Have your change log in this database as well. This database will be an excellent source of information for when you go to troubleshoot a server, a piece of hardware goes bad or if you have to go into disaster recovery mode. One can never have too much

documentation.

O.S. Service Packs – Hot Fixes and Patches:
You have finished inventorying the servers; now apply the latest service packs to the Operating System of the servers that it has not been applied to. As of September 28, 2002, the latest service pack for Windows NT 4.0 is SP6a and the latest service pack for Windows 2000 is SP3. You should ensure the following is done before applying the service packs.

> Consult Microsoft's documentation on the service pack you are installing.
>
> Note of caution. Apply the service packs first on non-production servers, preferably in a test environment.
>
> Inform the department that is responsible for monitoring network traffic of what you are doing and that they should expect to see more traffic on the wire.

Remote locations need to be handled differently. When dealing with remote locations you need to work closely with the department that oversees and monitors data flow, corporate routers and firewalls. Ask them what the best times would be to push out updates because they know the data flow. Let them know ahead of time when and where you are going to push out updates and from what source. Notify them of the size of the updates as well. Some of the remote locations operate 24x7. Every reboot of a server has to be scheduled. Notify every remote manager of the date and time frame that the remote servers will be rebooted. If that specific time frame does not work for a particular site, that remote manager notifies me and we schedule a time more suited to the site's production schedule. Schedule the reboot of non-production servers during off-hours, late night or on weekends. You also need someone at the remote location to be your eyes, ears and hands if something goes wrong during an update. If a server goes down in the building where your office is located, not a problem, you walk to the server, assess the situation and address the problem. If a server goes down at a remote site, you need someone there that you can ask questions to help troubleshoot the problem. We are fortunate to have field engineers on location or with in a 4 hour driving distance of each remote location. They can be dispatched at a moments notice if need be. I should also note that we have dedicated circuits to each remote location.

Do one server at a time at each remote location first. Time it, you will have a baseline to go by. In the future when you need to apply a service pack immediately, you will be able to tell management how long it will take to update every server on the network.
Remember to document everything you do on each and every server. Documentation is crucial. As you are applying service packs and hot fixes, you should be writing policies and procedures on updating servers. Decide on what

bulletins and newsletters you are going to subscribe to. (2)SANS and (3)Microsoft offer you opportunity to subscribe to their newsletters that will notify you of new vulnerabilities that have been discovered.

Decide what procedure you will follow when a bulletin comes out on a new vulnerability. Who will you notify? Determine how critical this vulnerability is to your environment. Now that you have inventoried all servers, you now know what vulnerabilities apply to you and which ones do not. Consider creating a vulnerability ranking system and form that fits your corporation. When Microsoft, SANS or Cert issues an advisory or vulnerability, fill out a vulnerability assessment form. Give the vulnerability an overall risk rating to your corporation, we use a rating of 1 – 5 with 5 being critical and 1 being hoax. The form should include the name of threat, type of threat, description, distribution method, systems affected, potential impact to your corporation, recommendations and technical details of the vulnerability. Vulnerability assessments with a risk rating of 1, 2 or 3 should be sent to management. Vulnerability assessments with a risk rating of 4 and 5 should be sent to senior management as well as the CEO and CIO. A monthly report of all vulnerability assessments that were dealt with the previous month should be sent to management.

All operating systems now have the latest service packs installed. Apply the necessary hot fixes and patches to the Operating System. Consult Microsoft's documentation first before applying the patches and hot fixes.

Internet Explorer Upgrade and Service Pack:
Your operating systems are now patched. Next, upgrade Internet Explorer to version 6 and then apply Internet Explorer service pack 1. The reason I decided to upgrade to Internet Explorer 6 and not just apply patches to the earlier versions of Internet Explorer was because I believe that Microsoft will eventually stop supporting the earlier versions of Internet Explorer with more upgrades and service packs. I would upgrade now while I was updating every server, that way I would not have to come back to the servers and upgrade to Internet Explorer to 6.0 at a later date. This would also eliminate having to keep track of updates for the earlier versions of Internet Explorer as well as version 6.0, now I only have to keep track of updates for Internet Explorer 6.0.

IIS Patches:
Now apply the necessary IIS patches to the servers that are running IIS. Consult Microsoft's documentation first before applying the IIS patches.

SQL Service Packs and Patches:
Before applying the appropriate service packs to SQL 7 and SQL 2000, ensure that all of your databases are being backed up. Consult Microsoft's documentation first. Apply the service packs and then apply the appropriate patches that were released after the service packs to your SQL servers.

I choose not to upgrade IIS or SQL at this time because extensive testing must be done on our applications that interface with IIS and SQL. I do not know what impact the upgrades would have on these applications. The upgrade of IIS and SQL will be another project in itself.

Now that all servers are up to date with the latest service packs, patches and hot fixes make an ERD for each server.

Anti-Virus:
Before checking the status of the anti-virus software on each server, review the anti-virus policies and procedures for the servers to ensure they include the following.

What version of anti-virus software should be running on the servers.

What time should you schedule the anti-virus software to check for the latest pattern file.

What time should you schedule the anti-virus software to scan all partitions.

Should real time scanning be set to scan incoming and outgoing files.

What procedures will be followed when a virus is detected.

Whether you are able to scan all partitions daily or enable real time scanning will depend on your environment. You may have terra bytes of data that would make it impossible to scan all partitions daily and depending on the server function, you may only set it to scan only incoming files or scan only out going files or scan only certain files. It will also depend on what Anti-Virus Software you are running as to what settings you can enable. It is crucial that you know the function of each and every server you are responsible for. The function will determine what you should or should not enable. You have to assess your environment and write policies and procedures to fit it. Every business is different. I have found that (4)Norton Anti-virus by Symantec best fit the needs of our corporation. Make sure Anti-Virus Software is installed and configured to your corporation's policies and procedures.

Services:
Review the services that are running on each server. Disable all unnecessary services. Again, know the function of the server, what it is running, is it a PDC, BDC or a Member Server. Know your servers. Document what you do on each server. If you have issues, you will know what services you have disabled and you will have a reference.

Basic Server Tasks:
(5)NetIQ's Security Analyzer Tool was ran against a test server and produced the following recommendations to further secure this test server.

The standard Windows NT installation with NT File system (NTFS) provides a reasonable degree of access control security. For a higher level of security, system file permission settings should be strengthened on the following:

\WINNT\Repair

The Repair directory contains a backup of the SAM database. This file is very sensitive and contains password information. Strengthen permissions on the Repair subdirectory by allowing only the Administrators group to have access. Set the Administrators group to Full control. No other users or groups should have access.

Strengthen Permissions on the Run Key and the RunOnceEx Key. The Run key and the RunOnceEx key defines programs to be run at startup. If the permissions are incorrect, any user can configure a program to run. The program could be a Trojan horse or exploit.

Set the Run Key to Read access for the Everyone group
Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows\CurrentVersion\
Name: Run

Set the RunOnceEx Key to Read access for the Everyone group
Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows\CurrentVersion\
Name: RunOnceEx

Disable Guest access to the NT Application Log, NT Security Log and the NT System Log. The following key's may not exist by default, and may need to be created.

For the Application Log:

Hive: HKEY_LOCAL_MACHINE
Kay: System\CurrentControlSet\Services\EventLog\Application
Name: RestrictGuestAccess
Type: REG_DWORD
Value: 1

For the Security Log:

Hive: HKEY_LOCAL_MACHINE

Kay: System\CurrentControlSet\Services\EventLog\Security
Name: RestrictGuestAccess
Type: REG_DWORD
Value: 1

For the System Log:

Hive: HKEY_LOCAL_MACHINE
Kay: System\CurrentControlSet\Services\EventLog\System
Name: RestrictGuestAccess
Type: REG_DWORD
Value: 1

Review the following keys to ensure there are no unauthorized programs being run at startup.

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows\CurrentVersion\Run

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows\CurrentVersion\RunOnceEx

Disable OS/2 subsystem if unneeded, delete the following registry key value and delete the \WINNT\SYSTEM32\OS/2 subdirectory.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Control\Session Manager\SubSystems
Name: Os2

Disable POSIX subsystem if unneeded, delete the following registry key value.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Control\Session Manager\SubSystems
Name: POSIX

Disable and rename the Guest Account. The Guest account should be renamed to a more obscure name to make it more difficult to execute a brute force attempt at password guessing.

Some registry key's can be used maliciously against users of a system. By default, protections are set on the various components of the registry that allow work to be done while providing standard-level security. In addition to the considerations for standard security, the administrator of a high-security installation might want to set protections on the following keys in the registry. Strengthen the Registry Permission on the following keys. You can set registry permissions through REGEDT32. Set the permissions on the following keys to:

Administrators – Full Access
System – Full Access
Everyone – Read Access

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows\CurrentVersion\App Paths

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\Compatability

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows\CurrentVersion\Controls Folder

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\Drivers

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\Drivers32

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\Embedding

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows\CurrentVersion\Explorer

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows\CurrentVersion\Extensions

Hive: HKEY_CLASSES_ROOT

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows\CurrentVersion\Internet Settings

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Control\LSA

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\MCI

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows\CurrentVersion\ModuleUsage

Hive: HKEY_LOCAL_MACHINE
Key: Software\ODBC

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\Ports

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\ProfileList

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows\CurrentVersion\Setup

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows\CurrentVersion\SharedDlls

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows\CurrentVersion\Shell Extensions

The following registry key can be used to change the startup directory. This could allow an attacker to determine what files are launched at login. Set permissions to:

Administrators – Full Access
System – Full Access
Everyone – Read Access

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

The following registry key can be misused to change several important system settings, including the NullSession shares List and the option to hide the computer from the network Neighborhood browser. Set permissions to:

Administrators – Full Access
System – Full Access
Everyone – Read Access

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\LanmanServer\Parameters

By default Windows NT places the name of the last user to log on to the system in the user name field. This can give an intruder a possible account to exploit. Suppress display of last user name in login dialog. The following key may not exist by default and may need to be created.

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\Winlogon

Name: DontDisplayLastUserName
Type: REG_SZ
Value: 1

Clear Pagefile at shutdown. The pagefile is used for virtual memory management. It contains temporary memory and may include sensitive data such as user names or passwords. On Windows NT 4.0 servers, set the following registry key value.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Control\Session Manager\Memory Management
Name: ClearPageFileAtShutdown
Type: REG_DWORD
Value: 1

On Windows 2000 Servers:

Start the Administrative Tools application in Control Panel
Open Local Security Policy
Expand Local Policies and select Security Options
Double-click Clear virtual memory pagefile when system shuts down
Click Enabled

Display Legal Notice Banner. Windows NT can display a logon banner before user logon with a caption and any text you choose. This banner can be used to display legal notices about authorized use or information regarding site policy. The absence of such a notice could be interpreted as an invitation to enter and browse the system. Consult your corporation's legal department for correct legal wording before implementing.

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Type: REG_SZ
Name: LegalNoticeCaption
Value: set this value to what you would like the caption of the legal notice to say (remember to consult legal department first)
And
Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Type: REG_SZ
Name: LegalNoticeText
Value: set this value to what you would like the text of the legal notice to say (remember to consult legal department first)

Those were just a few of the registry changes that can be made to secure a server. There are many, many more, I felt that these were some of the more

critical ones that should be covered in this document.

The following is a list of items that should be addressed as well as questions you should consider while reviewing each item.

Enable Auditing on each server, decide what you are going to audit, are you going to audit successes or failures or both? Who will be responsible for monitoring these logs? Will you store archives of these logs in a central location?

Enable Screen Saver Passwords on all servers, train the server administrators to lock the server console when they are done with their task on that server.
Review Account Policies, Rename Administrator Account, Disable Guest Account. Review who is in the Domains Administrators Group, who has rights to backup files and who has rights to add workstation to the Domain. Only a select few should be members of these groups. Review the Advanced Rights; find out who and what group has advanced rights and who is a member of these groups.
Remove unnecessary Dormant Users and unnecessary Inactive Users.
Review your corporations Password Policy, is it strong enough, are passwords being changed often enough? Review Physical Security of the Servers, are the servers in a locked room? Who has access to these rooms? Review rights on shares and NTFS permissions. If exceptions are made, document it and have managers involved sign document. For example, say an employee in the Telecommunications department needs access to a file on the accounting server. Have the managers in the accounting department and the telecommunications department sign a document stating that employee X needs access to file Y on the accounting server.
Have an incident-handling plan listing the procedures you would follow if one of the servers were attacked by an inside or outside source. Who will you notify first, at what point do you notify law enforcement and your legal department? Are you prepared to take that server off line and put another in its place?
Review Backup and Restore Policies and Procedures. Will you do a full, incremental or differential backup, will your tapes be sent off site to a secure location, will you set up a scheduled time to do a test restore of random files to ensure backups are truly successful?
Review the trusts setup between the other corporate domains. Are the trusts necessary? Who are the Domain Administrators? Could these servers be put into one domain? There may have been a business reason as to why there is more than one domain and why there are trusts between these domains. What ever the reason, document it, is it a one way trust or a two-way trust? Who is the trusting domain and who is the trusted domain. Review who has access to what resources in each domain.
Have a Disaster Plan. This in itself is a project and a half. Are you truly prepared to setup shop at another location if your current location was completely destroyed? Documentation is critical. You must know the function

of each server and have it documented, you will then be able to begin the process of rebuilding and restoring. There are so many things to take into consideration when writing a Disaster plan. You must consider everything, from where will a disaster recovery site(s) be located, adequate power source at that site, where will I get hardware from, is the site cabled properly, is it physically secure, is there software stored off site that you can rebuild a server with?

State of Server at End of Project:
Quite the task list you have completed. Are the servers secure? No, nothing is secure. Are they in better shape than what they were? Absolutely!
Server security is continual and never ending. New vulnerabilities are discovered all of the time. Let's review the items we have accomplished. You now have software that enables you to push out service packs, patches and hot fixes to the servers. All servers are up to date with the latest updates. You are able to produce reports to management on what has been applied to the servers. The current version of Anti-virus software is on all servers with the latest pattern file. All servers are being backed up successfully. Documentation was being done as every change was being made to each and every server. Policies and Procedures have been reviewed and new ones wrote. You have reviewed physical security, user accounts, share;s and have an incident handling plan along with a host of other tasks you have completed. You now have a solid foundation on which to further secure the servers.

Simply applying service packs, hot fixes and patches to the servers does not totally secure them. You must further lock down the (6)Operating System, IIS, SQL and Internet Explorer. Procedures for locking these down exceeds the scope of this document. I would also strongly encourage the reader to implement Host Based and Network Based Intrusion Detection Systems. I would also encourage the reader to scan the servers for vulnerabilities.

My goal was to leave the reader with a structured check off list of tasks that I have come up with and some tools that I use in my work environment. This document is intended to be the first steps taken. There is more work to be done to further secure the servers, but the reader should know that it can be done! Be organized, thorough, pay close attention to detail and you will be fine!

References:

1. St. Bernard – UpdateExpert: Click on this link for a full description of what UpdateExpert is capable of doing.

http://www.stbernard.com/products/updateexpert/products_updateexpert.asp

2. SANS: Click on this link to subscribe to SANS Newsletter Subscription Service.

http://server2.sans.org/sansnews

3. Microsoft: Click on this link for Product Security Notification.

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp

4. Symantec – Norton Anti-Virus Corporate Edition: Click on this link for a description of Norton Anti-Virus Corporate Edition.

http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=155

5. NetIQ Security Analyzer: Click on this link for a description of NetIQ's Security Analyzer.

http://www.netiq.com/solutions/security/default.asp

6. Microsoft Security Checklists for Windows 2000 Server Baseline Security, Windows NT 4.0 Server Baseline Security, IIS 4 and IIS 5 Baseline Security

http://microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/

7. National Security Agency: NSA Windows 2000 and Windows NT Guides.

http://nsa1.www.conxion.com/index.html

Security Tools

Hfnetcheck

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/hfnetchk.asp

Dumpsec

http://www.somarsoft.com/