Three Defenses to a Secure System: Virus Scanning, Applying Patches and System Monitoring

Angelina Lucero

Three Defenses to a Secure System
Virus Scanning, Appling Patches and System Monitoring

Angelina Lucero
SANS Security Essentials GSEC Practical Assignment
Test Ver. 1.2e

After attending the Security essentials class I was overwhelmed. Before the class as a system administrator I had a few leads on security. After the three days of information building I was inundated with many new security ideas and tried to gather a security plan of attack from the manuals and notes gathered from SANSFIRE. A common theme came up over and over again, it was to build layers of defense called "Defense in Depth." In starting to build a strong security plan of action keep in mind that as you build security the "defense in depth" model requires you to put layer upon layer of security to be in place. Begin security with the basics much as you would any project. So even tasks that may seem too basic and maybe even mundane can become very important for placing layers of security in place. Virus scanning is very important because the ultimate goal is to detect malicious code before it attacks computer systems within your organization. Use automated tools to keep up with the numerous patches are needed for Windows operating systems. Become familiar with your operating system and know what applications and processes are currently running on your computer servers and workstations.

The purpose of this paper is to share with other system administrators the "how to" on tools that can be used for basic security configuration. Most of the documentation on securing windows systems that I initially found was very general in terms. For example, apply patches to the operating system. That is a great idea but how to get started and use available tools to streamline the process is just as important. After some research I have found that Microsoft has specific tools to determine what patches you need and how to apply them a bit more streamlined and automatic using tools to begin the layers of security in a Windows environment. This document describes issues to consider when setting up virus scanning software, using Microsoft tools to make patching operating systems easier, and a few specific tools that you can use to benchmark or monitor your operating system that might help you spot those abnormalities that should not be there.

VIRUS SCANNING

It is important to use virus detection programs. Keep virus detection running on all computer systems in the office, in all computer systems that remotely access the office computer systems and on all the computer systems for the home computer systems of your office staff. It important to have all these computer systems covered and current software and virus definition files installed. Several software products can help automate this process. Check to see if the following can be applied to the product currently used.

Make sure each computer on your network has some form of virus scanning software installed. It almost goes without saying, but double check the following:

- Is the most current software version installed
- Is the software loaded for a system scan every time the computer system boots up or has the user disabled it

- If the user can disable system scan virus detection, try to lock the software with a password so that they can not disable it
- Does the software scan all appropriate files, determine what files other that executables or macros that can be scanned.
- How often are updates being made to the virus definitions file from the vendor, setup on a daily or weekly schedule if possible
- Can updates be made automatically if connected to the network if so have you scheduled these updates
- Regularly distribute non-automated updates for computers not connected to the LAN
- Setup automatic notification of any problems and just in case this fails be sure to check the log files periodically

One of the best allies a system administrator can gain in the fight against malicious code is the support of the computer users. They have the potential to help be the best defense against malicious code entering computers.

- Include office staff in discussions about virus protection of their home computers; remember they can introduce malicious code by brining in an infected application on a CDR, zip disk, or floppy disk from home
- Help staff learn how to use the virus detection software you use and purchase corporate licenses that allow staff to install a copy of the virus protection software on their home computer
- When staff comes to you with a "potential virus" listen to what they have to say. Even if you know this isn't a virus attack they can initiate dialogs about security issues and learn from system administrators. Assure them that you want to hear about any irregularities.
- Schedule routine scans of the local drives when the user is not in "high use" mode of the workstation. This way they feel more involved in the process and hopefully will be more inclined to work with you towards a secure environment.

Even after scanning all the files on a local system on a regular schedule it is important to setup the virus protection software to scan files as they are executed or opened. This adds one more layer of protection to scanning files for malicious code. You can think of it as a micro "defense in depth" model.

- Is system scan enabled for inbound and outbound files of all workstations and servers
- Are compressed files scanned
- Can system scan be disabled
- Setup the virus detection software to clean the infected file and alert the system administrator
- Be sure to check the log file for two reasons, one to check for any alerts that did not get forwarded, secondly to determine what "normal" logging looks like this makes it easier to pick out abnormalities later
- Be very sure to only exclude files and/or directories that are absolutely necessary

OPERATING SYSTEM PATCHES (Microsoft)

An important thing you can do to protect your systems is keep the operating system patches up to date. For instance there was vulnerability in Windows IIS that had been detected by a security

company named eEye Digital Security in May 2001 and they reported it to Microsoft (eEye). Microsoft published a fix on their web site on June 18, 2001. The New York Times reported that on July 19, 2001 an estimated 350,000 computers were infected by the Code Red Worm that took advantage of the vulnerability that eEye had reported in May (Schwartz). By the last of July and the first of August, 2001 the media was reporting on the worm regularly. System administrators were becoming more aware of the patch from Microsoft and installing it. When the mainstream media started reporting the problem to the public, about the first week in August, there had been a fix available for over one month that had not been widely applied. Perhaps if more system administrators had been aware of the patch and applied it early, the problems from the worm would have not been as far reaching. New tools available from Microsoft can be used to help automate the patching process.

Several sources identify installing patches as part of securing a windows environment. The Carnegie Mellon CERT center indicates that "A minimum installation for NT servers includes NT 4.0, the latest Service Packs, recommended patches and relevant security Hotfixes released by Microsoft."(CERT) One issue is to identify what patches need to be on what systems. Recently Microsoft has published some tools to assist the system administrator in keeping up with the patches available. The Personal Security Advisor (MPSA) tool and the Hot Fix Checker can be accessed from www.microsoft.com/technet/security/tools.asp . A tool named qchain will allow multiple hotfixes to be applied with one reboot to the system. These tools can help you keep up with keeping patches current.

As a system administrator of MS operating systems I have seen the abundant overflow of patches that MS puts out. All of this can become so overwhelming that this becomes an easy step to avoid. After all it sure seems quite a bit more intriguing to get to the more technical stuff like Intrusion Detection (ID) and Protocol analyzing! But wait just one minute the entire security essentials common theme was "defense in depth". Appling patches are one more layer that can prove to be just as important as all the fun stuff to come.

Microsoft Personal Security Advisor (MPSA) is valuable in identifying security risks on a computer by computer basis. From the computer you want to scan do the following (see figures 1,2,3):

- The web based scanner identifies weaknesses on the system you executed the scan from
- It provides a report for you indicating changes that you can make to improve security these might include patches, stronger passwords, IE security settings and macro settings Figure 3
- Presented below is the sample output from MPSA
    - Figure 1 shows a connection to MSPA tool to initiate the program click on scan now (Figure 1) URL: http://www.microsoft.com/technet/mpsa/start.asp

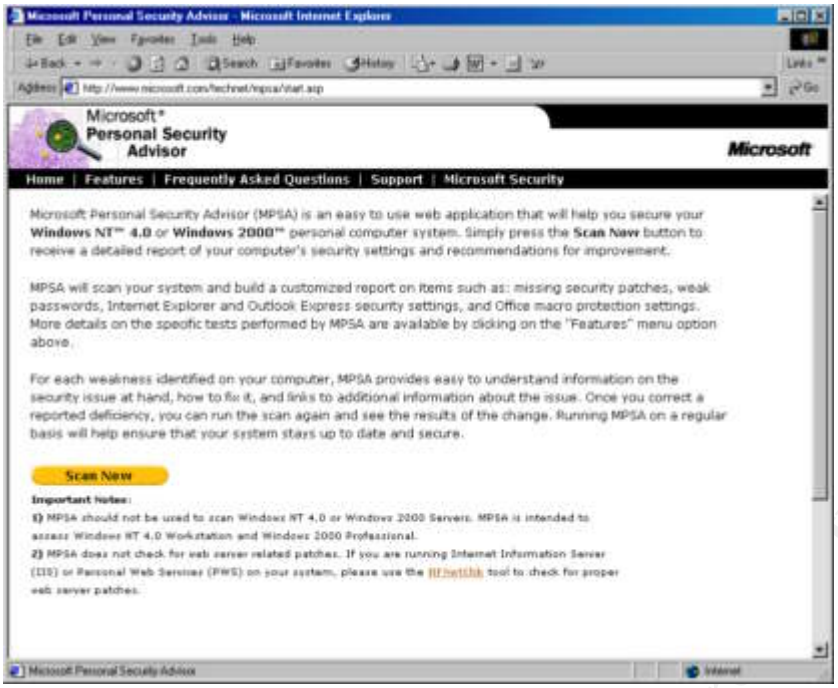

Figure 1 Initial Screen

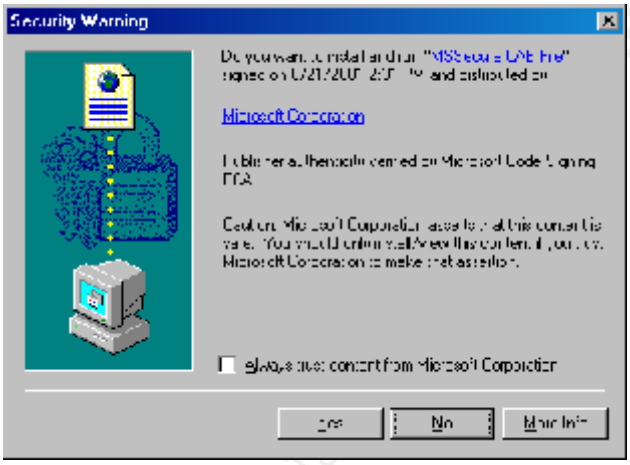

Figure 2 -Select Yes to execute

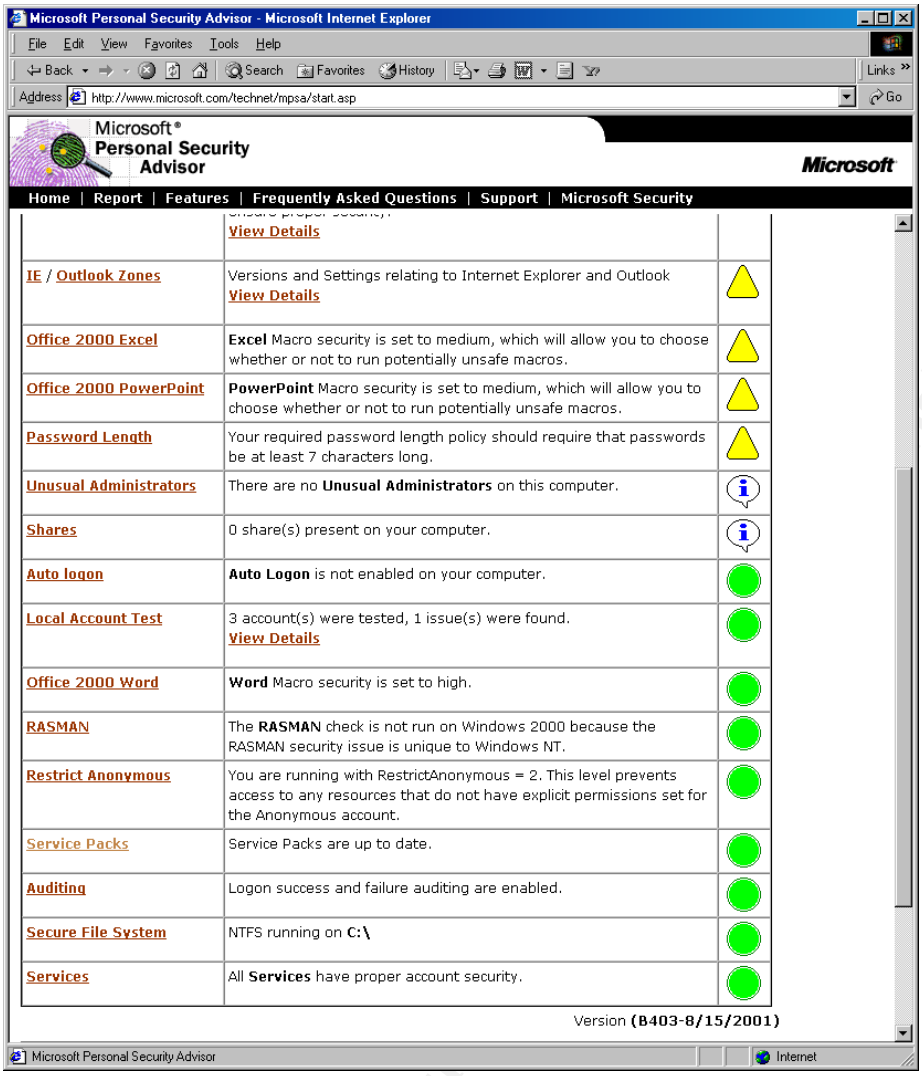

Figure 3 - Sample output after executing program

Hot Fix Checker

This program from Microsoft allows checking for patches on systems across the network. According to Jim Minatel, Editor in Chief "Exchange & Outlook" magazine, "Hfnetchk checks a list of known available security patches for the services running on the computer or computers you check and returns a list of all the missing patches, complete with Microsoft Knowledge base article numbers so it's easy for you to look up each path, read about it, and install it."(Minatel)

Features:

- checks all machines on a network from a central location
- according to HFNetChk web site

  http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/hfnetchk.asp checks multiple operating systems
  - Windows NT 4.0
  - Windows 2000
  - All system services, including Internet Information Server 4.0 and 5.0

    - SQL Server 7.0 and 2000 (including Microsoft Data Engine)
    - Internet Explorer 5.01 and later
  - You have to have administrative rights to scan remote machines
  - First release, future releases will have improved features. Be sure to check the Microsoft site for most current information on options.
  - Review knowledge base Article ID : Q305385 for FAQ's and Article ID: Q303215 for general information on Hfnetchk.exe

In order to use this tool you have to download the zipped file nshc.exe from Microsoft download center. After saving the file to disk execute it to install the program. There are several command line parameters that you can use to control what host gets scanned, displaying installed, missing, or necessary hotfixes. Output can be tab or wrap formatted. Options to perform or not to perform registry checks and options exist. See Figure 4 below for a complete list and examples using the command line options.

```
hfnetchk.exe [-h hostname] [-i ipaddress] [-d domainname] [-n] [-r range]
             [-a action] [-t threads] [-o output] [-x datasource] [-z] [-v]

Description:
       The HFNETCHK tool assesses a machine or group of machines for security
       hotfixes that have either been installed and/or need to be installed.
       For more information on this tool, please refer to Microsoft Knowledge
       Base Article Q303215.

Parameter List:
       -h      hostname       Specifies the NetBIOS machine name to scan.
                              Default is the localhost.

       -i      ipaddress      Specifies the IP address of the machine to scan.

       -r      range          Specifies the IP address range to be scanned,
                              starting with ipaddress1 and ending with
                              ipaddress2 inclusive.  <ipaddress1-ipaddress2>

       -d      domain_name    Specifies the domain_name to scan.  All
                              machines in the domain will be scanned.

       -n      network        All systems on the local network will be
                              scanned.  (i.e., all hosts in Network
                              Neighborhood)

       -a      action         Displays (i)nstalled hotfixes,
                              (m)issing hotixes, (n)ecessary hotfixes or
                              (b)oth installed and missing.  Default will
                              display necessary hotfixes.

       -t      threads        Number of threads used for executing scan.
                              Possible values are from 1 to 128. Default is 64

       -o      output         Specifies the desired output format.
                              (tab) outputs in tab delimited format.
                              (wrap) outputs in a word wrapped format.
                              Default is wrap.

       -x      datasource     Specifies the xml datasource containing the
                              hotfix information.  Location may be an xml
                              filename, compressed xml cab file, or URL.
                              Default is mssecure.cab from the Microsoft
                              website.

       -z      reg checks     Do not perform registry checks.
```

```
                              in wrap mode.

        -?      help          Displays this menu.

Examples:
        HFNETCHK.exe
        HFNETCHK.exe -h hostname
        HFNETCHK.exe -h h1,h2,h3
        HFNETCHK.exe -i 192.168.1.1 -a m -t 10 -v
        HFNETCHK.exe -i 192.168.1.1,192.168.1.8 -h hostname -x mssecure.xml
        HFNETCHK.exe -d domain_name -a b -o tab -x c:\temp\mssecure.xml
        HFNETCHK.exe -r 192.168.1.1-192.168.1.254 -a i -t 20
        HFNETCHK.exe -x http://www.xyz.abc/mssecure.xml
        HFNETCHK.exe -x "c:\Space In Path\mssecure.xml"
```

Figure 4 – options for hfnetchk.exe /?

Next you have the task to evaluate the output, download and install the recommended patches. The output lists the security bulletin number and the Article ID Q # for the patch or warning. See sample output in Figure 5 *(note the ip addresses have been changed to xxx for privacy purposes. In your output each IP address will be explicitly cited.)* Output from the hfnetchk program and be redirected to a file by inserting *>filename* at the end of the command.

Note the difference in necessary patches from a system with Windows 2000 sp1 and Windows 2000 sp2 in Figure 5. If service pack 2 is installed on system # 3 (Figure 5) several of the listed patches will be taken care of. After installing patches be sure to re-execute the hfnetchk program to assure you have installed all the necessary patches and hotfixes. To further automate this process schedule the hfnetchk program to run regularly and have the data forwarded to an administrator email account. This utility can help keep up with patches.

```
---------------------------
xxx.xxx.xxx.xx1
---------------------------
        WINDOWS 2000 SP2
                Patch NOT Found     MS00-077 Q299796
                Patch NOT Found     MS00-079 Q276471
                Patch NOT Found     MS01-007 Q285851
                Patch NOT Found     MS01-013 Q285156
                WARNING             MS01-022 Q296441
                Patch NOT Found     MS01-025 Q296185
                Patch NOT Found     MS01-031 Q299553
                Patch NOT Found     MS01-037 Q302755
                Patch NOT Found     MS01-041 Q298012
                Patch NOT Found     MS01-046 Q252795
        Internet Explorer 5.01 SP2
                Patch NOT Found     MS01-027 Q295106
---------------------------
xxx.xxx.xxx.xx2
---------------------------
        WINDOWS NT4 SP6a
                WARNING             MS99-036 Q155197
                WARNING             MS99-041 Q242294
                Patch NOT Found     MS00-081 Q277014
                WARNING             MS01-022 Q296441
                Patch NOT Found     MS01-041 Q299444
        Internet Explorer 5.5 SP1
                Patch NOT Found     MS00-093 Q279328
                Patch NOT Found     MS01-012 Q283908
                Patch NOT Found     MS01-027 Q299618
---------------------------
xxx.xxx.xxx.xx3
---------------------------
        WINDOWS 2000 SP1
                Patch NOT Found     MS00-036 Q262694
                Patch NOT Found     MS00-047 Q269239
                Patch NOT Found     MS00-052 Q269049
                Patch NOT Found     MS00-053 Q269523
                Patch NOT Found     MS00-065 Q272736
                Patch NOT Found     MS00-066 Q272303
                Patch NOT Found     MS00-067 Q272743
                Patch NOT Found     MS00-069 Q270676
                Patch NOT Found     MS00-070 Q266433
                Patch NOT Found     MS00-077 Q299796
                Patch NOT Found     MS00-079 Q276471
                Patch NOT Found     MS00-085 Q278511
                Patch NOT Found     MS00-089 Q274372
                Patch NOT Found     MS00-096 Q266794
                Patch NOT Found     MS01-001 Q282132
                Patch NOT Found     MS01-005 Q281767
                Patch NOT Found     MS01-007 Q285851
                Patch NOT Found     MS01-013 Q285156
                WARNING             MS01-022 Q296441
                Patch NOT Found     MS01-025 Q296185
                Patch NOT Found     MS01-031 Q299553
                Patch NOT Found     MS01-037 Q302755
                Patch NOT Found     MS01-041 Q298012
                Patch NOT Found     MS01-046 Q252795
        Internet Explorer 5.01 Gold
                Patch NOT Found     MS00-009 Q251109
                Patch NOT Found     MS00-042 Q265258
                WARNING             MS00-043 Q261255
                Patch NOT Found     MS00-055 Q269368
                Patch NOT Found     MS00-037 Q259166
```

Figure 5 – sample output of hfnetchk program

Qchain.exe - Install multiple hotfixes with 1 reboot.

Now that you have a listing of patches and hotfixes to install Microsoft provides another tool to streamline the process of installing all the patches. The Microsoft Knowledgebase Article ID # Q296861 identifies the benefits as:

- "It increases uptime for servers because computers are not being rebooted between each hotfix installation
- It Allows faster installations of multiple hotfixes on a single computer.
- It is a solution that works on both Windows 2000 and Windows NT 4.0." (Q296861)

The MS knowledge base article previously cited has a link to download the qchain program. To view Microsoft knowledge base articles go to http://support.microsoft.com/ . It is important to use the qchain program to install multiple hotfixes if you don't plan to reboot after every update because potentially files will be overwritten by each hotfix causing damage to the hotfix or the operating system. When more that one hotfix is installed before reboot the entire patch may not be applied as you expected it to. To install multiple fixes at one time execute each hotfix with a –m option at the end of the command line. After all hotfixes have been installed run qchain.exe. This command line utility can also be run in a batch file to further automate the process.

KNOW THY SYSTEM

Know your operating system and what it usually does and does not do. How will you know if something looks different on your system? How can you monitor the changes made if you don't know what normal looks like? The Windows Resource Kit has some tools to help with research and monitoring of the operating system. They can help you track what your system normally looks like and then you can compare differences to help you determine if there is a problem.

Netwatch – If you use Windows operating systems there is a tool in the resource kit that allows monitoring of the shares of the server and all the PC's on the LAN that use NTFS. Options allow you to monitor several PC's at one time or only view shares with open connections.

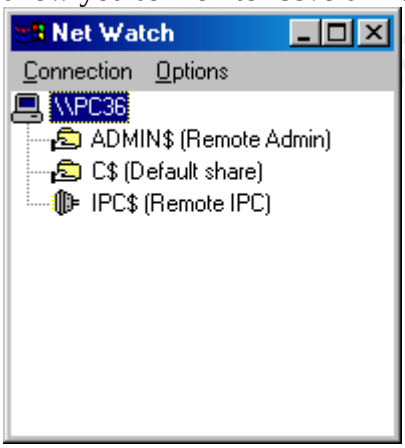

Figure 6 – View of Shares using NetWatch

Figure 6 shows the shares available on pc36. The shares listed are created with a standard install of MS Windows 2000 Professional. If another computer system connects to PC36 the NetWatch display indicates the user account name and the files that are open from the remote system as shown in Figure 7. The user "administrator" from PC6 has connected to PC36 and has the file

1ELS0006.TMP open on the C$ share of PC36. In this example a drive was mapped to PC36 from PC6 and the file was open using notepad. Notice the user administrator and the location PC6 are identified.

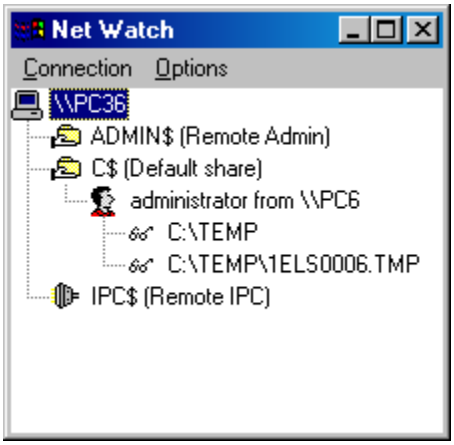

Figure 7 – NetWatch View of open files from remote PC

Some connections to the system shares such as IPC$ do not have usernames listed. Figure 8 shows an example of a connection to PC 36 using a Null session command listed on page 1-10 of Security Essentials, Part 1 book (SANS).

- The command issued from PC 6 was C:\>**net use *xxx.xxx.xxx.xxx*\IPC$ "" /USER:""**

Where *xxx* is the address of PC36. In this example a Null session has been used which can enumerate information using dumpsec. To stop listing of domain usernames and share names set the RestrictAnonymous key in the registry. For more information on how to setup this key refer to "Windows NT Configuration Guidelines" from CERT Coordination Center (CERT). Currently the link is : http://www.cert.org/tech_tips/win_configuration_guidelines.html. In this document you will also find several other registry settings to improve security.

Figure 8 – NetWatch View of remote access using "net use" command

With the NetWatch tool you can monitor the use of the "net use" and other commands used to remotely connect to computer shares. Shares listed include administrative shares and shares that have been created on the pc. On the example provided here only system shares were present. To identify how each connection looks on NetWatch make different connections and view the results. Being familiar with the different connections will help to track abnormalities.

System Logs – The system log files can be a very critical part of getting to know how your system operates. You can use this as baseline of operation to compare regular activity with abnormal activity. Several items are recorded to the Application and System logs but you have to setup the system to record events into the Security log. To view the logs in Windows 2000 right click on My Computer, select Manage. The Computer Management Window (figure 9) lists the event viewer option.

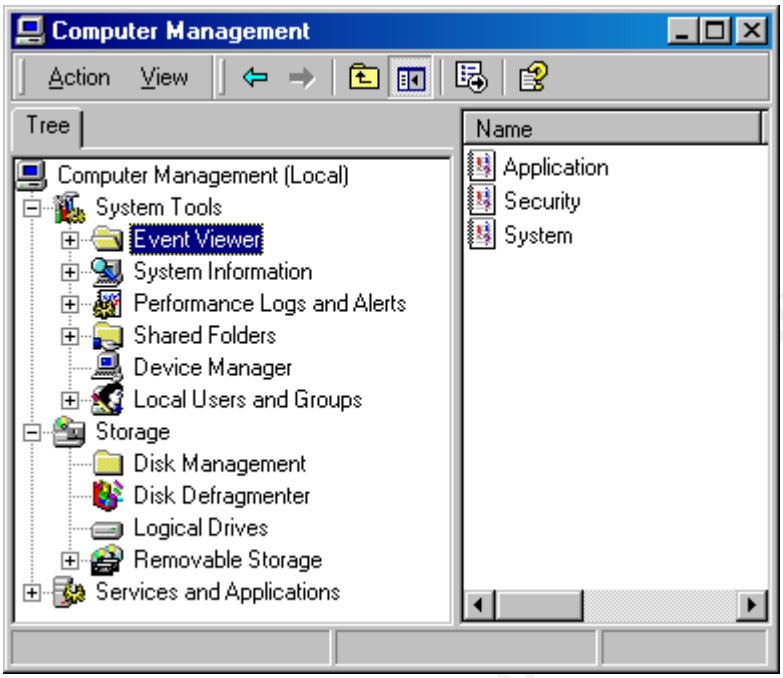

Figure 9

The next step is to select event viewer and click on one of the logs on the right pane. There are numerous items in Windows 2000 that can be logged. In fact there are so many that this entire paper could be consumed by Windows event log configuration. Rather the intent of this portion is to help point out other resources for setting up logs and a general description of log usefulness. Each log contains different information. A document titled "Windows NT Event Log explained" from Beyond-Security's SecuriTeam.com site gives the following definitions (NtWak0):

> "System log
> Tracks miscellaneous system event, e.g. track events during system startup and hardware and controller failures.
>
> Application log
> Tracks application related events, e.g. applications generate informational (sic) such as failing to load a DLL with appear in the log.
>
> Security log
> Tracks events such as logon, logoff, changes to access rights, and system startup and shutdown. NOTE: By default the security log is turned off."(SecuriTeam)

The document at SecuriTeam also identifies the location of log files at

%SYTEMROOT%\system32\config\
system file = sysevent.evt
security event file = secevent.evt
application log = appevent.evt

Some of the most important items to track are logon events contained in the security log. To enable the security log on Windows 2000 follow these steps (MS 2000 Resource Kit):

Start → Settings → Control Panel → Administrative Tools → Local Security Policy → Local Policies → Audit Policy

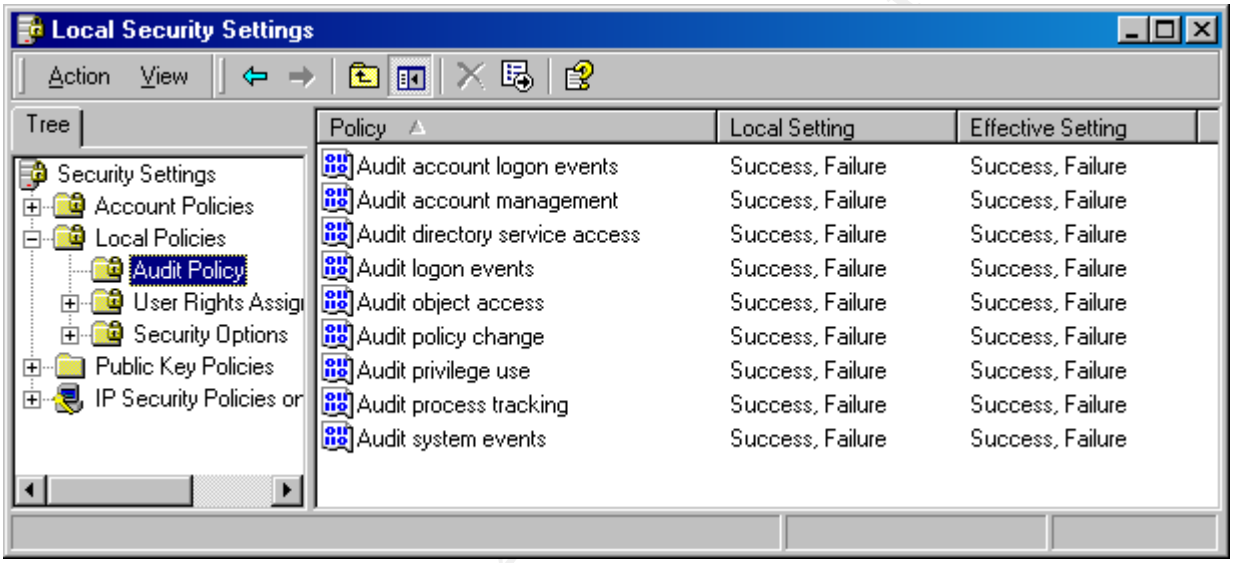

Figure 10

The window shown in figure 10 lists the types of security events that can be audited including logon and logoff. Auditing can also be configured to monitor files and folders. It is important to configure your system according to your specific need. The following table details important information about each of the settings listed in the audit polity and what type of threat can be detected by logging each event.
Figure 10 it was retrieved from Microsoft at (MS Planning):

http://www.microsoft.com/WINDOWS2000/techinfo/reskit/en/Deploy/dgbe_sec_cspz.htm

Audit Event	Threat Detected
Failure audit for logon/logoff.	Random password hack
Success audit for logon/logoff.	Stolen password break-in
Success audit for user rights, user and group management, security change policies, restart, shutdown, and system events.	Misuse of privileges
Success and failure audit for file-access and object-access events. File Manager success and failure audit of read/write access by suspect users or groups for the sensitive files	Improper access to sensitive files

Success and failure audit for file-access printers and object-access events. Print Manager success and failure audit of print access by suspect users or groups for the printers.	Improper access to printers
Success and failure write access auditing for program files (.exe and .dll extensions). Success and failure auditing for process tracking. Run suspect programs; examine security log for unexpected attempts to modify program files or create unexpected processes. Run only when actively monitoring the system log.	Virus outbreak

Another good resource to locate information on event logging is LabMice at http://www.labmice.net/troubleshooting/EventLog.htm. There is a sample output from LabMice in Figure 11 below.

Figure 11 – sample LabMice output for event logging

As you can see there are several options to consider when you start tracking events using the event logging utility provided by Microsoft. If you take the time to configure and review the log files this can be an important layer of defense for your computer system.

Providing security for your computer systems takes effort and perseverance. Managing the virus scanning, patches and monitoring your system are important to building layers of defense for computer systems. The tools listed here are available to make these processes more efficient. Taking the time to implement these and other tools can increase the defenses against unwelcome

advances towards the computer systems you operate and manage. Implement the basic strategies of good security and use the tools to help reduce the amount of time it takes to protect your system.

REFERENCE PAGE

CERT. "Windows NT Configuration Guidelines." April 17, 2000.
URL: http://www.cert.org/tech_tips/win_configuration_guilelines.html (August 28, 2001)

Eeye. Home Page: Home|About
URL: http://www.eeye.com/html/About/index.html (September 6, 2001)

LabMice. "Event Logging in Windows 2000" September 6, 2001
URL: http://www.labmice.net/troubleshooting/EventLog.htm (September 6, 2001)
Microsoft. "Security Tools."
URL: www.microsoft.com/technet/security/tools.asp (September 10, 2001)

Microsoft. "Personal Security Advisor."
URL: http://www.microsoft.com/technet/mpsa/start.asp (September 10, 2001)

Microsoft. "Hot Fix Checker."
URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/hfnetchk.asp
(September 10, 2001)

Minatel, Jim. "Patch Holes with Microsoft's New Security Tool." Exchange & Outlook Magazine: August 21, 2001.
URL: http://www.exchangeworkshop.com/features/ednotes/ed082001.asp

MS 2000 Resource Kit. Microsoft Windows 2000 Server Operations Guide. Redmond, Washington: Microsoft Press, 2000 Page 582

MS Planning. "Planning Distributed Security, Auditing" Windows 2000.
URL: http://www.microsoft.com/WINDOWS2000/techinfo/reskit/en/Deploy/dgbe_sec_cspz.htm
(September 4, 2001)

NtWak0. "Windows NT Event Log explained." December 9, 2000
URL: http://www.securiteam.com/windowsntfocus/5EP0E0K2KW.html (September 6, 2001)

Q296861. Microsoft Knowledge Base Article # Q296861. "Use Qchain.exe to Install Multiple Hotfixes with Only One Reboot." August 17, 2001
URL: http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q296861 (September 10, 2001)

SANS. Security Essentials, Part1. SANSfire Washington D.C. July 30- August 4,2001
Page 1-10.

Schwartz, John. "Return of computer 'Worm' Feared Today;TECHNOLOGY." July 31,2001.
New York Times. Section:Business/Financial Desk.