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.

Configuring a Free Automated Host Auditing System for windows 2000 Server and 2003 Server.

This project will bring together a collection of tools that monitor different aspects of a host. This host auditing system has been deployed on our more critical servers in order to reduce the time between an intrusion and its detection as well as to monitor the system state in order to more easily identify important changes to the operating system. In this way even if an attack isn't stopped, it can be detected early, perhaps even before a hacker has a chance to fully exploit their entry. The characteristics monitored...

Copyright SANS Institute

Author Retains Full Rights

AD

Table of Contents 1
RyanMortensen-GSEC.doc 2

© SANS Institute 2005, Author retains full rights.

Configuring a Free Automated Host Auditing System for windows 2000 Server and 2003 Server.

GIAC Certification (GSEC) version 1.4b Option 2

Ryan Mortensen

Date Submitted – Jan 10, 05

© SANS Institute 2005 - Author retains full rights.

Abstract:

This project will bring together a collection of tools that monitor different aspects of a host. This host auditing system has been deployed on our more critical servers in order to reduce the time between an intrusion and its detection as well as to monitor the system state in order to more easily identify important changes to the operating system. In this way even if an attack isn't stopped, it can be detected early, perhaps even before a hacker has a chance to fully exploit their entry. The characteristics monitored include unneeded services, unnecessary open ports, multiple system/security events, drivers, shared folders, programs that load during startup and network configurations .

Most software security tools (especially free ones) track a single aspect of a computer's state such as file usage, user accounts or network status. Similarly, the event log tracks changes to objects such as single user accounts, but it is does not provide any kind of overview of the system. These gaps require system administrators to employ multiple tools, each of which can generate voluminous output in order to get a good idea of what is happening on a server. This project provides one method for combing multiple tools to measure most of the important aspects of a system. Care was taken to select the most important aspects of a system from a security perspective, while not monitoring so much that the audit tool would significantly degrade performance on the system or take too long to run. For this audit system, some of the most useful free utilities are configured to run on a schedule and report back only the more critical events. This approach could be considered Anomaly Detection because it only logs changes to the system. (see A Taste of Computer Security)

Before:

I work in a large university with a very complex and open network. The network consists of around 55,000 jacks connected to a high speed backbone. Our main security department maintains a database of critical servers. These servers are regularly scanned for vulnerabilities and suspicious open ports. Even so, it can take up to a week at times for this department to spot a problem with a

connection due to the volume of jacks they are monitoring. Because my department deals with financial data, this gap is too long. My unit is responsible for around 20 servers but this chances frequently.
The department I work in deals with sensitive information, yet there is very little in the way of a firewall. The only protection we have is a very limited packet filter on the border of the university network despite the attention university networks are given by hackers. This filter blocks only a few ports associated with SQL, and Windows networking. In the past, intrusions have occurred and my department only became aware of them when network security shut off the machine's Ethernet jack. We luckily encountered no loss of sensitive data but the compromise of several less critical systems highlighted the need for more oversight.

In recent years, my department has seen a proliferation in demand for mid-level servers that are not used university wide, and therefore aren't managed by our enterprise technology group yet contain sensitive data such as invoices and credit card numbers. These systems are not mission critical to the university as a whole, and therefore receive minimal resources. Yet most servers in a university environment contain private data and there are now many regulations requiring the safeguarding of this information. With the plethora of smaller systems we have, it was difficult to provide adequate oversight of these systems. What was needed then was a system that could help keep track of a large number of smaller servers without drowning us in unnecessary information or consuming too many resources.

Security Before the Audit System:

Each of our servers runs zonealarm or Ipsec. These help, but are not enough by themselves. Intrusions can still happen and when they do, these solutions provide little or no warning and very little information about what happened after a successful intrusion. Zone alarm at least logs possible intrusion attempts and the ip address they came from. This helps administrators notice attacks and determine whether they are internal or external, but when an exploit is successful, zone-alarm generally isn't much help.

Our servers also comply with the university security standards. This includes disabling unneeded ports and services, using ntlmv2 password encryption, disabling Null sessions, regular patching and so on. Even with all of these precautions in place, we have still encountered problems. After hardening our servers, we still had to find a way to keep a close eye on them because no system connected to the internet is impregnable.

This audit system could be considered a poor-man's HIDS. For this project, I chose to focus on the host instead of the network for several reasons. The major reason is that it is far easier to implement but it also requires much less bandwidth, It is easier to implement, it is more flexible, and doesn't have a single point-of-failure. (see "Host-Based IDS vs Network-Based IDS). While many HIDS detect network traffic and compare it to signatures to detect

© SANS Institute 2005 Author retains full rights.

suspicious traffic, this system relies on watching system and network states. Besides being much easier to implement, this approach has a few other advantages. First, you don't need updated signatures for packets. Second, encrypted network traffic is not a problem because it is looking at the results of the traffic rather than the traffic itself. Third, it uses less resources. Last, this system detects internal attacks as easily as external network threats. It is estimated that "%70 of security breaches are committed from inside a networks perimeter" (The Science of Host Based Security) The major disadvantage to this conception of a HIDS is that it cannot block unwanted traffic before a compromise occurs. Because it only reports what is happening, it can be considered a passive IDS. (see Intrusion Detection Systems Part 2-Classification;Methods;Techniques) This implementation of a HIDS is probably most closely related to host-level security services like the SentryTools suite for Unix.

In the section "Automation and Auditing" in the Sans course books there is a list of the ideal information that should be collected to get a snapshot of a system. The list is extensive, and some of the items on the list, such as all folders and their sizes are not practicle in most situations. I attempted to set up an optimal system that records as much of the charactoristics listed as possible without overwhelming the system or the admin. Many of the items on the list are covered indirectly such as the groups existing on the system. Any changes to user groups is logged, therefore it doesn't seem as necessary to retrieve a full list of all groups every audit.

During:

Pre-configuration:

Scheduling

Install System Scheduler (you can use the built-in windows scheduler but I have not found it to be very reliable.) A good, free alternative I have found is called System Scheduler by Splinterware. Setup the scheduler to run at whatever interval you think is appropriate. It could run as often as every three or four minutes for critical systems. This system monitors two different types of changes, changes of state, and events. States are a snapshot of the network state or process list. These are only reported at the intervals set in the scheduler. Therefore the time the state changed can only be estimated between runs. Events are stored in the system logs along with the time they occurred and therefore can give an accurate accounting of the time at which an event occurred. This can then be correlated with other events in the log to gain a more complete picture of what happened. Therefore it is probably a good idea to determine the run schedule of this tool based on how closely the system should be monitored and the resources available to review the logs.

© SANS Institute 2005 Author retains full rights.

Enable Security auditing.
By default, windows does not log security events. In the control panel under local security policy security event logging can be configured.

For my systems, I have chosen the following configuration:

Audit account logon events	Success,Failure
Audit account management	Success, Failure
Audit logon events	Success, Failure
Audit Object Access	Success, Failure
Audit Policy Change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Success, Failure
Audit system events	Success, Failure

This configuration generates a large amount of events but so the event logs need to be cleared regularly. The volume of the logs is not a problem because this system will extract only the more important events and display them only once.

Tool described:

I developed a batch script that takes a system baseline and periodically compares a new system status with the baseline. This then logs only changes to the basic system so that you don't have to dig through tons of extraneous data in order to spot important changes. Here is a table of the type of events and system states logged and the free program used to gather this information.

Characteristic	Program
Network open ports and applications connected to these ports	Windows 2000: Foundstone fport.exe Windows2003: built-in netstat -o
Threads running	Tlist
Drivers, Network Configuration, Startup applications	MSinfo
Key Log events	DumpEL (Microsoft Resource Kit)
Shared folders	Winfo

What this audit system helps identify:

Trojans or backdoors
Viruses
Brute force logon attempts
Unauthorized changes to accounts
Unsecured shares

© SANS Institute 2005 Author retains full rights.

System Restarts
Unneeded ports and services that represent vulnerabilities.

Trojans:

Trojans will generally register in at least two places within the logs. First, the new process that was created after the baseline will show up under the process list. Second, the port on which the Trojan is listening will show up under the port list. Both of these events are easy to spot because the normal system processes and ports are filtered from the report. (see example output below)

Viruses:

Viruses will generally register in the logs generated by this tool in several places. They will register as new processes and depending on the type of virus, they may show up in the port log. Most viruses will also show up under the startup processes header because viruses must add themselves to the startup routine in some way.

Brute force logon attempts

User accounts should be configured to lock after a certain number of failed attempts to logon. This account lockout will show up in the logs. This tool will tell you which user is locked and when it happened. This will show up under the Events heading in the output. It is important to log both success and failure of logon events. While just logging the failures may show you when a brute force attempt has been made, it will not tell you whether the attempt was successful.

Unauthorized Changes to accounts:

Our servers are generally pretty static. Users are relatively rarely added or deleted. This allows for monitoring most account changes without being buried in data. The exact account changes that are logged are described below. Under the Events header, any new or removed accounts, changes to group membership, or even account parameter changes will be logged.

Shared Folders:

All shared folders are enumerated using the winfo tool. This uses the same diff process to filter repetitive log entries. Any shared folders that are added or removed show up in the logs. As a rule, we do not run windows file-sharing if we can at all avoid it. The services associated with windows file and print sharing have a lot of vulnerabilities associated with them. This shared folder information can be used to determine whether file and print sharing are enabled on a machine so that we can turn it off if not necessary. Unfortunately, many of our server require these services due to the implementation of the software they run.

Some viruses use open shares to spread. They scan the network for unsecured shares and use them to spread and infect users. Many times shares

© SANS Institute 2005 Author retains full rights.

get created for temporary use and are forgotten. These temporary shares usually are not secured and can be an exposure risk for your data. Sometimes shares are used to distribute sensitive or copyrighted material so file sharing is an important thing to monitor. Some attack tools known to target windows shares are W32/Deloder, GT-bot, sdbot, and W32/Slackor. (see CERT® Advisory CA-2003-08)

Something that is easy to forget is that by default, windows installs administrative shares that do no show up under shared folders or using net view. Admin shares are sharing of root partitions, the system root folder, the FAX$ share, the IPC$ share, and the PRINT$ share. The last of three of the shares listed always use the same name and are consequently prime targets for scripts. These shares are supposed to allow administrators to access systems over the network and therefore are naturally security risks. Disabling file-sharing takes care of this risk. When file-sharing can't be removed completely this tool will enumerate these shares as well.

System Restarts:

I chose to disable harvesting of the system restart log because when the system reboots, it is obvious by looking at the other aspects logged. A reboot generates a great deal of log information. Most processes, except a few system processes, are assigned a new PID every time the service restarts. Therefore a reboot will generate a list of processes other than those processes like system that are always the same. The system process is always 8. Also, many of the driver and network configurations dumped by Msinfo list the time and date of the last reset.

Open Ports:

Keeping track of the open ports on a server is important for several reasons. It is a key way to spot backdoors installed on a system but also a way to verify that un-needed vulnerable services are disabled. Using a program like fport (netstat –o in Windows 2003) also correlates the port with the software communicating on a given port. This allows system administrators to see at a glance all of the services and software that are open to the network and therefore open to attack. Changes to ports are therefore critical to keep track of. With certain server applications like SQL, fport (or netstat) will even show the remote hostname of the machine connected to a certain port. This can be useful to determine how many SQL connections exist and who is connected at any given time. Unauthorized connections are generally easy to spot. This depends, however, on whether you have a standard for host names so that hostnames that don't fit your standard are easily spotted.

Most server daemons generally keep specific ports open in order to constantly wait for incoming connections. Once the server is configured and

© SANS Institute 2005 Author retains full rights.

locked down, a set of ports will be always open. The batch file filters these ports from the log file after the baseline is taken so that the administrator only sees when ports change, appear, or disappear. Other services (like SQL) create new ports for each connection to the server.

Process List:

The batch file uses tlist.exe available from the Microsoft security toolkit. This tool lists all of the processes open. The output is the same as you see in the task manager under the processes tab. The batch script detects either if a new process exists or if a process has restarted (if it changed pid) or if a process has closed. Using the parameter -s when calling tlist, all of the services active in a process. Some system processes encompass several services. Tlist output for the service.exe process using the –s flag may return:

248 SERVICES.EXE Svcs:
Alerter,Browser,dmserver,Eventlog,lanmanserver,lanma
nworkstation,LmHosts,PlugPlay,ProtectedStorage,seclogon,Wmi

Events Audited:

The dumpel tool is available from Microsoft. It is available in the Microsoft Resource Kit or freely downloadable from the Microsoft website at: http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/dumpel-o.asp

It dumps specific types of events from the windows log. It is a command line tool that takes an event id argument specifying the type of event to dump. I gathered a list of the most critical events that were likely to show suspicious activity. (Some of these events occurred during regular use in the test runs, these events are fairly frequent and often overlapped with less frequent events and were disabled. The disabled event logs have "off" in the 4th column of the table but were included for the sake of completeness.)

ID	Event Name	Type	
512	Windows starting up	System	
517	The security log was cleared.	System	
529	The logon attempt was made with an unknown user name or a known user name with a bad password.	Security	
531	Account currently disabled	Security	
533	User not allowed to logon at this computer	Security	

© SANS Institute 2005 Author retains full rights.

534	The user attempted to log on with a logon type that is not allowed, such as network, interactive, batch, service, or remote interactive.	Security	
535	The specified account's password has expired	Security	
539	Logon failed-Account locked out	Security	
576	Special privileges assigned to new logon	Security	off
577	A user attempted to perform a privileged system service operation.	Security	off
578	Privileges were used on an already open handle to a protected object.	Security	off
592	A new process was created	Security	off
608	A user right was assigned.	Security	
612	An audit policy was changed.	Security	
614	IPSec policy agent disabled	Security	
624	A user account was created.	Security	
626	User account enabled	Security	
627	A Password Change Attempted; this event records both successful and failed attempts.	Security	off
628	User account password set	Security	off
630	User account deleted	Security	
636	User added to Administrators group	Security	
642	A user account was changed.	Security	
644	A user account was locked out; when an account is locked out, two events will be logged at the primary domain controller (PDC) emulator operations master. A 644 event will occur, indicating that the account name was locked out. Then a 642 event will be recorded, indicating that the user account is now locked out. This event is logged only at the PDC emulator.	Security	

© SANS Institute 2005 Author retains full rights.

MSInfo:

This tool is built into windows 2000 and 2003. It reports many different aspects of windows in great detail. This system uses this program to log changes to registry entries related to startup programs, network configuration, and drivers. This tool generates very detailed reports for each aspect. This is the slowest part of the system as each run of msinfo can take a minute or two and it is run separately for each of the three types of reports. The reports generated by msinfo are quite extensive. They are actually dumped in a table format. These tables are tab delimited and are much more understandable when imported into excel than viewed as text.

Filtering:

I used a free program called windiff to filter the output. The way that I set the system up, the batch program generates a baseline the first time it is run. The second time it is run, the program uses windiff to compare the original output with the output generated by the second run and displays only differences between the two. This means that a new baseline is generated each time the program is run. This will catch all changes, but these changes will only show up once in the logs. The batch program could easily be modified to take only one baseline if that would suit your needs better. If logs are not going to be reviewed daily for instance, it would be easy to miss key events because they only show up once or twice in the logs using this comparing method. Events sometimes show up twice because they are reported when they are new events in the logs, and a second time when they are cleared from the logs.

DumpEL bat contents:

These batch files are all the same except the filenames, event source and ID. The source and event ID in these bats correspond to the log entry type described by the bat filename. I found that dumpel required different amounts of time to process the event dumps. This meant that putting the dump commands contained in the batches in a single file would cause the whole process to fail after the first dump command. There are tools that will pause the script for a time to wait for a secondary process to end, but this way each process only takes as much time as it needs and doesn't slow the execution of the batch script more than necessary.

Sample Dumpel Batch:

Each bat file will generate a corresponding text file of the same name in the C:\CSD\Compare\Dumpbats\out\ folder.

```
C:\CSD\bin\DUMPEL.EXE -f
C:\CSD\Compare\Dumpbats\out\AccountCurrentlyDisabled.txt -l security -c -m
```

© SANS Institute 2005 Author retains full rights.

```
Security -e 531 -d 1
Exit
```

fileappend.bat contents:

This batch file appends the output of the individual batch files into a single file. It then compares the older and newer dump output and appends the difference to the main report. Any events dumped by the dumpel tool will be are collected under the Events heading in the output.

```
del C:\CSD\Compare\Dumpbats\out.txt
C:\CSD\Compare\bin\forall C:\CSD\Compare\Dumpbats\out\*.txt : type @f >>
C:\CSD\Compare\Dumpbats\out.txt


C:\CSD\bin\diff.exe C:\CSD\Compare\Dumpbats\out.txt
C:\CSD\Compare\Dumpbats\out2.txt >> C:\CSD\Compare\reportc.txt
del C:\CSD\Compare\Dumpbats\out2.txt
rename  C:\CSD\Compare\Dumpbats\out.txt out2.txt

exit
```

Output:

The output is file C:\CSD\Compare\reportc.txt. The batch file inserts the date and time that it is run every time using built-in windows commands. Dividing lines are inserted between the output of the different programs to make reading the output easier. New processes, ports, or account modifications will be proceeded with the < symbol. Processes, ports that are closed between runs appear in the log after the > symbol. Most events will show up twice.

Sample Output: Normal operation- no significant changes in ports, accounts, shared folders, drivers or processes.

```
Server Name
Thu 12/16/2004
10:48p
Port Scan--------------------------------------
10c10
< 8     System        ->  1030  TCP
---
> 8     System        ->  1029  TCP
Process Scan-----------------------------------------
24,25c24,25
< 1172 CMD.EXE          C:\WINNT\system32\cmd.exe
<  364 tlist.exe
---
> 1216 CMD.EXE          C:\WINNT\system32\cmd.exe
> 1040 tlist.exe
Drivers----------------------------------------
```

© SANS Institute 2005 Author retains full rights.

```
1c1
< System Information report written at: 12/16/2004 10:48:40 PM
---
> System Information report written at: 12/16/2004 09:48:10 PM
Network--------------------------------------
1c1
< System Information report written at: 12/16/2004 10:50:47 PM
---
> System Information report written at: 12/16/2004 09:50:17 PM
startups-------------------------------------
1c1
< System Information report written at: 12/16/2004 10:50:47 PM
---
> System Information report written at: 12/16/2004 09:50:17 PM
SharedFolders--------------------------------------
Events-------------------------------------
```

Note: the CMD and tlist entries in the log will always show up because they are run as new processes each time the batch is run. Each time they are run, they are assigned a new pid and therefore will register as a difference when compared. The Winfo dumps under the headings Drivers, Network, and Startups in the report will always have the date and time of the current and last runs because these lines will always differ. This is kind of nice because this way you can verify that all the dumps were executed successfully. The process with a pid of 8 called system also frequently shows up, usually on ports around 1030.

Output After sub7 infection:

The following output shows what it looks like when the box is infected with the Sub7 Trojan. Under the Fport header, the entry hwiynvs.exe is shown to be listening on port 27374. It also shows up under the tlist header as pid 1560 hwiynvs.exe. The < symbol means that it is a new process added since the last scan. In most cases sub7 will also show up under new startup processes.

```
Sat 12/11/2004
 6:18p
Fport----------------------------------------
18d17
< 1560  hwiynvs      ->  27374 TCP   C:\WINNT\hwiynvs.exe
tlist----------------------------------------
32d31
< 1560 hwiynvs.exe
34c33
< 1400 tlist.exe
---
>  144 tlist.exe
Drivers--------------------------------------
1c1
< System Information report written at: 12/11/2004 06:18:40 PM
---
> System Information report written at: 12/11/2004 05:18:09 PM
Network--------------------------------------
```

© SANS Institute 2005 Author retains full rights.

```
1c1
< System Information report written at: 12/11/2004 06:19:42 PM
---
> System Information report written at: 12/11/2004 05:19:20 PM
startups--------------------------------------
1c1
< System Information report written at: 12/11/2004 06:19:43 PM
---
> System Information report written at: 12/11/2004 05:19:15 PM
SharedFolders-------------------------------------
Events-----------------------------------
```

Output after new user created:

This is the output generated after a new user is created. It shows the output of the dumpel tool and the type of information that is logged. It is a little cryptic but the event ids, in this case 642 and 624 are described in the table above. 624 means a user account was created. 642 means a user account was changed. The log lists the date, time, and parameters such as whether the "password never expires" box is checked. If a user is created, the new username is listed, in this case l33t. These logs appear only once, but a list of these important dumped events occurring over the course of the last day can be found in the file C:\CSD\Compare\Dumpbats\out2.txt.

```
Sun 12/12/2004
12:06a
Fport----------------------------------------
tlist----------------------------------------
36,37c36,37
< 1420 CMD.EXE          C:\WINNT\system32\cmd.exe
< 1740 tlist.exe
---
> 2120 CMD.EXE          C:\WINNT\system32\cmd.exe
> 1964 tlist.exe
  Drivers---------------------------------------
1c1
< System Information report written at: 12/12/2004 12:08:40 AM
---
> System Information report written at: 12/12/2004 11:08:09 PM
Network-------------------------------------
1c1
< System Information report written at: 12/12/2004 12:10:22 AM
---
> System Information report written at: 12/12/2004 11:11:31 PM
startups--------------------------------------
1c1
< System Information report written at: 12/12/2004 12:13:11 AM
---
> System Information report written at: 12/12/2004 11:12:12 PM
SharedFolders-------------------------------------
Events-----------------------------------
13,15d12
```

© SANS Institute 2005 Author retains full rights.

```
< 12/12/2004,12:06:08 AM,8,7,642,Security,PANDORA\user,,PANDORA,Account Enabled.
        'Password Not Required' - Disabled l33t PANDORA %{S-1-5-21-1993962763-
963894560-725345543-1011} user PANDORA (0x0,0xC08A) -
< 12/12/2004,12:06:09 AM,8,7,642,Security,PANDORA\user,,PANDORA,- l33t PANDORA %{S-
1-5-21-1993962763-963894560-725345543-1011} user PANDORA (0x0,0xC08A) -
< 12/12/2004,12:06:09 AM,8,7,642,Security,PANDORA\user,,PANDORA,- l33t PANDORA %{S-
1-5-21-1993962763-963894560-725345543-1011} user PANDORA (0x0,0xC08A) -
22d18
< 12/12/2004,12:06:08 AM,8,7,624,Security,PANDORA\user,,PANDORA,l33t PANDORA %{S-1-
5-21-1993962763-963894560-725345543-1011} user PANDORA (0x0,0xC08A) -
```

Administration:

On my systems, I decided to schedule the batch script to run every hour. Once a day, another batch script kicks off that zips the logs and ftps them to my workstation and resets the logs. This is really quite necessary because it would be too time consuming to go to each server every day and check the audit output. Sending the audit information to another machine also ensures that the data is not manipulated during a compromise. Now I have a daily report from each of our servers that describes any changes in the system that occurred over the last day.

After:

I have found that on our systems I can review the daily activity on each server in about 10 minutes unless major changes have occurred. While this package will not detect all the possible hacks out there it at least provides some notification if any significant changes have been made by an attacker. This system still requires an understanding of standard windows processes and ports. You still have to know what to look for in the logs because windows generates lots of events and changes during a standard day. It does not solve the problem of monitoring security but simply provides more information for the administrator. The shortcomings of the windows event log has long been a source of frustration to administrators and this tools provides valuable perspectives that make up for these shortcomings and combine its functionality with other important tools.

This system has proven useful not only in regard to security, but also has helped us spot other kinds of problems early. When a problem occurs on a server, I now check the audit logs very early in the troubleshooting because it often contains hints about what happened. If a service fails, a user account is locked, or a driver is corrupted, it shows up in the logs.

This audit system provides a good ongoing overview of the system, but to run system securely, the box must also be configured correctly. This tool does not address this issue. It does not audit policies or do vulnerability testing. The main reason this wasn't included in the audit system was that my workplace already has auditing tools for determining policy compliance in regard to

© SANS Institute 2005 Author retains full rights.

settings like minimum password length and password encryption level. Also, this tool was developed in order to monitor the server as it is deployed and configuration information would be added noise to the reports.

This system has provided a useful perspective on the everyday use of our servers and helped me to understand what events and changes occur regularly on a system and which are more suspect. It has taken some refining to get the balance between too much and too little information to log. This will probably continue evolving but so far we have had no major incidences since this system was installed and we now have a much greater overview of what is occurring on our servers on a daily basis. This system is quite simple but not much of importance can occur on the system without something showing up in the logs. I have found it to be a very useful addition to our defense-in-depth strategy.

References:

Magalhaes, Ricky "Host-Based IDS vs Network-Based IDS (part 1)". July 10, 2003
http://www.windowsecurity.com/articles/Hids_vs_Nids_Part1.html

Rowland,Craig "Sentry Tools Summary". June 06, 2003
http://sourceforge.net/projects/sentrytools/

Kazienko, Przemyslaw & Dorosz, Piotr "Intrusion Detection Systems (IDS) Part2-Classification;Methods;Techniques" June 15, 2004
http://www.windowsecurity.com/articles/IDS-Part2-Classification-methods-techniques.html

Singh, Amit "A Taste of Computer Security".
http://www.kernelthread.com/publications/security/intrusion.html

Zadjmool, Ray "The Science of Host Based Security". July 23, 2004
http://www.windowsecurity.com/articles/Science_Host_Based_Security.html

N/A "CERT® Advisory CA-2003-08 Increased Activity Targeting Windows Shares" March 11, 2003 http://www.cert.org/advisories/CA-2003-08.html

Links:

Fport - http://www.foundstone.com/knowledge/proddesc/fport.html
Tlist – Comes on Windows server disk
Dumpel - http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/dumpel-o.asp
Windows Scheduler - http://www.splinterware.com/products/wincron.htm

Appendix - Batch code:

© SANS Institute 2005 Author retains full rights.

The Batch file code:

Note: I have put the fport.exe, tlist.exe, winfo.exe and DumpEL.exe in a folder in C:\CSD\Bin\ and the reports in a folder C:\CSD\Compare\. Make sure to recreate this or modify the batch program to suit your needs.

```
type C:\CSD\Compare\ServerName.txt >> C:\CSD\Compare\reportc.txt

date /T >> C:\CSD\Compare\reportc.txt
Time /T >> C:\CSD\Compare\reportc.txt

rem fport compare
echo Fport---------------------------------------- >> C:\CSD\Compare\reportc.txt

C:\CSD\bin\fport.exe > C:\CSD\Compare\fport1.txt
C:\CSD\bin\diff.exe -a C:\CSD\Compare\fport1.txt C:\CSD\Compare\fport2.txt >>
C:\CSD\Compare\reportc.txt
del C:\CSD\Compare\fport2.txt
rename  C:\CSD\Compare\fport1.txt fport2.txt


rem tlist Compare
echo tlist---------------------------------------- >> C:\CSD\Compare\reportc.txt

C:\CSD\bin\tlist.exe > C:\CSD\Compare\tlist1.txt
C:\CSD\bin\diff.exe -a C:\CSD\Compare\tlist1.txt C:\CSD\Compare\tlist2.txt >>
C:\CSD\Compare\reportc.txt
del C:\CSD\Compare\tlist2.txt
rename  C:\CSD\Compare\tlist1.txt tlist2.txt


rem MSinfo Driver compare
echo Drivers------------------------------------- >> C:\CSD\Compare\reportc.txt

C:\Progra~1\Common~1\Micros~1\MSInfo\MSInfo32.exe /report
C:\CSD\compare\msinfob1.txt /categories +SWEnvDrivers
type C:\CSD\compare\msinfob1.txt > C:\CSD\compare\msinfo1.txt

C:\CSD\bin\diff.exe -a C:\CSD\Compare\msinfo1.txt
C:\CSD\Compare\msinfo2.txt >> C:\CSD\Compare\reportc.txt
del C:\CSD\Compare\msinfo2.txt
rename  C:\CSD\Compare\msinfo1.txt msinfo2.txt


rem MSinfo Network Config compare
echo Network------------------------------------- >> C:\CSD\Compare\reportc.txt
```

© SANS Institute 2005 Author retains full rights.

```
C:\Progra~1\Common~1\Micros~1\MSInfo\MSInfo32.exe /report
C:\CSD\compare\nmsinfob1.txt /categories +ComponentsNetwork
type C:\CSD\compare\nmsinfob1.txt > C:\CSD\compare\nmsinfo1.txt

C:\CSD\bin\diff.exe -a C:\CSD\Compare\nmsinfo1.txt
C:\CSD\Compare\nmsinfo2.txt >> C:\CSD\Compare\reportc.txt
del C:\CSD\Compare\nmsinfo2.txt
rename  C:\CSD\Compare\nmsinfo1.txt nmsinfo2.txt


rem MSinfo Startup Programs compare
echo startups------------------------------------- >> C:\CSD\Compare\reportc.txt

C:\Progra~1\Common~1\Micros~1\MSInfo\MSInfo32.exe /report
C:\CSD\compare\startupsb1.txt /categories +SWEnvStartupPrograms
type C:\CSD\compare\startupsb1.txt > C:\CSD\compare\startups1.txt

C:\CSD\bin\diff.exe -a C:\CSD\Compare\startups1.txt
C:\CSD\Compare\startups2.txt >> C:\CSD\Compare\reportc.txt
del C:\CSD\Compare\startups2.txt
rename  C:\CSD\Compare\startups1.txt startups2.txt


rem shared folders
echo SharedFolders------------------------------------- >> C:\CSD\Compare\reportc.txt

C:\CSD\Compare\bin\Winfo.exe 127.0.0.1  > C:\CSD\compare\shares1.txt
C:\CSD\bin\diff.exe -a C:\CSD\Compare\shares1.txt
C:\CSD\Compare\shares2.txt >> C:\CSD\Compare\reportc.txt
del C:\CSD\Compare\shares2.txt
rename  C:\CSD\Compare\shares1.txt shares2.txt


rem dumpEL Compare
echo Events------------------------------------- >> C:\CSD\Compare\reportc.txt
del C:\CSD\Compare\Dumpbats\out.txt
start C:\CSD\Compare\Dumpbats\AccountCurrentlyDisabled.bat
start C:\CSD\Compare\Dumpbats\AccountLocked.bat
start C:\CSD\Compare\Dumpbats\AuditPolicyChanged.bat
start C:\CSD\Compare\Dumpbats\IPSecDisabled.bat
start C:\CSD\Compare\Dumpbats\LogonAccountLocked.bat
start C:\CSD\Compare\Dumpbats\LogonBadUserOrPass.bat
start C:\CSD\Compare\Dumpbats\LogonWrongType.bat
start C:\CSD\Compare\Dumpbats\PasswordExpired.bat
start C:\CSD\Compare\Dumpbats\Rightassigned.bat
```

© SANS Institute 2005 Author retains full rights.

```
start C:\CSD\Compare\Dumpbats\SecLogCleared.bat
start C:\CSD\Compare\Dumpbats\TimeRestrictionViolation.bat
start C:\CSD\Compare\Dumpbats\UserAccountChanged.bat
start C:\CSD\Compare\Dumpbats\UserCreated.bat
start C:\CSD\Compare\Dumpbats\UserEnabled.bat
start C:\CSD\Compare\Dumpbats\UserNotAllowedLogon.bat
start C:\CSD\Compare\Dumpbats\WinStartup.bat
start C:\CSD\Compare\Dumpbats\UserDeleted.bat
start C:\CSD\Compare\Dumpbats\UserMadeAdmin.bat
start C:\CSD\Compare\Dumpbats\fileappend.bat
exit
```

© SANS Institute 2005, Author retains full rights.

Last Updated: July 31st, 2016

Upcoming SANS Training

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

SANS Vienna	Vienna, AT	Aug 01, 2016 - Aug 06, 2016	Live Event
SANS Boston 2016	Boston, MAUS	Aug 01, 2016 - Aug 06, 2016	Live Event
DEV531: Defending Mobile Apps	San Francisco, CAUS	Aug 08, 2016 - Aug 09, 2016	Live Event
SANS Portland 2016	Portland, ORUS	Aug 08, 2016 - Aug 13, 2016	Live Event
SANS Dallas 2016	Dallas, TXUS	Aug 08, 2016 - Aug 13, 2016	Live Event
DEV534: Secure DevOps	San Francisco, CAUS	Aug 10, 2016 - Aug 11, 2016	Live Event
Data Breach Summit	Chicago, ILUS	Aug 18, 2016 - Aug 18, 2016	Live Event
SANS Chicago 2016	Chicago, ILUS	Aug 22, 2016 - Aug 27, 2016	Live Event
SANS Virginia Beach 2016	Virginia Beach, VAUS	Aug 22, 2016 - Sep 02, 2016	Live Event
SANS Alaska 2016	Anchorage, AKUS	Aug 22, 2016 - Aug 27, 2016	Live Event
SANS Bangalore 2016	Bangalore, IN	Aug 22, 2016 - Sep 03, 2016	Live Event
SANS Brussels Autumn 2016	Brussels, BE	Sep 05, 2016 - Sep 10, 2016	Live Event
SANS Adelaide 2016	Adelaide, AU	Sep 05, 2016 - Sep 10, 2016	Live Event
SANS Northern Virginia - Crystal City 2016	Crystal City, VAUS	Sep 06, 2016 - Sep 11, 2016	Live Event
SANS Network Security 2016	Las Vegas, NVUS	Sep 10, 2016 - Sep 19, 2016	Live Event
SANS ICS London 2016	London, GB	Sep 19, 2016 - Sep 25, 2016	Live Event
SANS London Autumn	London, GB	Sep 19, 2016 - Sep 24, 2016	Live Event
Security Leadership Summit	Dallas, TXUS	Sep 27, 2016 - Oct 04, 2016	Live Event
SANS Seattle 2016	Seattle, WAUS	Oct 03, 2016 - Oct 08, 2016	Live Event
SANS Oslo 2016	Oslo, NO	Oct 03, 2016 - Oct 08, 2016	Live Event
SANS DFIR Prague 2016	Prague, CZ	Oct 03, 2016 - Oct 15, 2016	Live Event
SANS Baltimore 2016	Baltimore, MDUS	Oct 10, 2016 - Oct 15, 2016	Live Event
SANS Tokyo Autumn 2016	Tokyo, JP	Oct 17, 2016 - Oct 29, 2016	Live Event
SANS Tysons Corner 2016	Tysons Corner, VAUS	Oct 22, 2016 - Oct 29, 2016	Live Event
SANS San Diego 2016	San Diego, CAUS	Oct 23, 2016 - Oct 28, 2016	Live Event
SANS Munich Autumn 2016	Munich, DE	Oct 24, 2016 - Oct 29, 2016	Live Event
SOS SANS October Singapore 2016	Singapore, SG	Oct 24, 2016 - Nov 06, 2016	Live Event
SANS FOR508 Hamburg in German	Hamburg, DE	Oct 24, 2016 - Oct 29, 2016	Live Event
Security Awareness Summit & Training	OnlineCAUS	Aug 01, 2016 - Aug 10, 2016	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced