

# Auditing Windows NT

## Verifying That Your Systems Remain Secure

Chris Brenton  
cbrenton@sover.net

*Auditing WinNT - SANS' LevelOne*

1

Greetings! I'm Chris Brenton and I'll be presenting today's talk on auditing Windows NT as a method of verifying that your computer systems remain secure. I would like to start by thanking JD Glasser of NTObjectives and Phil Sointu of Alpine Computers for their contributions in helping me to pull together this material. I would also like to thank all of the folks at SANS for providing this forum where we can all learn to work a little smarter. Now let's get busy as we have a lot of ground to cover.

## We're all in the same boat

- Too many systems to manage
- Little resources or budget
- The "pointy-haired factor"
  - Forrester Research released a report saying firewalls are "bad"
- How do you keep control?

*Auditing WinNT - SANS' LevelOne*

2

The first thing you should realize is that when it comes to security, we are all in the same boat. In "the good old days", IS departments received fairly large budgets considering the number of systems they needed to maintain. Typically, there was just a single mini or mainframe that the IS staff would be charged with maintaining. It was not uncommon for each member of the IS staff to have a fairly narrow scope of responsibility. This left everyone with plenty of bandwidth to make sure their jobs got done right.

Today all bets are off. Budgets are relatively tighter, systems are more complex and the ratio of support people to the number of systems has dropped dramatically. The Internet has also brought with it its own set of problems. Attackers now have a potential conduit into your network which is available 24 hours a day, as well as a transport for informing others about the latest hacks and exploits. If you do not keep up, you are setting yourself up to become a victim.

Another daemon at work is what I like to refer to as "the pointy-haired factor". Many of us have bosses that expect the world but are unwilling to give us the tools to get the job done. This is amplified by the fact that if your boss is not a "hands on" type, they are most likely pulling their information and advice from other non-hands on types.

A good example of this is a recent article published by Forrester Research on the drawbacks of trying to use a firewall in the modern e-commerce world. While the article has some valid points, unfortunately if the person reading the article is technically challenged the only real detail that seems to come through is "firewalls are bad". I say this because I have spoken to a number of CIO types since that publication that have begun their security dissertation with "Well according to Forrester Research...". So not only do you have too little resources to work with, you have upper management charting the IT course based on executive snippets.

So with all this going on you need to figure out how to maintain control of your environment. The question is, how? The objective of this course is to show you how to do exactly that

## Course Prerequisites

---

- Windows NT 4.0
- Service Pack 4 or higher
  - Service packs are available on Microsoft's FTP site
- Latest Copy of the NT Resource Kit
  - carried by most major book stores
- Basic Knowledge of NT

*Auditing WinNT - SANS' LevelOne*

3

Course Prerequisites. The prerequisites of this course are somewhat basic. You should be running a patched version of NT 4, either server or workstation. You will also need a copy of the NT Resource kit. I will include in my talk tools which are part of a standard NT install but unfortunately the stock tools are pretty weak. You need to go to the resource kit for the good stuff.

## What is an audit?

- Verification of system integrity
- Augment other security precautions
  - Security is **not** one stop shopping!
- Does not prevent intrusions!
  - Provide clues when it occurs
  - Help raise security awareness
- Last line of defense

*Auditing WinNT - SANS' LevelOne*

4

What is an Audit? An audit, simply put, is the verification the integrity of a system. When you perform an audit, you are insuring that only authorized access has taken place and all changes made to the system are in accordance with your security policy. In other words, you are making sure that everyone is playing nice on your system.

Auditing should not be considered a replacement for the other security precaution you are currently enforcing on your network. For example don't throw away your password policy just because you are performing regular audits. The old analogy is that security should be like an onion with your data tucked safely away at the center. Think of your security measures as being the different layers of the onion. The more layers you have in place, the safer your data will be. Auditing is simply one of these layers.

Its important to keep in mind that auditing does not directly prevent people from attacking your system. Its more of a last line of defense when all other security precautions fail. For example a strong password policy will help keep an intruder out while auditing will not. If an intruder does break in however, it will be auditing that helps you to spot the attack. Auditing is also a very good way of becoming aware of what is normal activity for your systems. For example, try the exercise shown in the next slide titled "How well do you know your own system"?

## How well do you know your own system?

- If you are running Windows or Unix, open a command prompt
- Type: netstat -a |more
- Look for lines marked "listening"
- These are open service ports
- Can you identify them all?

*Auditing WinNT - SANS' LevelOne*

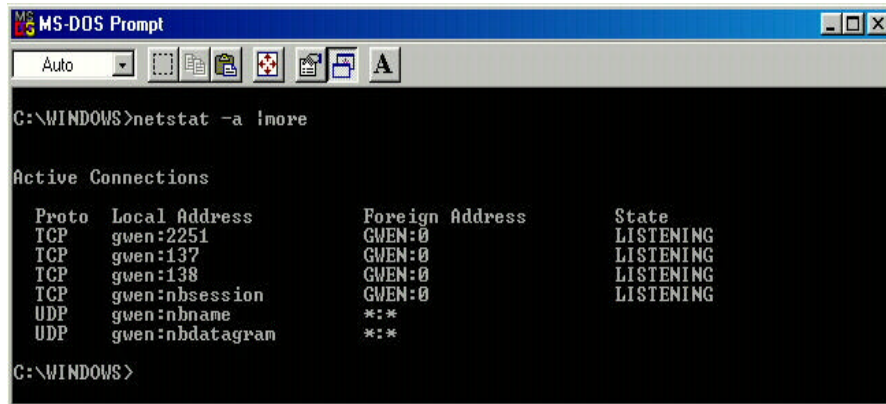
5

In this exercise I want you to open a command prompt on the computer you are currently using. At the command prompt, I want you to type the command "netstat -a |more" and then press the enter key.

Now, take a good look at the output being reported. This is the current connection table for your system. The local address column will show the communication port your system is using while the foreign address column will identify the name of the remote system as well as the communication port that system is using. If you look at the state column, any connections listed as "established" are active connections. You may also see a few "time wait" or "syn sent" entries.

The real interesting entries are the one's labeled "listening". These are open service ports on your system which are waiting for a remote system to connect to your machine. In other words, there is some active process running on your system that is offering services to any system on the network that tickles this port. The \$64 question is, can you identify each of the processes running on your machine that have opened each of the listed listening ports?

## Why is TCP/2251 open?



```
MS-DOS Prompt
Auto
C:\WINDOWS>netstat -a /more

Active Connections

Proto Local Address           Foreign Address         State
TCP   gwen:2251                GWEN:0                  LISTENING
TCP   gwen:137                 GWEN:0                  LISTENING
TCP   gwen:138                 GWEN:0                  LISTENING
TCP   gwen:nbssession         GWEN:0                  LISTENING
UDP   gwen:nbname              *:*
UDP   gwen:nbdatagram         *:*
```

Auditing forces you to figure out what's going on

*Auditing WinNT - SANS' LevelOne*

6

If you take a look at the slide “Why is TCP/2251 open?”, you’ll see a screen capture from one of my systems. This computer has four ports listed as listening. The last three are used by Windows for file and print sharing but the first entry is an odd ball. I am unaware of any process running on this system that should be listening on TCP port 2251. So why is this port open? Obviously I need to do some investigation work to find out exactly what is running on this machine.

This is one of the cool things about auditing, it forces you to look at the system in great detail and come up with a logical explanation for everything you see. What better way to figure out all of the nuances of how your system functions?

## Why perform audits?

---

- Identify when an intrusion occurs
- Identify extent of the compromise
- Useful when all other security measures fail
  - Damage control
  - Document for corrective action and/or legal action

So, why perform audits? We perform audits to identify when an intrusion occurs. If an intrusion is detected, our audit is used to then determine what portions of the system have been compromised. For example did the attacker load up a back door which is now waiting for them to come back in? Did the attacker change or access critical system or data files? In short, our audit should tell use the amount of damage control we need to perform.

## But I have a firewall!!!

- Most intrusions occur from within
- A strong security posture is layered
  - Single point of failure is “a bad thing”
  - Backup tapes are a form of layering
- FW-1 DNS hole
  - [www.geek-speak.net/tricks&tips.html](http://www.geek-speak.net/tricks&tips.html)
  - What about other products?

A common query I hear is “But I have a firewall. Why do I need to perform audits?”. There are a number of reasons why you do not want to rely on just your perimeter security to keep your environment secure. To start there have been quite a few studies that have looked at where attacks originate, from within the compromised network itself or from an outside location such as the Internet. While the statistics vary from study to study, one common thread is that a majority of attacks originate from inside the network perimeter. From a statistical point of view, this means that your firewall has less than a 50% chance of protecting you from possible attack. Clearly this number should not leave you with the warm fuzzes.

A good security posture is layered. This is why we do backups. It's not that we need to keep track of yet another copy of our data, rather we are hedging our bets against hard disk failure, fat fingered end users as well as a host of other potentially data lethal situations. So by auditing we are “backing up” the other security measure we have put into place, including the firewall.

One last point on why layered security is important before we move on. Go to the page in the indicated URL and follow the link to Checkpoint Firewall-1 and then Invisible Traffic Due to Default Properties Setting. This page documents a security hole with Firewall-1 which showed up in version two and still exists in version four which is the current shipping version. In short, the default settings of the firewall allow an attacker to pass traffic to internal systems and not have any of the traffic show up in the logs. Let me repeat, if you leave Firewall-1 at the default properties settings, an attacker can get at your internal systems without making an entry in your firewall log. This means that if Firewall-1 is your only line of defense and you have not changed these settings, you're hosed. While this example is specific to Firewall-1, I think it illustrates why relying on a single security precaution should be considered to be a bad thing.



## What's makes a good audit?

- Detailed baseline
  - Just like a before and after cartoon
  - Too much info is just enough
  - Who cares about successful logons?
- Strong verification
  - Similar to system authentication
  - File dates and sizes can be altered

What makes a good audit? Now that we have discussed why auditing is important, let's take a look at what goes into developing a proper audit. A good audit starts with a detailed baseline. Think of the before and after cartoons you see in the Sunday comics and you'll get the idea. Your baseline is similar to the "before" picture and will be used as a reference to tell you if anything about your system has changed. This is how we go about detecting if something fishy is afoot.

You want to collect as much data as possible. As an example, think about successful logons. Logic tells us that if a potential intruder starts whacking away at the system with a dictionary attack, they are going to generate failed logon attempts. So why not simply log failed logons instead of having to sort through all of the successful logons as well? To answer a question with a question, what happens once the attacker gets in? For example let's say you look at your log and see that someone has been beating up on Bob's logon account. There are quite a few failed logons that show up in the logs but these eventually stop. If you are not tracking successful logon attempts as well, you have no way of knowing if the attacker actually got in or decided to go play else where. In other words you know you've been attacked, but you can't say for sure if the attacker actually got in.

One thing to keep in mind when determining what information should be included in your baseline is how accurately can you verify the data. For example file date and time stamps can easily be changed. Log entries which are stored on the system in question can also be changed. This means that any information you derive from these sources should be considered questionable and verified through some other means.

## What makes a good audit?

---

- A written procedure
  - scope, frequency, responsibility
  - What is considered “normal” data
  - What to do when intrusions are found
  - Detailed disaster recovery plan
  - Could your boss follow the procedure and perform a good audit?

What makes a good audit. In this slide we see that one component of a good audit is a well documented procedure. A procedure ensures that audits are performed in a consistent manner. For example you don't want to find out later that Admin Mary takes the time to look at open listen ports while Admin Bob does not bother. Your procedure should clearly indicate what should be checked, how it should be checked and how often. The mark of any good written procedure is that it is easy to follow. If you can hand your audit procedure over to your boss and they can perform a successful audit, you know you are on the right track.

## What's included in a good Audit?

- As few clues as possible that regular audits are performed
  - Don't leave tools on the system!
    - Burn your tools to a CD
  - Use a secured system for data review
  - Vary the times an audit is performed
  - Let your foe underestimate you

What's included in a good audit? A good audit should leave as few clues as possible that a regular audit is being performed. Armed with the knowledge of what you audit and how, a potential attacker will take steps to try and cover their tracks. Obviously this is a bit of security through obscurity but the less information your attacker has, the more likely they'll trip up and you'll catch them.

Also, make sure you secure the tools you use when performing your audits. I personally like to burn a CD which includes a copy of all my tools as well as the baseline for each of my machines. This insures that I do not have to worry about an attacker replacing them with tools or data that will help to cover their tracks.

## What's included in a good audit?

---

- Who has accessed the system?
  - Share access, Web, FTP, DNS, etc.
- What ports are being serviced?
- Additional services, drivers or tasks running on the machine?
- User/group or permission changes?
- Unexpected files/registry changes?

The next slide talks about what types of information you may wish to include in your audit. Obviously one of the first things you want to check is your access logs. Don't limit the scope to just Windows share sessions. Make sure you include the logs for any active service running on the machine which offers a network service. Remember that network services leave listening ports open so any of these could be a potential portal into your machine.

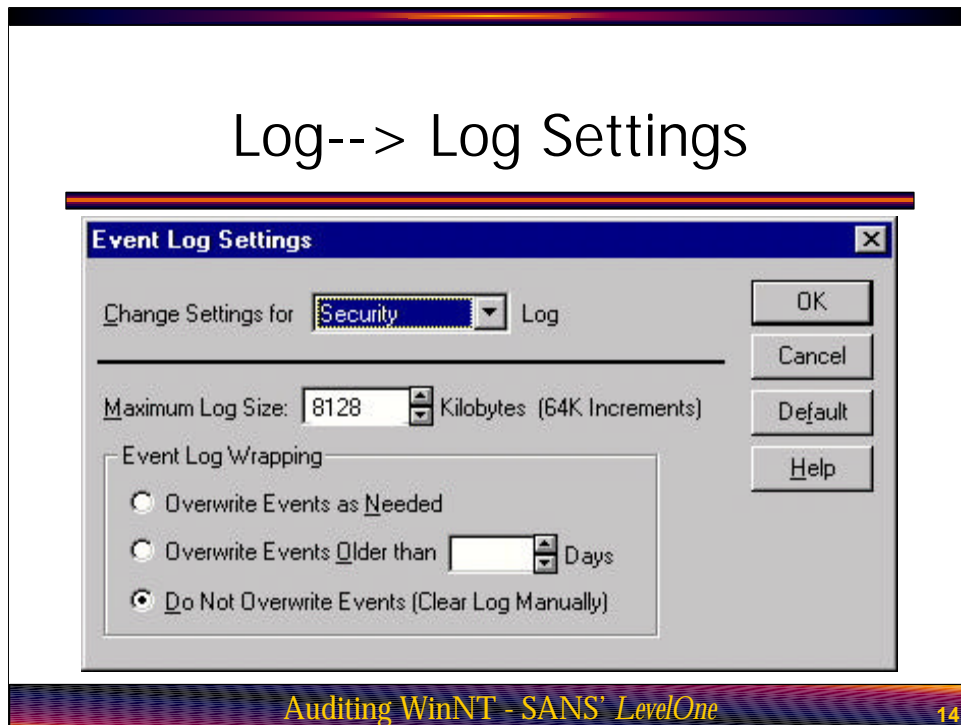
## Working with Event Viewer

- Part of Administrative Tools Group
- Central logging utility for NT
  - Not all applications use Event Viewer
    - IIS logs to WINNT\system32\LogFiles
    - Proxy logs to WINNT\system32\msplogs
- NT does minimal logging by default
- NT saves minimal data

Working with Event Viewer. Its now time to get into the nitty gritty or performing our audit by looking at the Event Viewer utility. Event Viewer can be found in the Administrative Tools group of your NT system. Event Viewer is the central logging utility of any NT system. Most application, including the NT system itself, log events to one of Event Viewer's three logs. These logs are system, security and application. Obviously most of the information we will be working with shows up in the security log.

One of the problems with NT is that it performs and saves minimal logging by default. Obviously if we will be auditing the system we will want to tweak these settings a bit. From the Event Viewer menu, select Log, Log Settings. This will produce a dialog box similar to the one shown in the next slide.

## Log--> Log Settings



Log, Log Settings. From the Event Log Settings dialog box, we can use the “Change settings for” pull down menu to view settings for each of the three logs. One of the first things I like to do is bump up the maximum size of each of the logs to 8 megs or so. Disk space is cheap. What better way to use it than to keep track of your systems health? Note that when you change the log size it only effects the log shown in the “Change settings for” display. You will need to select all three logs in order to change the size of each.

Now take a look at event log wrapping. By default, NT will overwrite events older than seven days if the maximum log size is reached. The “as needed” option will let NT overwrite entries prior to seven days if needed and the last option will never overwrite entries and requires you to clear the log manually.

Which setting to use is a judgment call on your part. Obviously from a security perspective the “do not overwrite” setting is best. The only problem is that NT has a really bad habit of crashing when its logs become full. With this in mind you may wish to opt for the “overwrite as needed setting”. If you are using a very large log size, this setting should probably not be a problem. Again, it’s a judgment call. Go with the setting that you feel most comfortable with.

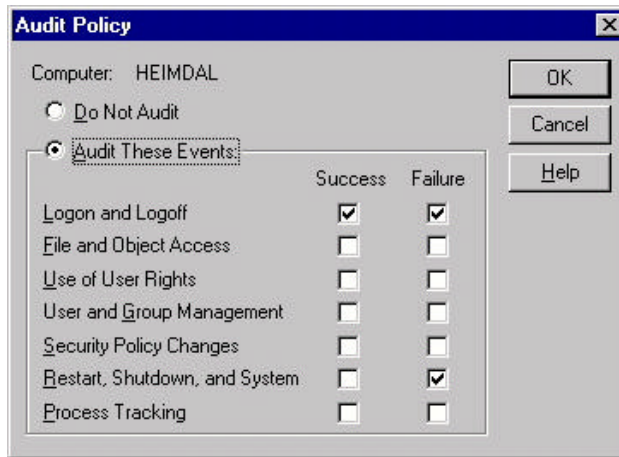
## User Manager

- Typically used for managing users and groups
- Also used to set account policies
  - password length, lockout, etc.
- Can be used to set user “rights”
  - Logon remote/local, change time, etc
- Used to identify which events to log

User Manager. User Manager is typically used for managing either local or domain users and groups. This utility is also used to set account policies such as password length, password aging and how many failed logon attempts can occur before an account is locked. User Manager can also be used to define user's rights to certain system activities. For example I like to remove the Administrator's ability to logon over the network. This keeps people from being about to crack the account over the network while still giving me a back door account into the system from the console if I need it.

When many people don't realize is that User Manager is also used to define what events should be recorded in the security log of Event Viewer. To access this screen select Policies, Audit, from the User Manager main menu. This should produce the audit policy window shown in the next slide.

## Policies--> Audit



*Auditing WinNT - SANS' LevelOne*

16

Policies, Audit. By default, NT is configured not to record any of the events listed in the Audit Policy window. Once you click the Audit These Events radial button, you are free to pick and choose which events you wish to record. For each event you can choose to audit successes, failures or both.

The big question is which events should you monitor. Of course the canned security geek answer is "all of them". This may not be practical however. When in doubt, fall back to your security policy to see just how much detail you should be collecting. At a minimum, I suggest you track successes and failures for:

Logon and logoff

Use of User rights

User and group Management

Security policy changes

System restarts and shutdowns



## Checking Logon Access

- Use dumpel.exe to create an ASCII copy of the Event Viewer Logs
- This data can then be imported into a spreadsheet or database for easy sorting

```
dumpel -L security -f logon.txt -s SERVER -c
```

Checking Logon Access. Now that we have tuned up Event Viewer and we are collecting all of the right information, its now time to look at how we're going to keep track of who is accesses the system. The first place to start is obviously the Event Viewer security log.

Log events for an hour or more and you will quickly realize that Event Viewer is pretty but not very functional. It would be time consuming at best to attempt to track when people logon and logoff of the system, let along ensure that you do not scan a record so quickly that you miss the fact that something nasty took place. With this in mind, we need another method of viewing Event Viewer entries.

The NT Resource kit includes a utility called dumpel.exe. This utility can be used to export the contents of Event Viewer to an ASCII file. Once we have exported the data, we can then import it into our favorite spreadsheet or database program. From there, we can sort the data looking for interesting traffic or create pretty graphs for upper management.

The bottom of the slide shows the syntax for using dumpel.exe. The -L switch allows you to define which log you want to export. The -F switch sets the name of the export file. The -S switch defines the name of the remote system to query. The -S switch is important because it allows you to use a batch file to quickly export the security logs from multiple systems on your network from a single location.

## Finding Data in the Logs

- Sort "reason" to look for failed logon attempts
- Sort "workstation name" to look for odd sources of logon
- Sort "Logon ID" to track sessions
- Hide acceptable entries to better hone in on the good stuff

Finding data in the logs. So now that we have exported our security log, let's talk about a few tricks you can use to finding interesting entries. The first thing you can do is sort of the reason column. This will allow you to quickly identify failed logon attempts. A secondary sort on date/time will allow you to hone in on brute force logon attacks.

Since the security log can become quite large, a slick trick is to first go through looking for "normal" traffic and then hide it. Normal is defined as entries you can easily identify which meet your security policy. For example the user khick logging on every morning at 8:00 AM and then logging off at 6:00 PM would be defined as normal if you know khick is a valid user account for a person who works first shift. You can then hide these entries in order to reduce the number of entries you must manually check for problems. Note that I did not say delete as you may find that you actually need these entries for further investigation. You simply want to get these entries out of site while you review the rest of your log.

## Reading The Logs

- Stock authentication package is MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0
- Each session is tracked using a unique Logon ID
  - can be used to match logon/logoff
- See auditcat.hlp for more EV info

Reading the logs. So what type of information should we be checking for in our Event Viewer logs? One of the first things you should check is the authentication package. Unless you have changed it, this should read Microsoft Authentication Package V1 0. If you see a different package, be afraid. As mentioned in the last slide you also want to keep an eye on the logon ID's. When a user connects to NT, they are assigned a unique logon ID. So while you may see 20 logon/logoff records for the user gshaw, each set of two will use a unique logon ID to identify each time the user logged on and then off of the system.

In the next slide we're going to talk about logon types, but I just wanted to mention before moving on that the resource kit includes a file named auditcat.hlp which has a lot of really useful information regarding the data you will find in the event viewer logs.

## Logon Types

- 2 - Interactive logon/logoff
- 3 - Network logon/logoff
- 4 - Started by batch process
- 5 - Started by running service
- 6 - Proxy logon
- 7 - Unlock console (screen saver)

Logon types. Every time a user logs on to the system, their connection will be identified with a logon type. This ID tells you what kind of connection the user made to the system. For example if you see a logon type of 2, this means the user logged on to the server from the system console. A logon type of 7 tells you that the user logged on at the console, but the system was locked via a screen saver password.

The only logon type that I do not have a good description listed for is logon type 6, proxy logon. This is because there appears to be zero information on this logon type. It sounds like it would log connections via a proxy server, but these connections are identified using logon type 3, a standard network logon. If anyone has more information on logon type 6, I would appreciate hearing about it.

## Checking Other Logs

- Web access via IIS

### **Normal file retrieval:**

192.168.1.50, -, 7/16/99, 0:23:35, W3SVC, WWW,  
172.30.252.10, 46277, 171, 145, 401, 5, GET,  
/default.asp, -,

### **Trying to access as Administrator:**

192.168.1.53, Administrator, 7/16/99, 0:33:44, W3SVC,  
WWW, 172.30.252.10, 20, 214, 317, 302, 0, GET,  
/secret\_dir/, -,

Checking Other logs. Along with the Event Viewer security log, you will want to check any other logs being created on the system. For example I mentioned the IIS Web server log. Since this log is already in comma delimited format, we can import it directly into our favorite spreadsheet or database. We could then apply many of the same tricks we use on the Event Viewer log to the IIS log in order to search for interesting information.

For example check out the two log entries. Do you notice some strange about the second entry? In the first log entry, the remote system accessed the Web server using a standard anonymous logon. While this is not stated we know this to be true based on the “-“ entry immediately following the remote system’s IP address. In the second entry the word “Administrator” appears because the user at 192.168.1.53 attempted to authenticate through IIS in order to access the secret dir directory.

## Baseline of Listening Ports

- netstat -a > listen.txt
- Refer to IANA port assignments
  - <ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers>
- Check for possible trojans
  - <http://www.simovits.com/nyheter9902.html>
- No tools to map ports to Service
  - you may have to disable services to find which one services the port

Baseline of Listening ports. At the beginning of this course we went through the exercise of checking the listening ports on your local system. As part of your baseline you will want to document which ports are normally listening. To do this simply run netstat again except this time direct the output to a text file.

Once you know what ports are open on your system, do a quick check of the port numbers to see if the well now port numbers associated with them makes sense. For example if you run the command on a Web server, you would expect to see port 80 open since that's the well know port for HTTP request.

Sooner or later you are going to run across an open port that you just can not figure out. Unfortunately, there are no tools in either stock NT or the resource kit to map open ports to the applications that are using them. This means the only effective way of finding out which application is listening on a specific port is to shut down services and programs one at a time until the port closes. Of course it would be handy to know what services and drivers are running on the machine as well. This procedure is covered in the next few slides.

## Baseline of Services

- netsh.exe will show local/remote running services and drivers

```
netsh \\SERVER /list > services.txt
```

Installed services on \\skylar:

<Abiosdsk>, No separate display name

<bh>, Display name is <Network Monitor Tools and Agent Drivers>

<Browser>, Display name is <Computer Browser>

Baseline of services. The NT resource kit includes a utility called netsh.exe which allows you to manage services and drivers on remote NT systems. While this is primarily a management tool, one of the switches allows you to document all running services and drivers. Since the tool runs over the network, you can again run a batch file from a single system in order to document all servers on your network.

The bottom of the slide shows only a few entries to give you an idea of how the output is formatted. Its not uncommon to see 20 or more entries on the typical NT system.

## Services on Stock NT

---

- "net start" can be used on stock NT
  - Shows services only
  - Must be run locally

These Windows NT services are started:

Alerter  
Computer Browser  
EventLog  
License Logging Service

*Auditing WinNT - SANS' LevelOne*

24

Services on stock NT. If you do not have a copy of the resource kit handy, you can still document running services. This is done using the net start command and a sample of its output is show at the bottom of the slide. Note that the caveats with net start are that only services are documented. You do not get both services and drivers like you did with netsvc.exe. Also, the command does not work over the network. You must run net start at a command prompt on the machine you wish to query. Needless to say you should use netsvc.exe unless you are in a pinch.



## Baseline Users & Groups

- addusers.exe can be used to document all users and groups

```
addusers \\SERVER /d usr_grp.txt
```

```
[User]
```

```
Administrator,,Built-in account,,,,  
cbren,Chris Brenton,,,,,web.bat
```

```
[Global]
```

```
Domain Admins,Designated administrators of the  
domain,Administrator,cbren
```

*Auditing WinNT - SANS' LevelOne*

25

Baseline users and groups. As I mentioned, you also want to document user and group accounts. One of the more difficult features with NT is the ability to have a system recognize both local and global accounts. This means that even if you religiously monitor domain accounts, an attacker could create a local account on a machine in order to allow them to gain remote access. Of course the difference is that while a global account can potentially provide access to every system on the network, a local account only provides access to that one machine. We still however want to make sure all of our accounts remain secure.

The resource kit includes a utility called addusers.exe. This tool can be used to list user and group account information as well as make changes. What's cool about this tool is that both local and global accounts are documented at the same time. If the system is a PDC or BDC both sets of accounts can be retrieved with a single command. The information returned includes everything from group membership to profiles to logon scripts. This means we can create a pretty good baseline of the user's network environment in order to monitor it for any changes.

## Additional Tools

---

- findgrp.exe - Show all local and domain groups for a user
- global.exe - Show all members of a specified domain group
- local.exe - Show all members of a specified local group

Additional tools. The NT resource kit includes a number of other tools for querying user and group information. While not as complete as the addusers command, they may be helpful if you identify a potential problem and need to hone in on additional information.

## Using Net.exe

---

- The "net" command can be used to collect user & group info
- Not as complete as addusers and does not show local users

```
net user > users.txt
```

```
net group > domgrp.txt
```

```
net localgroup > lclgrp.txt
```

Using Net.exe. So what if you need to query user and group information but do not have access to the resource kit. In the case the net command has a few useful switches you can use. Our two caveats here is that again the net command must be run directly on the system you wish to query. Also, you can not list local user accounts using net.exe.

# Sysdiff

- sysdiff was created to help Admins auto-install software
- It takes a snapshot of the registry & file system for later comparison
- This comparison “feature” can be used to check the registry and file system for changes

Sysdiff. Sysdiff is a tool which was created to help system admins automate the install process of software. What sysdiff does is take a snap shot of the registry and file system. You then install the software and run sysdiff again in order to identify the changes made to the system by the software install process. If you are trying to automate your installs, you can then create scripts to copy files into their correct locations as well as make registry changes to the target system.

For the purpose of auditing, we are only interested in sysdiff's ability to snapshot the system, and then to report any changes that have been made.

## Before running sysdiff

- Download the latest version  
ftp://ftp.microsoft.com/bussys/winnt/winnt-public  
/fixes/usa/NT40/utilities/Sysdiff-fix
- Determine what should be checked
  - Check C:\WINNT only?
  - exclude \*.tmp files
    - open files will cause sysdiff to abort

Before running sysdiff, you should download the latest version from the Microsoft FTP site. Incidentally, many of the resource kit tools have been updated so you may wish to check the utility directory for any other tools you will be using. You will then want to think about which directories and files you wish to include in your baseline. For example you will at least want to skip temp files because if sysdiff runs across an open file it will terminate. Excluding files that you know will be open during your audits will ensure that sysdiff is able to grab a complete image.

## Editing sysdiff.inf

```
[ExcludeDrives]
d
[ExcludeDirectoryTrees]
*:\recycler
[ExcludeFiles]
*:\pagefile.sys
*.tmp
*.log
```

Editing sysdiff.inf. Once you know which directories and registry keys you wish to record, edit the sysdiff.inf file. You can use the same sysdiff.inf file for multiple systems so long as you will be checking the same locations on each. The file contains a lot of good commentary so even if you plan on using the file as is, you should take a quick read through it.

## Comparing with sysdiff

---

- Create a baseline  
`sysdiff /snap baseline.img`
- Check the current system against the original image  
`sysdiff /diff baseline.img diff.img`
- Output changes in human form  
`sysdiff /dump diff.img diff.txt`

Comparing with sysdiff. Using sysdiff to audit your system is a three step process. First, run sysdiff with the “snap” switch to create your initial baseline. When you perform your later audits, run sysdiff again using the “diff” switch to compare the current system setup to the original baseline file. You will then need to run sysdiff using the “dump” switch in order to produce a diff file that is in readable format.

## Sample sysdiff Output

```
; Dump of sysdiff package diff.img  
; Sysroot: C:\WINNT  
; TotalDiffCount: 5
```

```
C:\WINNT\system32  
  Add/change hackme.exe
```

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa  
  RestrictAnonymous: REG_DWORD 0x310a10
```

If you look at the next slide titled “Sample sysdiff output”, you will see that sysdiff found 5 changes made to the system since the initial baseline was created. Two of these changes are shown in the sample output. The first is the addition of the file hackme.exe and the second is a registry key change which normally prevents anonymous users from enumerating server information. Obviously we would now want to go back and figure out where that file came from as well as why this particular registry key was changed.



## Baseline Just The Registry

---

- Use regdmp.exe to create an ASCII version of the registry
- Remember that it is normal for key values to change
- Run a couple of baselines to determine what is "normal"

```
regdmp -m \\SERVER > regfile.txt
```

Baseline just the registry. Even though sysdiff will report any registry key changes, its still a good idea to have a dump of your registry in raw text format in case you need to identify the original value of any key settings. This can be performed using the regdmp.exe utility. regdmp is another networkable tool so you can use it to query remote systems. Since it normally sends its output to the screen, you will need to redirect the data to a file. Remember that the registry can grow to be quite large so don't be surprised if it takes a while for this tool to run. Also make sure that you have plenty of free disk space before creating the output file.

## Probing The File System

- xcacls.exe allows you to check ACL for one or more files

```
xcacls c:\winnt\system32\hackme.exe
```

```
c:\winnt\system32\hackme.exe
BUILTIN\Administrators:F
    Everyone:C
    BUILTIN\Administrators:F
    NT AUTHORITY\SYSTEM:F
```

*Auditing WinNT - SANS' LevelOne*

34

Probing the file system. In the course of your audit or perhaps because you are investigating a potential intrusion, its nice to be able to quickly document the access control lists or ACLs associated with certain files or directories. The ACLs tells you who has permission to access specific files and what level of access has been granted. For example the file salaries.xls should probably not be accessible by everyone on the system.

Many times a savvy attacker will realize that elevating their privileges to that of a Administrator equivalent will set off certain alarms. Certainly its not all that difficult to check out the Domain Admins group to see who is a member. With this in mind they will opt for changing the ACL on critical files in order to give them access to the system through more subversive means. So if our file salaries.xls has an ACL which shows that the HR department has change permissions while the account bsowers who is not an HR person has been granted full control, this should send up a warning flare.

## Checking User ACL to Files

- Perms.exe allows you to check ACL of a specific user

```
perms domain\user c:\winnt\*.exe
```

```
#RWXDPOA c:\wtsrv\clspack.exe
```

```
#RWXDPOA c:\wtsrv\dooflop.exe
```

```
#RWXDPOA c:\wtsrv\explorer.exe
```

```
#RWXDPOA c:\wtsrv\EXTRAC32.EXE
```

```
#RWXDPOA c:\wtsrv\EXTRACT.EXE
```

*Auditing WinNT - SANS' LevelOne*

35

Checking user ACL to files. So lets say we identify that bsowers has ACL rights to a file or two which they should not and we wish to asses the extent of their access. We could then switch to the perms.exe utility which allows to specify a specific user but query multiple files. This will allow us to figure out in short order what level of access bsowers has achieved.

Remember that xcal.exe and perms.exe are complimentary. Use xcal when you need to query a single file for the access level of multiple users. Conversely, use perms when you need to query multiple files for the access level of a single user.

## Checking file stamps

- The DIR command can be used to check size and date/time
- A good attacker can change this information to hide their files!
- To check creation date/time and size of all EXE files:

```
dir c:\winnt\*.exe /s/t:c > exefiles.txt
```

Checking file stamps. The dir command can be used to query one or more files as to their creation or last access time. This information can be useful for nailing down what an attacker has done to a system during a given session. Remember that we said that file times can be changed. This makes the information reported by DIR as being questionable at best. While the information can not be completely trusted, its still worth the exercise in case our attacker slipped up.

The example at the bottom of the screen is using the /t:c switch which will report the date and time stamp of when the file was created. You can substitute the "c" for a "w" to see the last time the file was written to or "a" to see the last access time.

## Additional Useful Tools

---

- dommon.exe - Display all "trusted" domains (GUI)
- rasusers.exe - List all users granted dial-in access
- raslist.exe - List all RAS servers in the domain

The next slide, additional useful tools, shows a number of additional commands you can run as part of your regular audit depending on your network configuration. If you are using trust relationships between domains, the dommon.exe utility provides a quick way to verify these relationships. Note that this is a GUI utility so you will not be able to direct its output to a file.

The rasusers and raslist utilities can be used to document users who have been granted remote access to the network via RAS, as well as which machines are running RAS services. If you are providing remote access to your network, it is extremely important that you keep an eye on who has access to your network and through what means. During an audit I once identified a rouge server that was providing RAS services. Upon investigation, it turned out that the owner of this system was using the box to run their own little ISP service. Besides being a misuse of company property, this activity was also a very large security threat.

## Checking your systems

---

- Use your baselines to verify system integrity during future audits
- Your security policy should define how often audits are performed
- Your security policy should define how long audit data is retained
- Make sure your tools stay secure!

Checking your system. Ok, we have covered many of the useful tools that are available for baselining your systems. Its now time to put that information to good use and turn it into a full fledged audit. Remember that your audit procedure should document all of the checks that are to be performed during each audit, as well as the frequency that audits should take place. Don't forget to take precautions to keep all of your auditing tools secure. You can not trust the integrity of the data if you can not trust the integrity of your tools.

## Data Comparisons

- |   |   |
|---|---|
| <ul style="list-style-type: none"><li>• Use raw data<ul style="list-style-type: none"><li>– Event Viewer log</li><li>– All other logs</li></ul></li></ul> | <ul style="list-style-type: none"><li>• Baseline check<ul style="list-style-type: none"><li>– Open ports</li><li>– Running services</li><li>– Loaded drivers</li><li>– Users &amp; Groups</li><li>– Registry entries</li><li>– System files</li></ul></li></ul> |
|---|---|

Data comparison. When performing your audits, some of your data will be evaluated based on its raw content and some of the data will need to be verified against your baselines. For example when you are auditing a system and run the netstat command to check open ports, you will be taking this data and comparing it to the original system baseline. It's this comparison between the original baseline and your current audit that will tell you if any new listening ports have been opened up. Something like your IIS logs however will be evaluated based on solely on their current content because log entries can not be baselined.

So your log checks are pretty straight forward in that you need to go through them line by line. If you are using sysdiff, you are all set on your baseline comparison as this functionality is built right into the utility itself. What we need is an easy way to compare data from all of the utilities like netstat, netsvc and addusers that creates raw text files.

## Comparing ASCII files

- Compare baseline file to audit file
  - The fc.exe utility can be used to compare file contents
  - Useful switches
    - /C - Disregard case
    - /N - Display line numbers
- ```
fc -N c:\path\file1.txt c:\path2\file2.txt > diff.txt
```

Comparing ASCII files. Stock Windows includes a utility called fc.exe which can be used for comparing the contents of two files. This is much more efficient than trying to visually verify if two files are the same. Fc is cool because you can have the utility flag the differences between your baseline and your audit file so that all you need to check out is this diff file.

The bottom of the slide shows an example of how to use fc. Note that fc is comparing the contents of file1.txt and file2.txt and then generating a third file called diff.txt. All we need to do now is visually check diff.txt to see if there have been any changes since our baseline was created. A couple of useful switches are /C which tells fc to ignore alphabetic case when performing a comparison. The /N switch is cool because it adds reference line numbers to the diff file. If you are comparing two large files, /N can be extremely valuable in case you wish to manually check the files in order to verify the difference that fc has flagged.



## Spotting new ports

```
fc -N baseline-ports.txt z:\07-24-99-ports.txt
Comparing files baseline-ports.txt and 07-24-99-ports.txt
**** baseline-port.txt
   5:  TCP  skylar:ftp      0.0.0.0:0      LISTENING
   6:  TCP  skylar:80         0.0.0.0:0      LISTENING
**** 07-24-99-PORT.TXT
   5:  TCP  skylar:ftp      0.0.0.0:0      LISTENING
   6:  TCP  skylar:telnet   0.0.0.0:0      LISTENING
   7:  TCP  skylar:80         0.0.0.0:0      LISTENING
****
```

The next slide, Spotting new ports shows an example of `fc` in action. We are comparing the contents of two files, both of which have been created with the `netstat -a` command. One file is our original baseline while the other is a recent audit. Check out the output created by `fc`. `fc` is telling us that it has found a difference between the two files. In the baseline file, line 5 showed the FTP port as being open while line 6 showed port 80 or the HTTP port as being open.

Now, look at the contents of our audit file. There is a new service listening on the Telnet port. If we have no record of a Telnet server being sanctioned for this system, this entry should throw up a flag. While we should be concerned, it's not time to panic quite yet. Remember we said that you should always verify your findings through some other means.

So how do we verify that we have a new port open on our machine? Let's think about it logically. In order for the port to be open, there must be some application listening at this port. In other words, if we find a new service running on this machine as well, this would be a pretty good indication that a problem exists. With this in mind, let's go on to the next slide entitled "Finding new services and again use `fc` to perform a comparison.

## Finding new services

```
fc -N bl-services.txt z:\07-24-99-services.txt
Comparing files bl-services.txt and 07-24-99-services.txt
**** baseline-services.txt
153:  <Tcpip>, Display name is <TCP/IP Service>
154:  <tga>, No separate display name
**** 07-24-99-SERVICES.TXT
153:  <Tcpip>, Display name is <TCP/IP Service>
154:  <Telnetd>, Display name is <Telnetd (Inbound Telnet)>
155:  <tga>, No separate display name
****
```

This time we are using `fc` to compare the output generated by `netsh`. Again we are comparing the baseline file to a file created during a recent audit. If you review the output, you'll see that `telnetd` has been loaded on this machine. This certainly explains why the Telnet port is being held open. We would now need to do a bit of investigation work to determine who loaded `telnetd` on this system and why.

## Automating your audits

---

- Most tools run over the network
- For large environments, dedicate a “secured” workstation for auditing
- Most checks can be run via batch file though “AT”
- Program AT from the command line or use the resource kit GUI (winat)

Automating your audits. I'm sure by now your thinking “wow, auditing is a lot of work”. There are actually quite a few things you can do to automate the entire process. Remember that most of these tools will run over the network. This means you can run the commands via batch file from a single machine and query all of the systems on your network. In fact, you do not even have to manually run the batch files. If the audit system is NT simply use the AT command to schedule your batch files to run during off hours. Of course this breaks our “stagger the times you perform your audits” rule, but you are better of running scheduled audits than no audits at all.

While it would be nice to use a dedicated machine as your audit system, this is not always possible due to budget constraints. You can use your own Windows NT desktop so long as you take precautions to lock the system down. Again, dedicated is better but don't be afraid to use the tools that you have.

## Using AT

- Make sure the Scheduler service is running on the audit workstation
- Setup AT to run audits via batch

```
AT \\LOCAL 3:55 /every:monday "d:\tools\auditme.bat"
```

Using AT. The AT command requires that your system be running the scheduler service. Do a Start, Settings, Control Panel, Services to verify that it is running. If not, start the service and set it to automatically start at system boot time. The bottom of the slide shows an example at command. This command launches the file named auditme.bat on the machine named "local" every Monday at 3:55 AM. If you have your batch file run your file comparisons as well as the actual audit, when you come in Monday morning all you have to do is review the diff files that have been created.

## Sample commands

```
REM Get a dump of the security log
d:\tools\dumpel -L security -f c:\audits\server1\logon.txt
-s SERVER1 -c

REM Get a list of running services
d:\tools\netsvc \\server1 /list >
c:\audits\server1\services.txt

REM Check for new services
d:\tools\fc d:\server1\baseline-services.txt
c:\audits\server1\services.txt >
c:\audits\server1\diff-serv.txt
```

The slide titled “sample commands” shows a few possibilities for your batch files. Note that the command lines are pretty long so they have wrapped over multiple lines on the slide. Basically all lines following the REM statements should appear on a single line within your batch files.

In the first command we are running the dumpel command located on the “D” driver which is our CD ROM. We are pulling over the security log from the server SERVER1 and then storing it in a local directory we have dedicated to our audit files. Our second command queries SERVER1 for a list of running services and drivers and writes it to a local file. Our third command takes this local file and compares it to the original baseline. Again, if we run this batch file via AT, when we come in the following morning we can get straight to it by checking the diff-serv file to see if there are any new services we need to worry about.

## What if you find something?

- Don't panic!
- Verify your results
- Identify how they got in
  - Insider, IIS, password cracking
- Perform corrective action
- Document everything

What if you find something? So what should you do if you find a possible intrusion? As I mentioned the first thing to do is keep a clear head and go back and verify your results. Remember we are talking about computers so burps do happen. Verify that you actually have a real problem.

Next you want to determine how the attacker got in. I know many of you may be thinking "hey wait a minute, shouldn't I try to kick them out first?". Think of it this way, if you can not figure out how the attacker got in in the first place your going to end up chasing your tail. Sure you can start throwing patches at the machine, but this is a hit or miss proposition at best. You can pull the system off of the wire, but now you have a server off-line and who's to say the attacker will not simply move on to the next server in your network and gain access with the same exploit.

Obviously there may be certain situation where you can not wait. For example if the attacker is currently using your machine to launch attacks against other machines, you will want to bring it down ASAP.

So if you can, first figure out how the attacker got in. Armed with this knowledge you are then in a much better place to make sure that they can not come back. You can then take your time assessing the damage to determine what you next best course of corrective action should be. Above all, document everything. This will allow you to go back and perform a later sanity check to ensure you did not miss anything.

## Summary

---

- There are no magic security bullets
- Auditing enhances your existing security posture
- Can help to minimize the amount of damage done by an attacker
- Great motivation for learning the nuances of your systems

So in summary, there are no magic bullets in security. You need to layer your security posture to ensure that if any one of your security defenses are breached, another is there to pick up the slack. Treat your data as kings within a castle; with high walls, a nice big moat, and lots of armed guards. Use auditing as a method of not only securing your systems, but to learn more about their daily activity as well. There is no better security tool than an Administrator who knows their environment.

Thanks for your time, and I hope you have found this course to be helpful.