Global Information Assurance Certification Paper

TABLE OF CONTENTS

Scope

This document will cover some aspects of group, account type and account tracking auditing on a Microsoft Windows NT 4.0 Server with a minimum service pack level of 4 in the context of identifying internal and external hacking attempts.

Disclaimer

This document is not intended to be a comprehensive review of auditing NT 4.0 servers. This document assumes the reader has (at least) basic knowledge of Windows NT administration.

Purpose

The purpose of this document is to comply with the GIAC NT Curriculum Practical Assignments for SANS Security DC 2000 Version 1.2 Option 1 requirements.

Definitions

Auditing

Merriam-Webster[1]

Main Entry: 1au·dit
Pronunciation: 'o-d&t
Function: noun
Etymology: Middle English, from Latin auditus act of hearing, from audire
Date: 15th century
1 a : a formal examination of an organization's or individual's accounts or financial situation b : the final report of an audit
2 : a methodical examination and review
- au·dit·able /-di-t&-b&l/ adjective

Microsoft[2]

auditing

Tracking activities of users by recording selected types of events in the security log of a server or a workstation.

Why auditing is important

1. Auditing represents a piece of the overall security blanket for a network.
2. Auditing is one way to detect intruders.
3. Auditing can expose weaknesses in your system and allow you better secure those systems.[3]
4. Auditing provides a mechanism to track changes made to the system.

Background

Each Windows NT system has its own audit logs, which are viewed through Event Viewer. However, a moderately busy network will generate tremendous volumes of audit data. This leads to two distinct problems.

1. A significant performance penalty will be incurred on servers where indiscriminate auditing is performed.[4]
2. The volume of data that is generated is problematic to review.

Auditing at the level described by Figure 1 later in this document is not recommended unless:

1. The Primary Domain Controller is overpowered compared to the performance needed before auditing is enabled.
2. There is sufficient staff dedicated to the review of all the data gathered by auditing and can act upon any items that need attention

This document assumes that condition 1 and 2 above have been met.

Before you begin

Ensure that you have a valid tested backup.

Dumpel.exe and now.exe from the Microsoft Resource kit (supplement 4) are needed if the techniques in this document are to be used. An explanation of dumpel switches, echo set and now.exe can be found in Appendix A

A description of Security Log Event IDs can be found in Microsoft KB article 174074[5]

Dealing with the data

Before a discussion of physical auditing techniques can occur, a few words on the techniques of interpreting and the handling of the audit data that is logged are in order.

1. Communication is the key. This can not be emphasized enough. Communication with other staff members will allow you to determine what questionable events are legitimate and what events are indications of hacking attempts.
2. Look for patterns. Many hacking activities will leave a tell tale signature. For example, if someone were to deduce the account naming convention (say from an e-mail or company directory), they could attempt to log on several times to each account before they (hopefully) locked out the account. When in doubt, see item #1
3. If you don't know your users, get to know them. If you know that a particular user frequently has bouts of amnesia and forgets their password, you will be less concerned about the frequent multiple (failed) logon attempts at 9:02 am when that user starts their shift. When in doubt, see item #1.

4. Question everything. If something looks wrong or feels wrong, examine it thoroughly until you are satisfied that you know what is happening. When in doubt, see item #1
5. It is perfectly acceptable (if not warranted) to seem paranoid while reviewing auditing data (See #4 above). However do NOT jump to conclusions. Ensure that you have a complete picture of what is happening (perhaps by reviewing the raw event log(s), questioning users and or staff) before you do anything.
6. Save each day's logs in a secure location that will get backed up every night.

Things that should raise immediate concern if you (THE administrator) did not initiate:

1. Event log entries at unusual times. If you see a logon entry at 4:00 am for a user who works days, has no dial in access, has no physical access to his or the system after hours, it's a pretty good indication that something is amiss.
2. Changes made to the Domain Admins group
3. Changes made to the local Administrators group
4. Changes made to any account that is a member of the Domain Admins or local Administrators group
5. Changes to global group membership
6. Changes to local group membership
7. Changes made to any account where rights are assigned or removed
8. Addition or deletion of accounts
9. Password changes or account lockouts for any privileged account.
10. Changes in the Domain or Auditing policy
11. Reboots

When in doubt – communicate.

Auditing – Step by Step

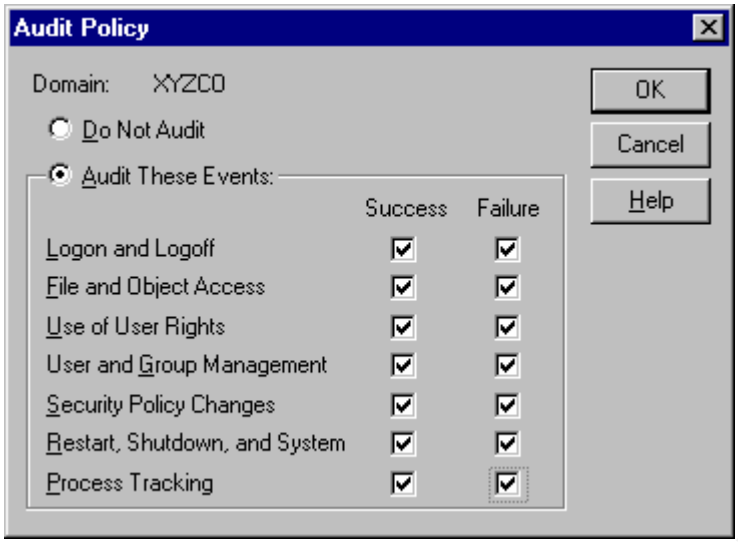
Step 1 Enable and configure auditing

The first step is to have auditing turned on at the PDC

Perform the following steps.[6]

1. Log on with administrative authority
2. Start User Manager for Domains
3. Select Policies, Audit, and the Audit These Events Check box
4. Choose all items and audit for success and failure.

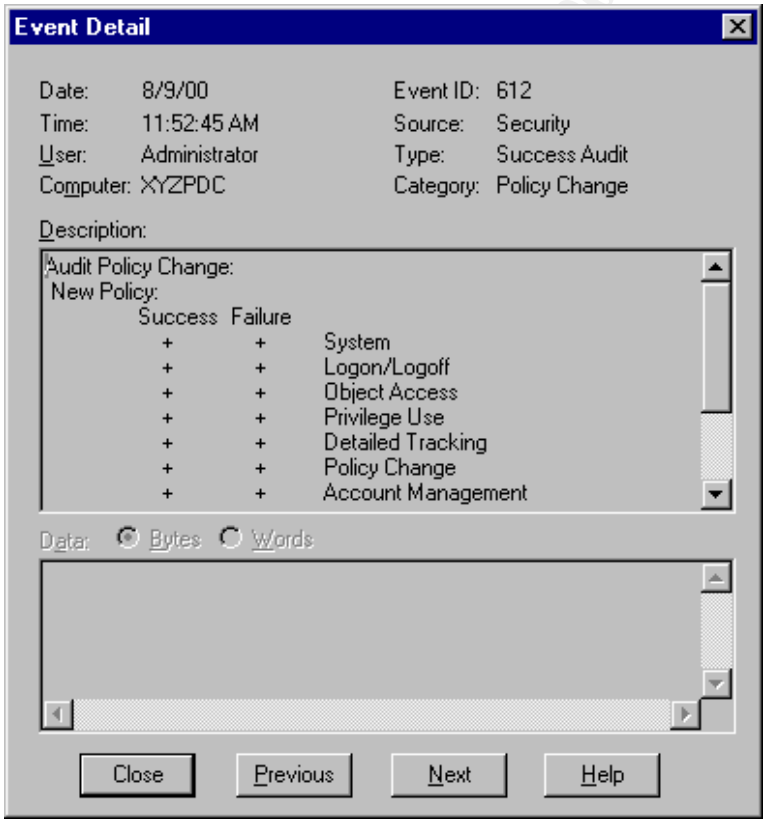
(Figure 1 – Auditing configured)



5. Click OK and auditing is enabled.

Open up the Security Log in the event viewer and confirm that auditing is enabled.

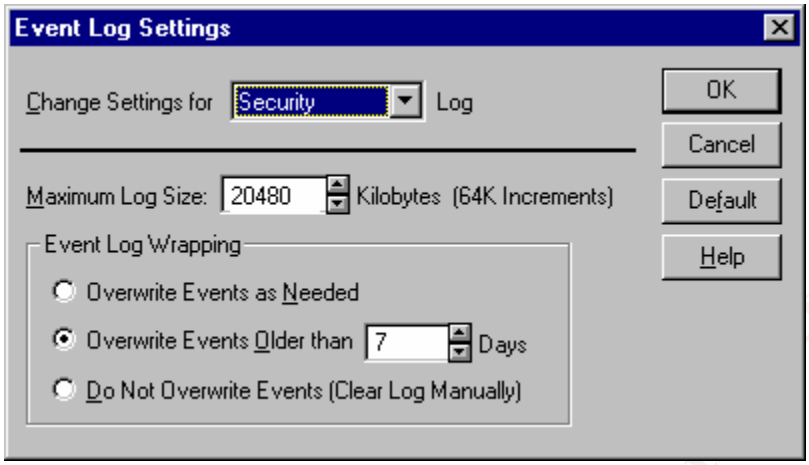
(Figure 2 – Auditing confirmed)



Step 2 Configure audit logs

While still in Security Log, go to Log, Event Log Settings and change the security log to a maximum log size of 20480 (20 MB) such that it looks like this.

(Figure 3 – Security Event Log Settings)



Step 3 Verify what you have is correct

First, verify that members of the current global groups are correct. Save this as a baseline and compare with and or modified against future changes. Next, verify local groups on the domain controller have the correct membership. Save this info as a baseline and will be compared with and or modified against future changes. Continue on with users that have advanced rights/special privileges. Compare these lists with any changes that are made and update the baseline list as needed. Be sure to keep the baseline lists is a secure area that is part of the normal nightly backup. Hard copy in a locked file cabinet with very limited access is a good backup.

Step 4 Set up your filesystem

Create a directory structure on the second partition (D:\) named scripts\audit\output. In the audit directory, place the following script that uses dumpel.exe to check the PDC for changes in Global Groups. Also place a copy of dumpel.exe and now.exe from the resource kit.

Open notepad and type "@echo off" save the file with a .bat or ..cmd

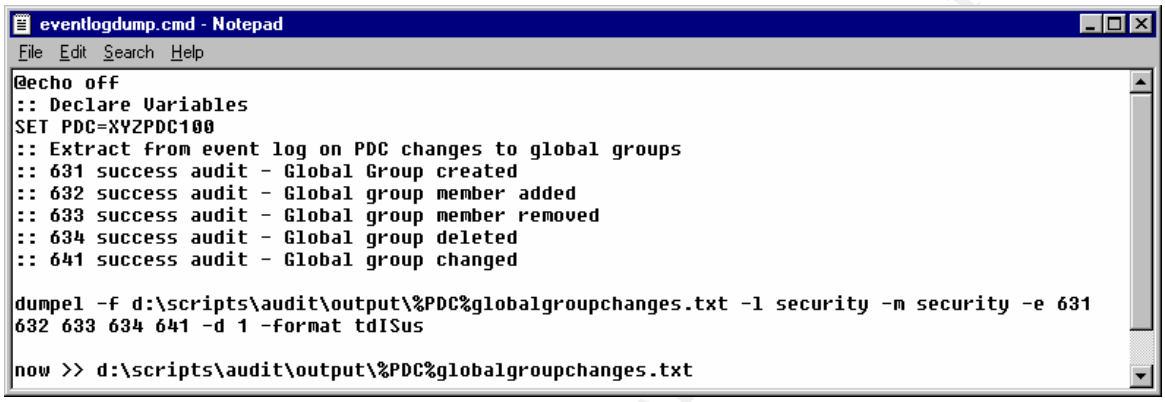
Step 5 Check for changes to global groups

The main purpose for this is to track changes made to the Domain Admins group. However, a secondary benefit is to allow inspection of all global group changes made by Account Operators. This would, in conjunction with communication with the (legitimate) Account Operators let you know when unauthorized changes were made to any global group

Things to look for specifically:

1. Additions to or deletions from the Domain Admins group
2. Additions to or deletions from any group that directly or indirectly has permission to sensitive corporate material, i.e. financial information, Human Resources…
3. Additions to or deletions from any group related to your corporate or local MIS/IS/IT department.

(Figure 4 – Global group changes)



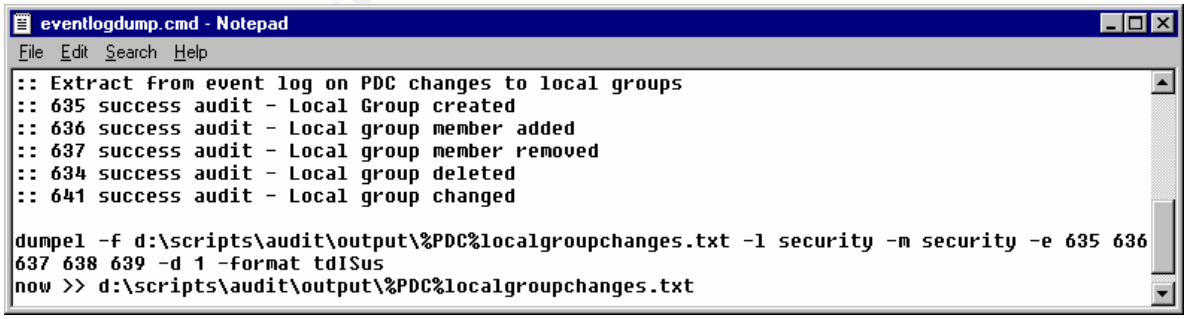
Step 6 Check for changes in local groups)

The next addition to the script is designed to detect changes in the local groups

The following are events to look for specifically

1. Additions to or deletions from the Administrators group
2. Additions to or deletions from the Server Operator group
3. Additions to or deletions from the Account Operators group
4. Additions to or deletions from the Backup Operators group

(Figure 5 Local group changes)

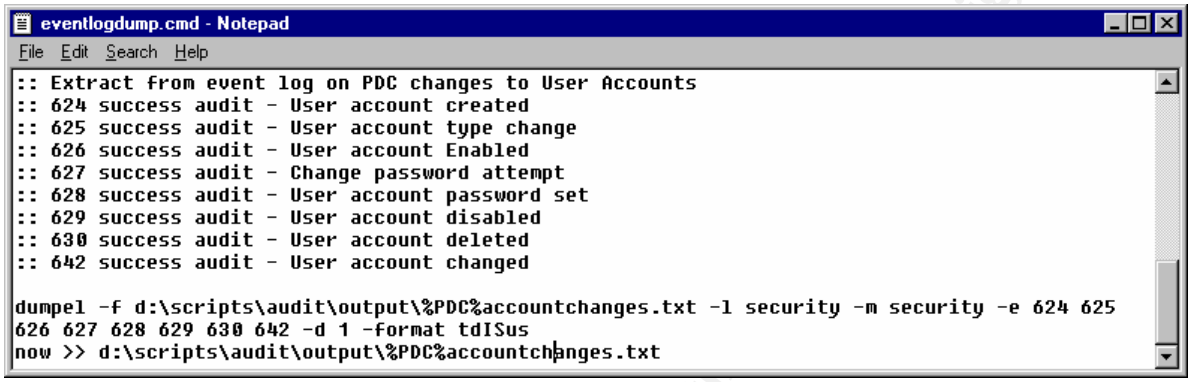


Step 7 Check for changes to user accounts

The next section checks for changes to user accounts. NT security is based on accounts and authentication. For a would be attacker, obtaining an account (especially an administrative level account) and authenticating with it in some manner, is crucial to further compromising the system.

A good practice to get into is to make sure that the account operators do not create, disable or otherwise modify any accounts or groups before or after normal business hours. This way, the new account with membership in the finance and human resources group that got created at 3:18 am sticks out like a sore thumb.

(Figure 6 User account changes)



Things to look for specifically:

1. Creation of accounts – immediately check global and local group scripts to see which group(s) the account was added to.
2. Deletion or disabling of accounts – if the service account that your anti-virus software runs on is disabled, it is all the easier to send a trojan horse in an e-mail.
3. Change password attempts – is someone attempting to lock a user out of their account because they were able to plant a keystroke recorder on their system and wanted to capture their password?
4. Password changes and attempts – It is a rare user that takes the initiative to change their password without being told (or forced) to.

Again, communication with other staff members (and possibly the users) is crucial in determining which events are legitimate and which may signal a hacking attempt

Step 8 Check for high level events

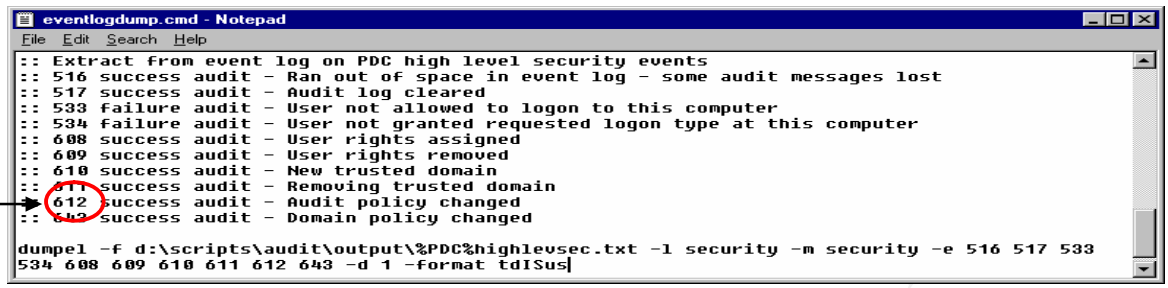
The next line(s) in the script pull high-level security events from the event log.

Look for:

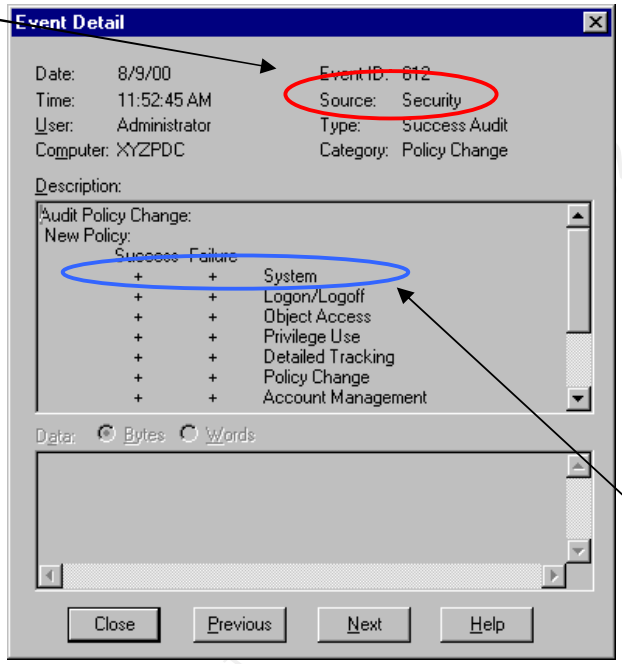
1. Audit log cleared – a sign of an intruder attempting to cover tracks.
2. Audit log ran out of space – a sign of an intruder attempting to cover tracks.
3. User rights assigned – why did that user in sales suddenly gain the right to force a shutdown from a remote system?
4. User not allowed to logon – did someone with a normal user account attempt to logon to a server?
5. New trusted domain – I always build new domains at 5:00 am and set up the trust relationships, don't you?

.

(Figure 7 High level events)

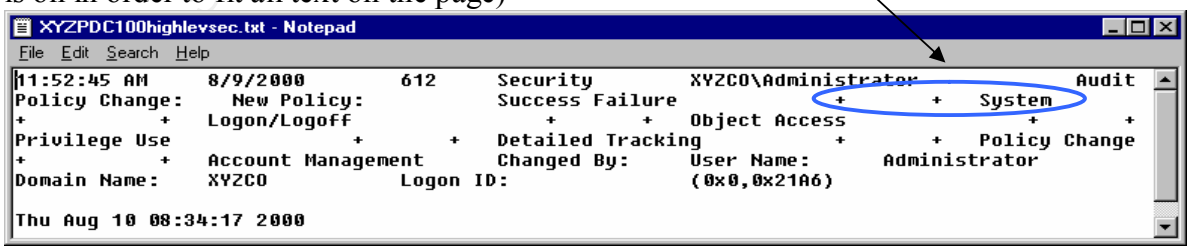


This is where you would find out if the security log overflowed or was cleared, if users are attempting to log onto restricted computers, if rights are assigned or removed, change in trust relationships with other domains and if the domain or audit policies have changed. Note that Figure 8 shows the change in audit policy.



(Figure 8 Audit policy change in Event Log and script)

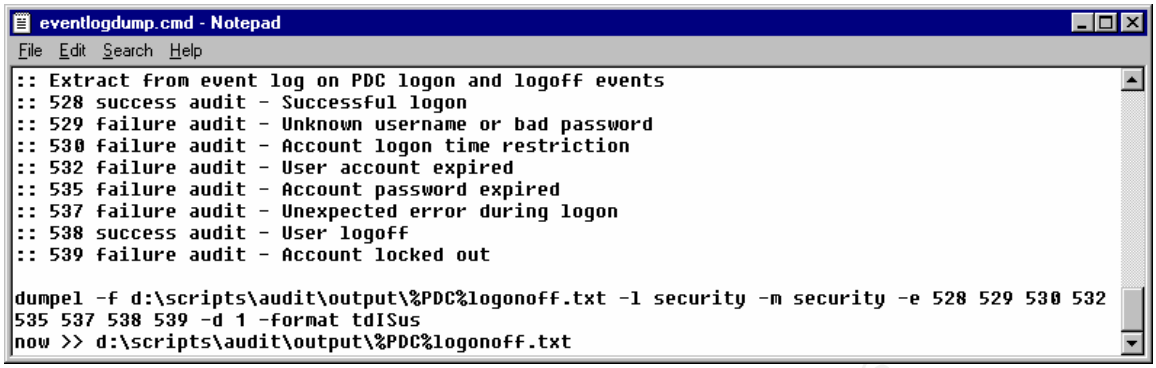
The corresponding entry in the log file (d:\scripts\audit\output\%PDC%highlevsec.txt would be as follows. (Note that word wrap is on in order to fit all text on the page)



Step 9 Check for logon and logoff events

The next section looks for logon and logoff events.

(Figure 9 Logon and logoff events)



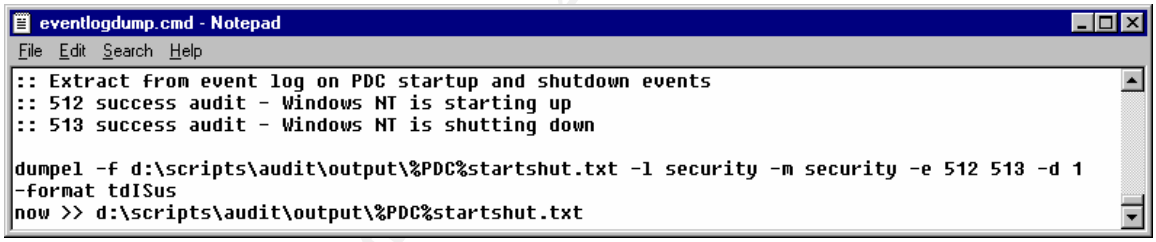
From this log you can see who is logging on and off (and at what times), logon attempts from locked accounts and other entries that could signal an attempted break-in such as:

1. Logon attempts from unknown users with the username they offered
2. Logon attempts from expired accounts – possibly former temp employees

Step 10 Check for startup and shutdown events

The last section of the script checks for startup and shutdown events.

(Figure 10 Startup and shutdown events)



Whether your servers are on a reboot schedule or not, you will know when they are rebooted. Additional listings are a possible indication of:

1. DOS attack
2. Trojan was placement on the box.
3. System crash on audit fail (if enabled) from a large amount of (attack generated) event log entries

The complete text of this script is available in Appendix B.

Summary

Auditing is important for several reasons, not the least of which is that proper auditing and reviewing of the audit information can allow you to detect intrusions.

Audited events in Windows NT 4.0 are logged to the Event Log.

The physical act of auditing an NT server is relatively simple to complete. Enable auditing, select what you wish to audit and sit back and collect the data.

What you do with the data is the key issue.

Indiscriminate auditing can lead to performance problems as well as make it easier for a key piece of data to get overlooked.

When scripting, it is helpful to create log files with similar data in the same file. For example, Figure 4 shows that all the information we want to see regarding global groups is contained in one log file, while Figure 5 shows that all information regarding local groups is in another.

This allows for smaller files and makes it less likely that a key piece of data will get lost in the enormity of the file. A busy domain with relatively few users can easily create large log files that are cumbersome to work with.

Review of the audited data and action on items that need attention can be a time consuming, meticulous process.

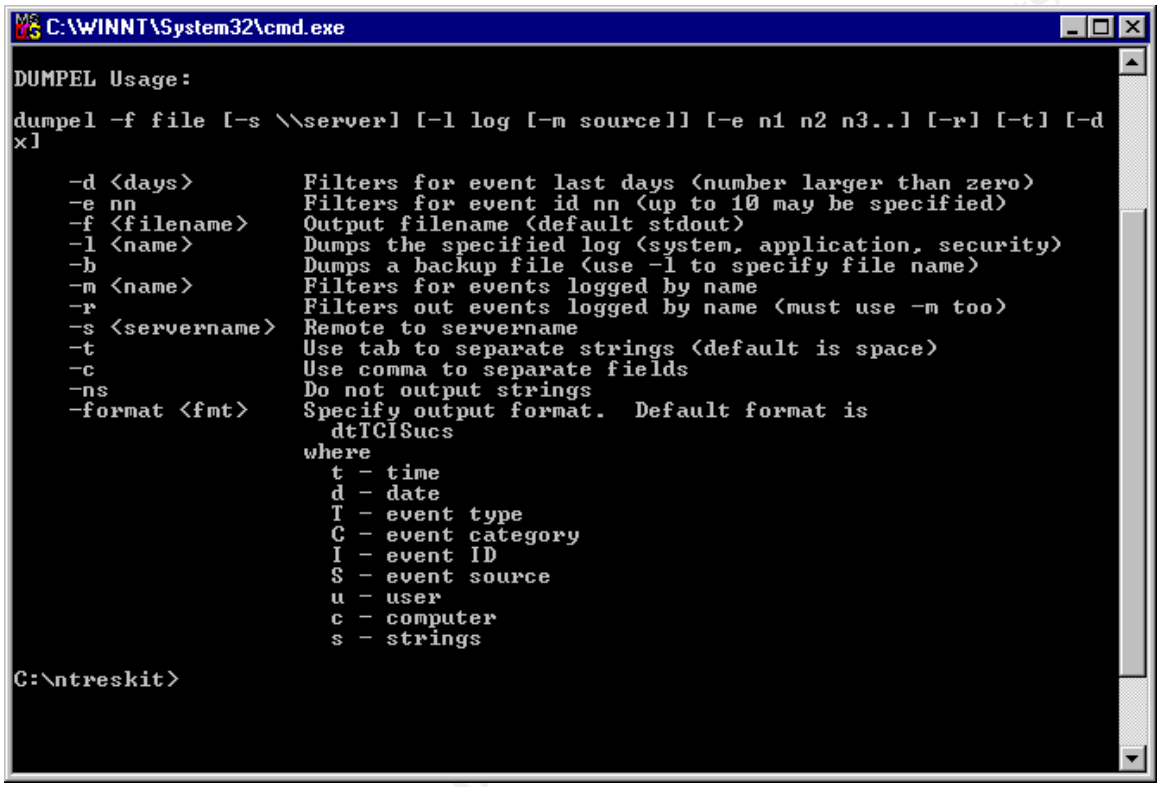
Watch for any and all changes to members of administrative groups (Domain Admin, local Administrator, Account Operator…)

Talk to your users; talk to the other staff. A failed logon attempt at 4:00am may be an attacker who found your RAS server, or it may be a legitimate user with insomnia. That entry for an unscheduled reboot might be a DOS attack, and it may be that the server had a "normal" BSOD.

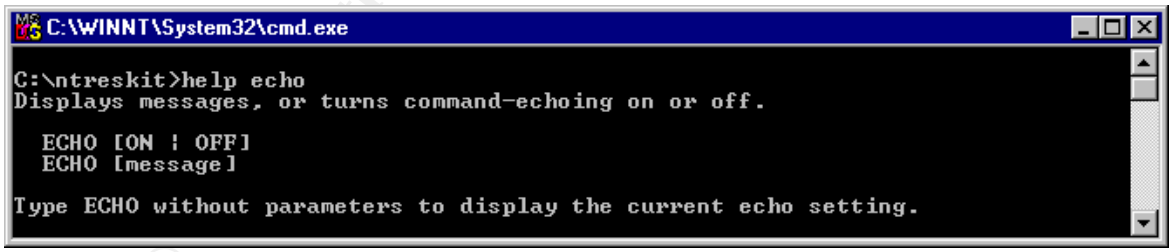
Question everything. Act paranoid but do not act on that paranoia until you have all the information you can.

Appendix A Command Reference

Dumpel.exe



echo



set

Displays, sets, or removes cmd.exe environment variables.

SET [variable=[string]]

variable Specifies the environment-variable name.

string Specifies a series of characters to assign to the variable.

Type SET without parameters to display the current environment variables.

If Command Extensions are enabled SET changes as follows:

SET command invoked with just a variable name, no equal sign or value will display the value of all variables whose prefix matches the name given to the SET command. For example:

```
SET P
```

would display all variables that begin with the letter 'P'

SET command will set the ERRORLEVEL to 1 if the variable name is not found in the current environment.

SET command will allow an equal sign (=) in the value of an environment variable in any position other than the first character.

A new switch is added to the SET command:

```
SET /A expression
```

The /A switch specifies that the string to the right of the equal sign is a numerical expression that is evaluated. The expression evaluator is pretty simple and supports the following operations, in decreasing order of precedence:

```
()              - grouping
* / %           - arithmetic operators
+ -             - arithmetic operators
<< >>           - logical shift
&               - bitwise and
^               - bitwise exclusive or
|               - bitwise or
= *= /= %= += -=    - assignment
  &= ^= |= <<= >>=
,               - expression separator
```

If you use any of the logical or modulus operators, you will need to enclose the expression string in quotes. Any non-numeric strings in the expression are treated as environment variable names whose values are converted to numbers before using them. If an environment variable name is specified but is not defined in the current environment, then a value of zero is used. This allows you to do arithmetic with environment variable values without having to type all those % signs to get their values. If SET /A is executed from the command line outside of a command script, then it

displays the final value of the expression. The assignment operator requires an environment variable name to the left of the assignment operator. Numeric values are decimal numbers, unless prefixed by 0x for hexidecimal numbers, 0b for binary numbers and 0 for octals numbers. So 0x12 is the same as 0b10010 is the same as 022. Please note that the octal notation can be confusing: 08 and 09 are not valid numbers because 8 and 9 are not valid octal digits. Environment variable substitution has been enhanced as follows:

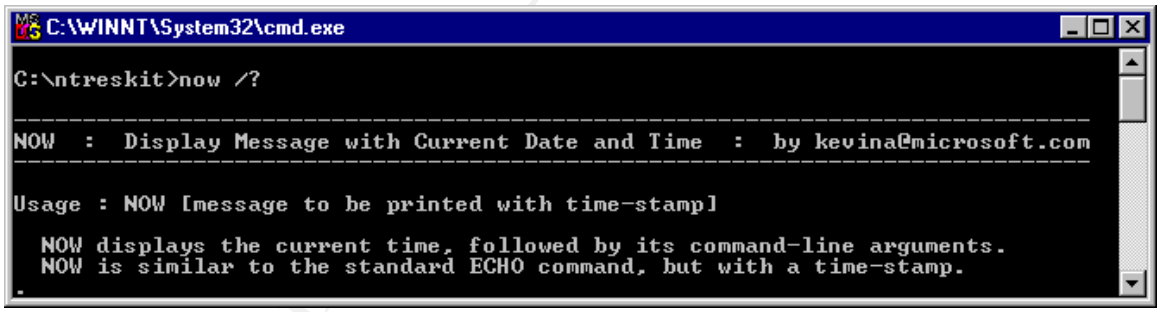
%PATH:str1=str2%

would expand the PATH environment variable, substituting each occurrence of "str1" in the expanded result with "str2". "str2" can be the empty string to effectively delete all occurrences of "str1" from the expanded output. "str1" can begin with an asterisk, in which case it will match everything from the begining of the expanded output to the first occurrence of the remaining portion of str1.

%PATH:~10,5%

would expand the PATH environment variable, and then use only the 5 characters that begin at the 11th (offset 10) character of the expanded result.

Now.exe



Appendix B – Script for extracting data from the Security Event Log

```
@echo off
:: Declare Variables
SET PDC=XYZPDC100
:: If you use this script, replace XYZPDC with the name of your PDC
:: This script is to be run locally on the PDC
:: See Appendix A for the switch that will allow it to be run remotely
:: If you will only monitor the output of this script Monday through Friday
:: change –d 1 in all lines to –d 3 (pull data for three days instead of 1)
:: for the script that you run on Monday

:: Extract from event log on PDC changes to global groups
:: 631 success audit - Global group created
:: 632 success audit - Global group member added
:: 633 success audit - Global group member removed
:: 634 success audit - Global group deleted
:: 641 success audit - Global group changed

dumpel -f d:\scripts\audit\output\%PDC%globalgroupchanges.txt -l security -m security -
e 631 632 633 634 641 -d 1 -format tdISus
now >> d:\scripts\audit\output\%PDC%globalgroupchanges.txt

:: Extract from event log on PDC changes to local groups
:: 635 success audit - Local group created
:: 636 success audit - Local group member added
:: 637 success audit - Local group member removed
:: 634 success audit - Local group deleted
:: 641 success audit - Local group changed

dumpel -f d:\scripts\audit\output\%PDC%localgroupchanges.txt -l security -m security -e
635 636 637 638 639 -d 1 -format tdISus
now >> d:\scripts\audit\output\%PDC%localgroupchanges.txt

:: Extract from event log on PDC changes to User Accounts
:: 624 success audit - User account created
:: 625 success audit - User account type change
:: 626 success audit - User account Enabled
:: 627 success audit - Change password attempt
:: 628 success audit - User account password set
:: 629 success audit - User account disabled
:: 630 success audit - User account deleted
:: 642 success audit - User account changed
```

```
dumpel -f d:\scripts\audit\output\%PDC%accountchanges.txt -l security -m security -e
624 625 626 627 628 629 630 642 -d 1 -format tdISus
now >> d:\scripts\audit\output\%PDC%accountchanges.txt


:: Extract from event log on PDC high level security events
:: 516 success audit - Ran out of space in event log - some audit messages lost
:: 517 success audit - Audit log cleared
:: 533 failure audit - User not allowed to logon to this computer
:: 534 failure audit - User not granted requested logon type at this computer
:: 608 success audit - User rights assigned
:: 609 success audit - User rights removed
:: 610 success audit - New trusted domain
:: 611 success audit - Removing trusted domain
:: 612 success audit - Audit policy changed
:: 643 success audit - Domain policy changed

dumpel -f d:\scripts\audit\output\%PDC%highlevsec.txt -l security -m security -e 516 517
533 534 608 609 610 611 612 643 -d 1 -format tdISus
now >> d:\scripts\audit\output\%PDC%highlevsec.txt

:: Extract from event log on PDC logon and logoff events
:: 528 success audit - Successful logon
:: 529 failure audit - Unknown username or bad password
:: 530 failure audit - Account logon time restriction
:: 532 failure audit - User account expired
:: 535 failure audit - Account password expired
:: 537 failure audit - Unexpected error during logon
:: 538 success audit - User logoff
:: 539 failure audit - Account locked out

dumpel -f d:\scripts\audit\output\%PDC%logonoff.txt -l security -m security -e 528 529
530 532 535 537 538 539 -d 1 -format tdISus
now >> d:\scripts\audit\output\%PDC%logonoff.txt

:: Extract from event log on PDC startup and shutdown events
:: 512 success audit - Windows NT is starting up
:: 513 success audit - Windows NT is shutting down

dumpel -f d:\scripts\audit\output\%PDC%startshut.txt -l security -m security -e 512 513 -
d 1 -format tdISus
now >> d:\scripts\audit\output\%PDC%startshut.txt

:: EOF
```

References

[1] Merriam-Webster Online Collegiate Dictionary - http://www.m-w.com/cgi-bin/dictionary
[2] Microsoft Help Files (glossary) included with Microsoft Windows NT Server 4.0
[3] Milne, Jay, The Hard and Soft of Server Auditing,
http://www.networkcomputing.com/707/707work1.html
[4] Fossen, Jason, *Windows NT Security: Step by Step*. The SANS Institute GIAC Training, 2000.
[5] Microsoft article PSS IS Number Q174074
[6] Focus / Mark Joseph Edwards, David LeBlanc / August 1, 1999
http://www.win2000mag.com/Articles/Print.cfm?ArticleID=5702

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 13, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**