Global Information Assurance Certification Paper

Developments in Auditing NT
Practical Assignment for SNAP San Jose

Submitted by: Anil K. Jain

Background:

Undoubtedly Auditing provides an important means to detect a potential security problem. Windows NT comes with built in extensive auditing capabilities. When auditing is enabled, the audited events are recorded in the Security Event Log which can be viewed in the Event Viewer. However many audit records lack essential information and many contain information of very little use for manual analysis. Therefore Windows NT's built in auditing capabilities turn out to be not much useful. Fortunately, Windows NT fully accommodates 3rd party audit analysis tools that can be used to overcome these limitations. There are many products available for this purpose.

For this project, I have picked one such product. It is called NtLast and it is developed by NTObjectives, Inc. The reason for choosing NTLast is the ease of its use, its versatility, and also the reasonable price.

Auditing with NTLast

Although information regarding logon and logoff is generated by NT in the security log and it can be viewed in the event viewer. As aforementioned, the information obtained in NT's native format is not very useful for analysis because not only it is tedious to say the least but certain information is not even available. This shortcoming can easily be overcome by the NtLast.

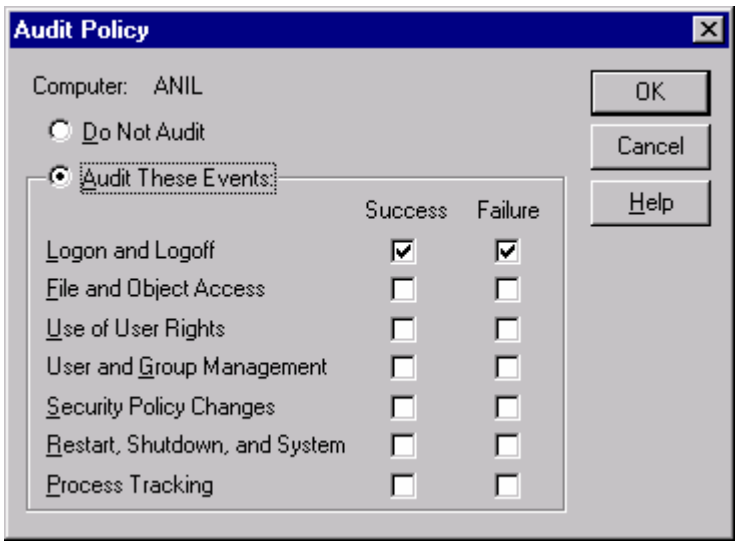
NTLast, a security audit tool for use with Windows NT, is a Win32 command utility with several switches that search the event log for logon and logoff records. It does the following major things that are not done by NT natively:

- **It can distinguish between remote and interactive logons.**
- **It matches logon times with logoff times**
- **A customized script can be created using multiple switches to generate usful reports.**

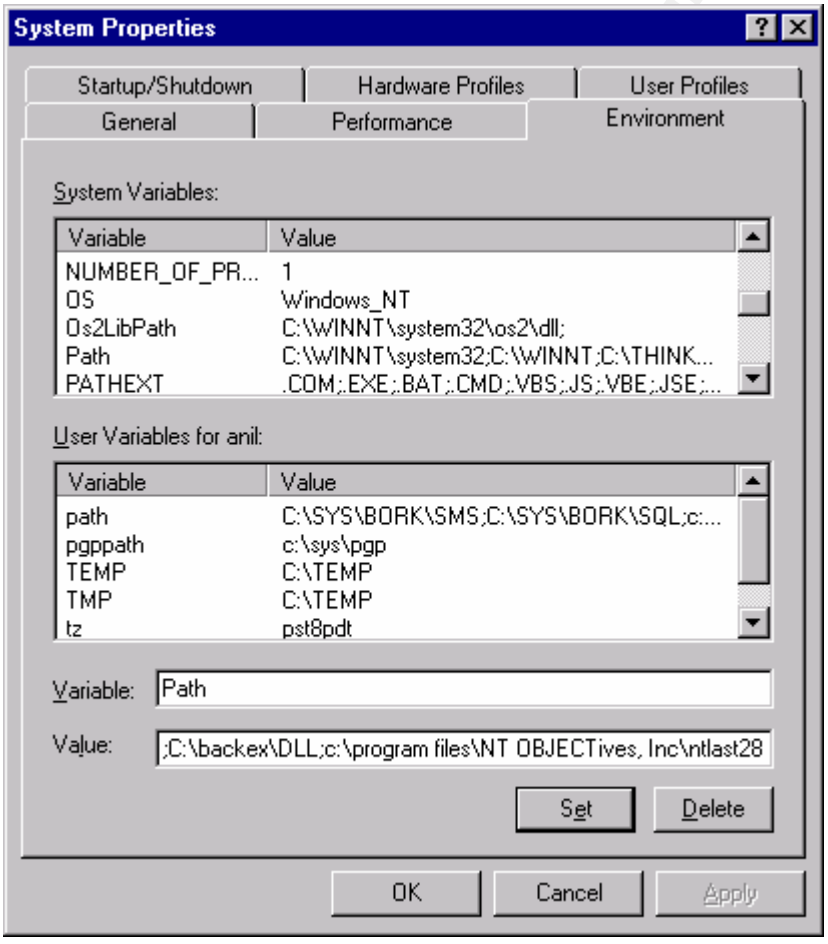
In this document, I will present the use of NTList step by step including above listed features.

Installing NTLast:

Installing Ntlast is straightforward. When purchased from the web, the latest version 2.8 is delivered in a package named **NTLast285.exe** which is 215 KB file. It can be launched by double clicking on this file. The suggested path for installation by the vendor is C:\Program Files\NTOBJECTives,Inc\NTLast28. Click OK to accept the suggested path. Five files will be placed in the NTLast28 folder. NTLast.exe, the program file is a 148KB. In order to use this tool, Auditing on that machine must be enabled through the use of user manager as shown below.



Add the path statement in System Properties as shown below so it can be run from any directory for the convenience.



Reboot the machine. Now, NTList is ready for use. Increasing the command line buffer size is also useful but it is not required.

Type ntlast with /? Switch to find various switches available for use as shown below.

```
C:\>ntlast /?
NTLast Copyright(c) 1998, NT OBJECTives, Inc. All Rights Reserved
v2.8.5 - Programming by JD Glaser
Command Line Switches
      -s      Last Successful Logons
      -f      Last Failed Logons
      -i      Last Interactive Logons
      -r      Last Remote Logons
      -u [u]  Logons by User - (u) = case sensitive username
      -m [m]  Name of machine to search - (m) = machine name
      -n [n]  Number of Last Logons - (n) = number of records records
      -from [\m]      Last logons from - (\m) = upper-case UNC server name
      -c      Condensed Output - Default
      -v      Verbose Output - shows logon/logoff/duration
      -not [u]        Filter out User - Case sensitive
      -null   Include null sessions - Ignored by default
      -mil    Military Time Output - Default matches event log time
      -file   File name - Saved .evt sec log to open
      -csv    Print output as CSV
      -rt     Raw date/times in CSV output
      -l      Last Successful Logon
      -l:i    Last Interactive Logon
      -l:r    Last Remote Logon
      -iis    IIS 4.0 logons only
      -ad     Include entries after this date/time - Specify military time
      -bd     Include entries before this date/time - Specify military time
                  Switches -ad and -bd can be combined to get between date
/time(s)
      - or /  Either switch statement can be used
      -?      Help
```

*Note - Switch arguments are case sensitive - 'UserX' and 'userx' are different
'HOSTX' and '\HOSTX' are different
*Note - To view IIS 4.0 logons, use IIS switch - off by default
*Note - Blank spaces for user name map to NT Anonymous logons
*Note - File switch usage #1-> ntlast -m \\HOSTX -file c:\log\sec.evt
*Note - File switch usage #2-> ntlast -file \\HOSTX\log\sec.evt
*Note - Time searches use 24hr time - Sept, 20th 7am is 20/9/1999-7:0:0
Sept, 20th 7pm is 20/9/1999-19:0:0
*Note - Using the /u switch last with no username generates list of NULL logons
*Note - For best usage - Set you console buffer to 1,000 lines or more
*Note - Redirect your output to a file - 'ntlast -v > report.txt'
*Note - Append your output like this - 'ntlast -v >> report.txt'

Sample uses of NTLast

NTLast by default lists the ten last successful logons.

```
C:\>ntlast -m \\edfdc
SMSClient_ED5  \\DC-BACKUP       ALLEDF      Wed Jun 14 11:16:02am 2000
SMSAdminNC     \\EDFNC           ALLEDF      Wed Jun 14 11:00:55am 2000
SMSAdminCO     \\EDFCO           ALLEDF      Wed Jun 14 11:00:52am 2000
SMSAdminCA     \\EDFCA2          ALLEDF      Wed Jun 14 11:00:07am 2000
SMSServer_ED5  \\EDFDC           ALLEDF      Wed Jun 14 10:50:51am 2000
SPETTAWAY      \\RECEPTION       ALLEDF      Wed Jun 14 10:48:07am 2000
JHOWARD        \\JHOWARD         ALLEDF      Wed Jun 14 10:47:13am 2000
JHOWARD        \\JHOWARD         ALLEDF      Wed Jun 14 10:47:12am 2000
JHOWARD        \\JHOWARD         ALLEDF      Wed Jun 14 10:47:11am 2000
AHO            \\AHO             ALLEDF      Wed Jun 14 10:47:05am 2000

C:\>
```

In the above example, 10 last successful logons have been listed from the server edfdc.

The –n switch allows to specify the number of records desired.

```
C:\>ntlast -m \\edfdc -f -n 20
NED            \\LAURIEK          GO2!0NIAN      Mon Jun 12 03:09:29pm 2000
LAURAG         \\LGASSLER                        Fri Jun 09 04:53:21am 2000
ARCServeAdminDC EDFDC             EDFDC          Tue May 23 10:08:30pm 2000
SPETTAWAY      \\RECEPTION                       Fri May 19 09:19:03am 2000
CARLOS         \\CRINCON                         Fri May 19 08:41:14am 2000
MICHAELR       \\MREPLOGLE                       Mon May 15 10:52:36am 2000
SSPENCER       \\SSPENCER                        Mon May 15 08:43:18am 2000
SSPENCER       \\SSPENCER                        Mon May 15 08:42:35am 2000
RTYLER         \\TOSHIMG                         Fri May 12 10:08:02am 200
RTYLER         \\TOSHIMG                         Fri May 12 10:07:59am 200
RTYLER         \\TOSHIMG                         Fri May 12 10:07:40am 200
ARCServeAdminDC EDFDC             EDFDC          Thu May 11 10:01:23pm 2000
JACKIE         \\JACKIE                          Thu May 04 10:22:10am 2000
anilrajankumar  EDFDC             ALLEDF         Thu May 04 08:52:53am 2000
MB             \\MBEAN                           Thu May 04 08:30:24am 2000
anilrajankumar  EDFDC             ALLEDF         Thu May 04 07:55:35am 2000
KOLSON         \\KOLSON                          Thu May 04 06:47:28am 2000
SPETTAWAY      \\RECEPTION                       Thu May 04 06:15:10am 2000
WARD           \\DWARD                           Thu May 04 05:59:15am 2000
HROSEN         \\HROSEN                          Thu May 04 05:16:42am 2000

C:\>
```

In the above example, 20 failed logon records are listed on the server edfdc.

Retrieving Interactive logons with –i switch.

```
C:\>ntlast -m \\edfdc -i
anil        EDFDC          ALLEDF       Wed Jun 14 11:52:01am 2000
 - End Of File -

C:\>
```

In the above example, the last interactive logon record is retrieved from the edfdc server.

Retrieving interactive failed logon records with –i and –f switch.

```
C:\>ntlast -m \\edfdc -i -f
ARCServeAdminDC EDFDC       EDFDC       Tue May 23 10:08:30pm 2000
ARCServeAdminDC EDFDC       EDFDC       Thu May 11 10:01:23pm 2000
anilrajankumar  EDFDC       ALLEDF      Thu May 04 08:52:53am 2000
anilrajankumar  EDFDC       ALLEDF      Thu May 04 07:55:35am 2000
ARCServeAdminDC EDFDC       EDFDC       Tue May 02 10:02:14pm 2000
ARCServeAdminDC EDFDC       EDFDC       Fri Mar 24 10:01:13pm 2000
 - End Of File -

C:\>
```

Retrieving detailed record with –v switch.

```
C:\>ntlast -m \\edfdc -i -v
Record Number: 5618
ComputerName: EDFDC
EventID: 528   -   Successful Logon
Logon:  Wed Jun 14 11:52:01am 2000
Logoff: Not Recorded
Details -
      ClientName:     anil
      ClientID:       (0x0,0xE334321)
      ClientMachine:  EDFDC
      ClientDomain:   ALLEDF
      LogonType:      Interactive

 - End Of File -

C:\>
```

In the above example, the detailed record for the last interactive successful logon on server edfdc is retrieved. Please note that it indicates that the user has not logoff yet. This information can be very useful for intrusion detection.

Filtering records with –not switch.

```
C:\>ntlast -m \\edfdc -i -f -n 20 -v -not ARCServeAdminDC
Record Number: 4664
ComputerName: EDFDC
EventID: 529     - Failed Logon Attempt
Time Attempted:  - Thu May 04 08:52:53am 2000
Details -
      ClientName:     anilrajankumar
      ClientMachine:  EDFDC
      ClientDomain:   ALLEDF
      LogonType:      Interactive

Record Number: 4660
ComputerName: EDFDC
EventID: 529     - Failed Logon Attempt
Time Attempted:  - Thu May 04 07:55:35am 2000
Details -
      ClientName:     anilrajankumar
      ClientMachine:  EDFDC
      ClientDomain:   ALLEDF
      LogonType:      Interactive

 - End Of File -

C:\>
```

In the example of retrieving failed interactive logons, if ARCServeadminDC is not a suspicious logon so we might want to filter this record and obtain the detailed information only about the rest of the failed interactive logons on the server edfdc as shown above.

Saving the output in a file.

```
C:\>ntlast -m \\edfdc >c:\output.txt

C:\>type output.txt
DCGUEST      \\GRAP          ALLEDF      Wed Jun 14 12:39:28pm 2000
DCGUEST      \\GRAP          ALLEDF      Wed Jun 14 12:39:11pm 2000
BILLIE       \\BILLIEJ       ALLEDF      Wed Jun 14 12:39:03pm 2000
BILLIE       \\BILLIEJ       ALLEDF      Wed Jun 14 12:39:00pm 2000
BILLIE       \\BILLIEJ       ALLEDF      Wed Jun 14 12:38:57pm 2000
DCGUEST      \\GRAP          ALLEDF      Wed Jun 14 12:38:54pm 2000
DCGUEST      \\GRAP          ALLEDF      Wed Jun 14 12:38:37pm 2000
DCGUEST      \\GRAP          ALLEDF      Wed Jun 14 12:38:21pm 2000
DCGUEST      \\GRAP          ALLEDF      Wed Jun 14 12:37:59pm 2000
DCGUEST      \\GRAP          ALLEDF      Wed Jun 14 12:37:44pm 2000

C:\>
```

Gathering logon and logoff information from various servers and writing it in one file.

```
C:\>ntlast -m \\edfdc
SMSAdminNC      \\EDFNC          ALLEDF        Wed Jun 14 06:01:00pm 2000
SMSAdminCO      \\EDFCO          ALLEDF        Wed Jun 14 06:00:46pm 2000
SMSAdminMA      \\EDFMA          ALLEDF        Wed Jun 14 06:00:11pm 2000
SMSAdminCA      \\EDFCA2         ALLEDF        Wed Jun 14 06:00:10pm 2000
SMSAdmin        \\EDFNY3         ALLEDF        Wed Jun 14 06:00:09pm 2000
SMSAdminTX      \\EDFTX          ALLEDF        Wed Jun 14 06:00:08pm 2000
WILD            \\WILD           ALLEDF        Wed Jun 14 05:45:07pm 2000
WILD            \\WILD           ALLEDF        Wed Jun 14 05:45:03pm 2000
WILD            \\WILD           ALLEDF        Wed Jun 14 05:45:03pm 2000
WILD            \\WILD           ALLEDF        Wed Jun 14 05:45:03pm 2000

C:\>ntlast -m \\dc-backup
anil            \\ANIL           ALLEDF        Wed Jun 14 06:07:58pm 2000
SMSAdminTX      \\EDFTX          ALLEDF        Wed Jun 14 06:01:41pm 2000
SMSAdminCO      \\EDFCO          ALLEDF        Wed Jun 14 06:01:33pm 2000
SMSAdminNC      \\EDFNC          ALLEDF        Wed Jun 14 06:00:51pm 2000
SMSAdminDC      \\EDFDC          ALLEDF        Wed Jun 14 06:00:11pm 2000
SMSAdminMA      \\EDFMA          ALLEDF        Wed Jun 14 06:00:03pm 2000
SMSAdminCA      \\EDFCA2         ALLEDF        Wed Jun 14 06:00:03pm 2000
SMSAdmin        \\EDFNY3         ALLEDF        Wed Jun 14 06:00:03pm 2000
SMSAdminDC      \\EDFDC          ALLEDF        Wed Jun 14 05:29:53pm 2000
SMSAdminCO      \\EDFCO          ALLEDF        Wed Jun 14 05:01:41pm 2000

C:\>ntlast -m \\edfdc >c:\output.txt

C:\>ntlast -m \\dc-backup >>c:\output.txt

C:\>type output.txt
SMSAdminNC      \\EDFNC          ALLEDF        Wed Jun 14 06:01:00pm 2000
SMSAdminCO      \\EDFCO          ALLEDF        Wed Jun 14 06:00:46pm 2000
SMSAdminMA      \\EDFMA          ALLEDF        Wed Jun 14 06:00:11pm 2000
SMSAdminCA      \\EDFCA2         ALLEDF        Wed Jun 14 06:00:10pm 2000
SMSAdmin        \\EDFNY3         ALLEDF        Wed Jun 14 06:00:09pm 2000
SMSAdminTX      \\EDFTX          ALLEDF        Wed Jun 14 06:00:08pm 2000
WILD            \\WILD           ALLEDF        Wed Jun 14 05:45:07pm 2000
WILD            \\WILD           ALLEDF        Wed Jun 14 05:45:03pm 2000
WILD            \\WILD           ALLEDF        Wed Jun 14 05:45:03pm 2000
WILD            \\WILD           ALLEDF        Wed Jun 14 05:45:03pm 2000
anil            \\ANIL           ALLEDF        Wed Jun 14 06:07:58pm 2000
SMSAdminTX      \\EDFTX          ALLEDF        Wed Jun 14 06:01:41pm 2000
SMSAdminCO      \\EDFCO          ALLEDF        Wed Jun 14 06:01:33pm 2000
SMSAdminNC      \\EDFNC          ALLEDF        Wed Jun 14 06:00:51pm 2000
SMSAdminDC      \\EDFDC          ALLEDF        Wed Jun 14 06:00:11pm 2000
SMSAdminMA      \\EDFMA          ALLEDF        Wed Jun 14 06:00:03pm 2000
SMSAdminCA      \\EDFCA2         ALLEDF        Wed Jun 14 06:00:03pm 2000
SMSAdmin        \\EDFNY3         ALLEDF        Wed Jun 14 06:00:03pm 2000
SMSAdminDC      \\EDFDC          ALLEDF        Wed Jun 14 05:29:53pm 2000
SMSAdminCO      \\EDFCO          ALLEDF        Wed Jun 14 05:01:41pm 2000

C:\>
```

CVS format file can be opened in Excel or Access for further analysis and for the presentation of data.

```
C:\>ntlast -m \\edfdc >c:\output.txt -csv

C:\>type output.txt
SMSAdminNC,\\EDFNC,ALLEDF,Wed Jun 14 06:01:00pm 2000
SMSAdminCO,\\EDFCO,ALLEDF,Wed Jun 14 06:00:46pm 2000
SMSAdminMA,\\EDFMA,ALLEDF,Wed Jun 14 06:00:11pm 2000
SMSAdminCA,\\EDFCA2,ALLEDF,Wed Jun 14 06:00:10pm 2000
SMSAdmin,\\EDFNY3,ALLEDF,Wed Jun 14 06:00:09pm 2000
SMSAdminTX,\\EDFTX,ALLEDF,Wed Jun 14 06:00:08pm 2000
WILD,\\WILD,ALLEDF,Wed Jun 14 05:45:07pm 2000
WILD,\\WILD,ALLEDF,Wed Jun 14 05:45:03pm 2000
WILD,\\WILD,ALLEDF,Wed Jun 14 05:45:03pm 2000
WILD,\\WILD,ALLEDF,Wed Jun 14 05:45:03pm 2000

C:\>
```

In the above example, the data is provided in the csv format that can easily be imported in Excel as shown below.

	A	B	C	D
1	SMSAdminNC	\\EDFNC	ALLEDF	Wed Jun 14 06:01:00pm 2000
2	SMSAdminCO	\\EDFCO	ALLEDF	Wed Jun 14 06:00:46pm 2000
3	SMSAdminMA	\\EDFMA	ALLEDF	Wed Jun 14 06:00:11pm 2000
4	SMSAdminCA	\\EDFCA2	ALLEDF	Wed Jun 14 06:00:10pm 2000
5	SMSAdmin	\\EDFNY3	ALLEDF	Wed Jun 14 06:00:09pm 2000
6	SMSAdminTX	\\EDFTX	ALLEDF	Wed Jun 14 06:00:08pm 2000
7	WILD	\\WILD	ALLEDF	Wed Jun 14 05:45:07pm 2000
8	WILD	\\WILD	ALLEDF	Wed Jun 14 05:45:03pm 2000
9	WILD	\\WILD	ALLEDF	Wed Jun 14 05:45:03pm 2000
10	WILD	\\WILD	ALLEDF	Wed Jun 14 05:45:03pm 2000

Conclusion:

NTList, a 3rd party product developed by NTOBJEctives, Inc. enhances Windows NT's built in capability of auditing logon and logoff events significantly. As shown in this document by examples, NTList distinguishes between remote and interactive logons. It also matches logon times with logoff times. NTList allows data from various machines to be gathered in one single file. Finally, NTList allows data to be presented in csv format which can easily be imported in many applications.

References:

Jason Fossen and Jesper Johansson:**Windows NT Security:Step by Step,** SANS Institute 2000.

Chris Bent:**Auditing Windows NT With NT OBJECTive Tools, ,** http://www.geek-speak.net/products/ntaudit1.html**,** updated 2000.

Steve Sutton**:NSA Windows NT Security Guidelines,** http://www.trustedsystems.com **,**updated 1999.

National Security Agency, Ft. Meade, MD:**Guide to Securing Microsoft Windows NT Networks,** March 1999.

Marcus Goncalves and Marcus Gonsalves: Windows Nt 4.0 Server Security Guide Prentice Hall ,1998.

Michael J. McInerney:**Windows NT Security,** Prentice Hall, 1999.

James D. Murray, Debby Russell (Editor):Windows NT Event Logging ,O'Reilly& Associates, 1998.

James G. Jumes (Editor):**Microsoft Windows Nt 4.0 Security, Audit, and Control,** Microsoft Press, 1998.