Auditing Windows NT 4.0

Sven Lehmberg
Agenda

- Event Viewer and User Manager
- Analyzing Audit Logs
- Tools
Auditing Step by Step

Two important programs in NT 4.0

- **Event Viewer**
- and

- **User Manager**

**User Manager for Domains**
**Event Viewer**

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Source</th>
<th>Category</th>
<th>Event</th>
<th>User</th>
<th>Computer</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/7/99</td>
<td>12:04:18 PM</td>
<td>Security</td>
<td>Privilege Use</td>
<td>578</td>
<td>Garuda</td>
<td>RLA01079</td>
</tr>
<tr>
<td>11/7/99</td>
<td>12:02:07 PM</td>
<td>Security</td>
<td>System Event</td>
<td>515</td>
<td>SYSTEM</td>
<td>RLA01079</td>
</tr>
<tr>
<td>11/7/99</td>
<td>12:02:07 PM</td>
<td>Security</td>
<td>Privilege Use</td>
<td>577</td>
<td>SYSTEM</td>
<td>RLA01079</td>
</tr>
<tr>
<td>11/7/99</td>
<td>12:02:02 PM</td>
<td>Security</td>
<td>System Event</td>
<td>515</td>
<td>SYSTEM</td>
<td>RLA01079</td>
</tr>
<tr>
<td>11/7/99</td>
<td>12:02:02 PM</td>
<td>Security</td>
<td>Privilege Use</td>
<td>577</td>
<td>SYSTEM</td>
<td>RLA01079</td>
</tr>
<tr>
<td>11/7/99</td>
<td>12:02:01 PM</td>
<td>Security</td>
<td>Privilege Use</td>
<td>577</td>
<td>SYSTEM</td>
<td>RLA01079</td>
</tr>
<tr>
<td>11/7/99</td>
<td>12:02:01 PM</td>
<td>Security</td>
<td>System Event</td>
<td>515</td>
<td>SYSTEM</td>
<td>RLA01079</td>
</tr>
<tr>
<td>11/7/99</td>
<td>12:01:51 PM</td>
<td>Security</td>
<td>Privilege Use</td>
<td>577</td>
<td>SYSTEM</td>
<td>RLA01079</td>
</tr>
<tr>
<td>11/7/99</td>
<td>12:01:51 PM</td>
<td>Security</td>
<td>System Event</td>
<td>515</td>
<td>SYSTEM</td>
<td>RLA01079</td>
</tr>
<tr>
<td>11/7/99</td>
<td>12:01:49 PM</td>
<td>Security</td>
<td>Privilege Use</td>
<td>577</td>
<td>SYSTEM</td>
<td>RLA01079</td>
</tr>
<tr>
<td>11/7/99</td>
<td>12:01:49 PM</td>
<td>Security</td>
<td>System Event</td>
<td>515</td>
<td>SYSTEM</td>
<td>RLA01079</td>
</tr>
<tr>
<td>11/7/99</td>
<td>12:01:46 PM</td>
<td>Security</td>
<td>Privilege Use</td>
<td>577</td>
<td>SYSTEM</td>
<td>RLA01079</td>
</tr>
</tbody>
</table>

**ZT IK 3, Siemens CERT**
HOWTO Enable Auditing?

<table>
<thead>
<tr>
<th>Username</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td></td>
<td>Decoy Account</td>
</tr>
<tr>
<td>Gandalf</td>
<td></td>
<td>User</td>
</tr>
<tr>
<td>Garuda</td>
<td></td>
<td>New Admin Account</td>
</tr>
<tr>
<td>Guest</td>
<td></td>
<td>Forgotten who that is :-)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Groups</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrators</td>
<td>Members can fully administer the computer/domain</td>
</tr>
<tr>
<td>Backup Operators</td>
<td>Members can bypass file security to back up files</td>
</tr>
<tr>
<td>Guests</td>
<td>Users granted guest access to the computer/domain</td>
</tr>
<tr>
<td>Power Users</td>
<td>Members can share directories and printers</td>
</tr>
<tr>
<td>Replicator</td>
<td>Supports file replication in a domain</td>
</tr>
<tr>
<td>Users</td>
<td>Ordinary users</td>
</tr>
</tbody>
</table>
What to Audit?

Audit Policy

Computer: RLA01079
 Do Not Audit

Audit These Events:

- Success
- Failure

- Logon and Logoff
- File and Object Access
- Use of User Rights
- User and Group Management
- Security Policy Changes
- Restart, Shutdown, and System
- Process Tracking

OK Cancel Help
Logon and Logoff

Audit Policy

Computer: RLA01079

- Do Not Audit
- Audit These Events:

- Logon and Logoff: Success: [ ] Failure: [ ]
- File and Object Access
- Use of User Rights
- User and Group Management
- Security Policy Changes
- Restart, Shutdown, and System
- Process Tracking

OK
Cancel
Help
Interactive Logon

ZT IK 3, Siemens CERT
### Logon Type and Processes

<table>
<thead>
<tr>
<th>Logon Type:</th>
<th>Authentication Package:</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 : Interactive</td>
<td>MICROSOFT_AUTHENTICATION_PACKAGE_V1_0</td>
</tr>
<tr>
<td>3 : Network</td>
<td></td>
</tr>
<tr>
<td>4 : Batch</td>
<td></td>
</tr>
<tr>
<td>5 : Service</td>
<td></td>
</tr>
<tr>
<td>6 : Proxy</td>
<td></td>
</tr>
<tr>
<td>7 : Unlock Workstation</td>
<td></td>
</tr>
</tbody>
</table>

**Logon Process:**
- KSecDD
- User32 or WinLogon\MSGina
- SCMgr
- LAN Manager Workstation Service
- advapi
- MS.RADIUS
Logon over the Network

User: Garuda
Date: 1/13/00
Time: 11:09:51 AM
Source: Security
Category: Logon/Logoff
Computer: M26248PP

Successful Logon:
User Name: garuda
Domain: KOSMOS
Logon ID: (0x0, 0x5CCE2)
Logon Type: 3
Logon Process: KSecDD
Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Workstation Name: \M27902PP

User: NT AUTHORITY\SYSTEM
Date: 1/13/00
Time: 11:09:39 AM
Source: Security
Category: Logon/Logoff
Computer: M26248PP

Logon Failure:
Reason: Unknown user name or bad password
User Name: garuda
Domain: M27902PP
Logon Type: 3
Logon Process: KSecDD
Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Workstation Name: \M27902PP
Event Detail – No Logon Right over Network

- Date: 1/13/00
- Time: 10:59:43 AM
- User: NT AUTHORITY\SYSTE
- Computer: M26248PP

Description:

Logon Failure:
- Reason: The user has not be granted the requested logon type at this machine
- User Name: stevemartin
- Domain: KOSMOS
- Logon Type: 3
- Logon Process: KSecDD

Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0

Workstation Name: \M27902PP
File and Object Access

Audit Policy

- Computer: RLA01079
  - Do Not Audit
  - Audit These Events:
    - Logon and Logoff
    - File and Object Access
    - Use of User Rights
    - User and Group Management
    - Security Policy Changes
    - Restart, Shutdown, and System
    - Process Tracking

Success / Failure

OK / Cancel / Help
Event Detail – Object Access: File

SIEMENS ZT IK 3, Siemens CERT
## File System Access Types

<table>
<thead>
<tr>
<th>Action and Permissions</th>
<th>Full control</th>
<th>Modify</th>
<th>Read&amp;Execute, List folders</th>
<th>Read</th>
<th>Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traverse folder / Execute file</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>List folder / Read data</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Read attributes</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Read extended attributes</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Create files / Write data</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create folders / Append data</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Write attributes</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Write extended attributes</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Delete subfolders and files</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read permissions (READ_CONTROL)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Change permissions (WRITE_DAC)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Take ownership (WRITE_OWNER)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Synchronize</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
## Registry Access Types

- Query Value
- Set Value
- Create Subkey
- Enumerate Subkeys
- Notify
- Create Link
- Delete
- Write DAC
- Read Control
Use of User Rights

Audit Policy

Computer: RLA01079

- Do Not Audit
- Audit These Events:
  - Use of User Rights

Success: [ ]
Failure: [ ]

Other options:
- Logon and Logoff
- File and Object Access
- User and Group Management
- Security Policy Changes
- Restart, Shutdown, and System
- Process Tracking

OK
Cancel
Help
## 27 User Rights

<table>
<thead>
<tr>
<th>Access this Computer from Network</th>
<th>Debug programs – SeDebugPrivilege</th>
<th>Log on locally</th>
</tr>
</thead>
<tbody>
<tr>
<td>Act as part of the operating system - SeTcbPrivilege</td>
<td>Force shutdown from a remote system – SeRemoteShutdownPrivilege</td>
<td>Manage auditing and security - SeSecurityPrivilege</td>
</tr>
<tr>
<td>Backup files and directories – SeBackupPrivilege</td>
<td>Increase quotas – SeIncreaseQuotaPrivilege</td>
<td>Profile single process – SeProfileSingleProcessPriv.</td>
</tr>
<tr>
<td>Change the system time – SeSystemTimePrivilege</td>
<td>Load and unload device drivers – SeLoadDriverPrivilege</td>
<td>Replace a process level token – SeAssignPrimaryTokenPriv.</td>
</tr>
<tr>
<td>Create a token object – SeCreateTokenPrivilege</td>
<td>Log on as a batch job – SeBatchSID</td>
<td>Shut down the system – SeShutdownPriv.</td>
</tr>
<tr>
<td>Create permanent shared objects – SeCreate PermanentPrivilege</td>
<td>Log on as a Service – SeServiceSID</td>
<td>Take ownership of files or other objects – SeTakeOwnershipPriv.</td>
</tr>
</tbody>
</table>
Event Detail – Use of User Rights

Date: 11/15/99  
Time: 12:17:46 PM  
User: Garuda  
Computer: RLA01079  
Event ID: 578  
Type: Success Audit  
Category: Privilege Use  

Description:  
Object Server: EventLog  
Object Handle: 0  
Process ID: 2156729088  
Primary User Name: SYSTEM  
Primary Domain: NT AUTHORITY  
Primary Logon ID: (0x0,0x3E7)  
Client User Name: Garuda  
Client Domain: RLA01079  
Client Logon ID: (0x0,0x38A3)  
Privileges: SeSecurityPrivilege

Date: 17.01.00  
Time: 15:20:35  
User: Shiva  
Computer: RLA01079  
Event ID: 577  
Type: Success Audit  
Category: Privilege Use  

Description:  
Privileged Service Called:  
Server: Security  
Service: -  
Primary User Name: Shiva  
Primary Domain: RLA01079  
Primary Logon ID: (0x0,0x135E20)  
Client User Name: -  
Client Domain: -  
Client Logon ID: -  
Privileges: SeSystemtimePrivilege

ZT IK 3, Siemens CERT
User and Group Management

Audit Policy

Computer: RLA01079

Audit These Events:

- Logon and Logoff
- File and Object Access
- Use of User Rights
- User and Group Management
- Security Policy Changes
- Restart, Shutdown, and System
- Process Tracking

Success | Failure
--- | ---
| | |

[Checkboxes for success and failure for each event are present.]

OK | Cancel | Help
Event Detail – User and Group Management

ZT IK 3, Siemens CERT
Security Policy Changes

Audit Policy

- Computer: RLA01079
- Do NotAudit
- Audit These Events:
  - Logon and Logoff
  - File and Object Access
  - Use of User Rights
  - User and Group Management
  - Security Policy Changes
  - Restart, Shutdown, and System
  - Process Tracking

Success Failure

OK Cancel Help

ZT IK 3, Siemens CERT
ZT IK 3, Siemens CERT
Restart, Shutdown, and System

ZT IK 3, Siemens CERT
Event Detail: Restart, Shutdown, and System

Date: 11/14/99
Time: 5:17:17 PM
User: NT AUTHORITY\SYSTE
Computer: RLA01079

Event ID: 512
Source: Security
Type: Success Audit
Category: System Event

Description:
Windows NT is starting up.
Starting NT – Authentication and Trusted Logon

An authentication package has been loaded by the Local Security Authority. This authentication package will be used to authenticate logon attempts.

Authentication Package Name: msv1_0

A trusted logon process has registered with the Local Security Authority. This logon process will be trusted to submit logon requests.

Logon Process Name: \Winlogon\MSGina
Process Tracking

Audit Policy

Computer: RLA01079

- Do Not Audit
- Audit These Events:
  - Logon and Logoff
  - File and Object Access
  - Use of User Rights
  - User and Group Management
  - Security Policy Changes
  - Restart, Shutdown, and System
  - Process Tracking

Success | Failure
---|---

OK | Cancel | Help

ZT IK 3, Siemens CERT
### Windows NT Task Manager

#### Applications

<table>
<thead>
<tr>
<th>Image Name</th>
<th>PID</th>
<th>CPU</th>
<th>CPU Time</th>
<th>Mem Usage</th>
<th>Handles</th>
<th>Threads</th>
</tr>
</thead>
<tbody>
<tr>
<td>sens.exe</td>
<td>166</td>
<td>00</td>
<td>0:00:00</td>
<td>2120 K</td>
<td>51</td>
<td>6</td>
</tr>
<tr>
<td>Report.exe</td>
<td>177</td>
<td>97</td>
<td>1:55:29</td>
<td>1792 K</td>
<td>36</td>
<td>3</td>
</tr>
<tr>
<td>inetinfo.exe</td>
<td>187</td>
<td>00</td>
<td>0:00:00</td>
<td>3104 K</td>
<td>69</td>
<td>4</td>
</tr>
<tr>
<td>LOADWC.EXE</td>
<td>191</td>
<td>00</td>
<td>0:00:00</td>
<td>900 K</td>
<td>24</td>
<td>2</td>
</tr>
<tr>
<td>cidaemon.exe</td>
<td>197</td>
<td>00</td>
<td>0:00:00</td>
<td>40 K</td>
<td>60</td>
<td>1</td>
</tr>
<tr>
<td>nukeabanber.exe</td>
<td>218</td>
<td>00</td>
<td>0:00:03</td>
<td>4476 K</td>
<td>113</td>
<td>3</td>
</tr>
<tr>
<td>PGPTray.exe</td>
<td>220</td>
<td>00</td>
<td>0:00:00</td>
<td>1428 K</td>
<td>19</td>
<td>1</td>
</tr>
<tr>
<td>USERINIT.EXE</td>
<td>227</td>
<td>00</td>
<td>0:00:00</td>
<td>1080 K</td>
<td>39</td>
<td>3</td>
</tr>
<tr>
<td>WINWORD.EXE</td>
<td>236</td>
<td>00</td>
<td>0:00:06</td>
<td>11820 K</td>
<td>147</td>
<td>3</td>
</tr>
<tr>
<td>OUTLOOK.EXE</td>
<td>240</td>
<td>00</td>
<td>0:00:20</td>
<td>16240 K</td>
<td>226</td>
<td>10</td>
</tr>
<tr>
<td>mgaqdesk.exe</td>
<td>241</td>
<td>00</td>
<td>0:00:00</td>
<td>808 K</td>
<td>18</td>
<td>1</td>
</tr>
<tr>
<td>EXPLORER.EXE</td>
<td>242</td>
<td>00</td>
<td>0:00:25</td>
<td>6172 K</td>
<td>136</td>
<td>6</td>
</tr>
<tr>
<td>CMD.EXE</td>
<td>247</td>
<td>00</td>
<td>0:00:00</td>
<td>1080 K</td>
<td>20</td>
<td>1</td>
</tr>
<tr>
<td>mghook.exe</td>
<td>249</td>
<td>00</td>
<td>0:00:00</td>
<td>584 K</td>
<td>13</td>
<td>1</td>
</tr>
<tr>
<td>CMD.EXE</td>
<td>250</td>
<td>00</td>
<td>0:00:00</td>
<td>1140 K</td>
<td>21</td>
<td>1</td>
</tr>
<tr>
<td>AcroTray.exe</td>
<td>251</td>
<td>00</td>
<td>0:00:00</td>
<td>712 K</td>
<td>18</td>
<td>1</td>
</tr>
<tr>
<td>NDDEAGNT.EXE</td>
<td>269</td>
<td>01</td>
<td>0:00:00</td>
<td>824 K</td>
<td>16</td>
<td>1</td>
</tr>
<tr>
<td>TASKMGR.EXE</td>
<td>282</td>
<td>01</td>
<td>0:00:02</td>
<td>1160 K</td>
<td>26</td>
<td>3</td>
</tr>
<tr>
<td>USRMGR.EXE</td>
<td>283</td>
<td>00</td>
<td>0:00:00</td>
<td>2272 K</td>
<td>25</td>
<td>1</td>
</tr>
</tbody>
</table>

#### End Process

- Processes: 43
- CPU Usage: 100%
- Mem Usage: 99692K / 248524K
Process IDs II

A new process has been created:
- New Process ID: 2154714560
- Image File Name: CMD.EXE
- Creator Process ID: 2154804928
- User Name: Garuda
- Domain: KOSMOS
- Logon ID: (0x0,0x128FD1)

A new process has been created:
- New Process ID: 2154491936
- Image File Name: CMD.EXE
- Creator Process ID: 2154714560
- User Name: Garuda
- Domain: KOSMOS
- Logon ID: (0x0,0x128FD1)

ZT IK 3, Siemens CERT
Process IDs IV – Windows 2000

Event Properties

Date: 1/17/2000  Source: Security
Time: 12:17    Category: Detailed Tracking
Type: Success  Event ID: 593
User: RLA01079\Garuda
Computer: RLA01079

Description:
A process has exited:
  Process ID: 436
  User Name: Garuda
  Domain: RLA01079
  Logon ID: (0x0x97DE)

ZT IK 3, Siemens CERT
One Click - Many Security Events

Audit Logs for a new user account:
- Event 632: Global Group Member Added
- Event 624: User Account Created
- Event 642: User Account Changed
- Event 636: Local Group Member Added
Additional Auditing settings

- Auditing Backup and Restore Activities
  Key: HKLM\System\CCS\Control\Lsa\%
  Data: FullPrivilegeAuditing
  Type: REG_BINARY
  Value: 1

- Base Object Auditing
  Key: HKLM\System\CCS\Control\Lsa\%
  Data: AuditBaseObjects
  Type: REG_DWORD
  Value: 1
“Account Lockout Event” stored on PDC

- Windows NT 4.0 SP4+

  When a user enters too many incorrect passwords in an attempt to log on to a domain, the account is locked out and an event is written to the workstations security logs (if auditing is enabled here). With SP4 this event is also written to the PDC security log.
Audit Policy

Audit Policy

Domain: KOSMOS

- Do Not Audit
- Audit These Events:
  - Success
  - Failure
  - Logon and Logoff
  - File and Object Access
  - Use of User Rights
  - User and Group Management
  - Security Policy Changes
  - Restart, Shutdown, and System
  - Process Tracking
Event Log Settings

Change Settings for Security Log

Maximum Log Size: 4096 Kilobytes (64K Increments)

Event Log Wrapping
- Overwrite Events as Needed
- Overwrite Events Older than Days
- Do Not Overwrite Events (Clear Log Manually)
Lesson learnt

- You can get a lot of information from the logs
- Not all information is relevant
- Some information is wrong
- You can’t get too much information about logging from MS
Filter Suspicious Events from all Events

Event IDs

- 512 - Windows NT is starting up
- 513 - Windows NT is shutting down
- 517 - The audit log was cleared
- 528 - Successful logon
- **529 - Unknown user name or bad password**
- 530 – Account logon time restriction violation
- 531 - Account currently disabled
- 532 - The specified user account has expired
- 533 - User not allowed to log on at this computer
- 534 – User has not been granted the requested logon type
- 535 - The specified account’s password has expired
- 536 – The NetLogon component is not active
- 537 – An unexpected error occurred during logon
- 538 – User Log off
- 539 - Account locked out
- 576 - Special privileges assigned to new logon
- 608 - User Right Assigned
- 609 - User Right Removed
- 612 - Audit Policy Change
- 624 - User Account Created
- 643 - Domain Policy Changed
Failed Logon Event ID – 529

Administrator and „Well Known Accounts“
Filter Suspicious Events from all Events

View From:
- First Event
- Events On:
  - 11/22/99
  - 12:50:58PM

View Through:
- Last Event
- Events On:
  - 11/28/99
  - 1:06:13PM

Types:
- Information
- Warning
- Success Audit
- Failure Audit

Source: (All)
Category: (All)
User:
Computer:
Event ID: 529
Deficiencies of NT Logging

- Portscans can not be detected
  - BOF – Back Officer Friendly (NFR)
    http://www.nfr.com
  - Nuke Nabber 2.9a (Dynamsol)
    http://www.dynamsol.com/puppet/
  - NetMonitor v0.90 (LeechSoftware)
    http://www.leechsoftware.com
  - BlackICE
    http://advide.networkice.com

- Workstation logs are kept locally
  - See next slide
SIEMENS

Logging Host

- EvntSLog 2.0
- NTSlog 1.02, 2.0
- NTOLog
- Siemens CERT

ZT IK 3, Siemens CERT
Further Tools

- Lservers (NT Objectives, Inc.)
- NPLList (NT Objectives, Inc.)
- WDumpEvt 1.2
- ELDump 0.12
- ELSaveClr
- NTLast
- Tripwire 2.1 for Windows NT
Literature etc.

- **MS Knowledgebase:**
  Q174073, Auditing User Authentication
  Q174074, Security Event Descriptions
  Q163905, Auditing User Right Assignment Changes
  Q101366, Definition and List of Windows NT Advanced User Rights et al.
  found at [http://support.microsoft.com/support/search/c.asp](http://support.microsoft.com/support/search/c.asp)

- **Books etc.:**
  Microsoft – Windows NT 4.0 Security, Audit and Control
  Microsoft Press – Microsoft Technical Reference
  Windows NT Server Resource Kit 4.0
  Visual C++: winnt.h