Practical Intrusion Detection Non-Unix Based Systems

Marcey Kelley

Intrusion Detection Workshop

Gaithersburg, MD

April 23-24, 1997

Work performed under the auspicies of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48

UCRL-MI-127226
CSTC 97-062

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial products, process or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

CIAC is the U.S. Department of Energy's Computer Incident Advisory Capability. Established in 1989, shortly after the Internet Worm, CIAC provides various computer security services to employees and contractors of the DOE, such as:

- Incident Handling consulting
- Computer Security Information
- On-site Workshops
- White-hat Audits

CIAC is located at Lawrence Livermore National Laboratory and is a part of its Computer Security Technology Center. CIAC is also a founding member of FIRST, the Forum of Incident Response and Security Teams, a global organization established to foster cooperation and coordination among computer security teams worldwide.

Reference to any specific commercial product does not necessarily constitute or imply its endorsement, recommendation or favoring by CIAC, the University of California, the United States Department of Energy, or the United States Government.

Technical Acknowledgements

- Kathryn Call - FedCIRC West
- Scott Denton - FedCIRC West
- Shawn Hernan - FedCIRC East
- Christopher Murray - FedCIRC West
- Derek Simmel - FedCIRC East

Overview

- Introduction
- Specific intrusion types
  - Windows NT
  - Macintosh
  - Novell
- Intrusion detection
- Resources

Introduction

- **Trends for computer systems are moving towards the desktop**
  - **The separation between Unix and desktop system capabilities is narrowing**
  - **Desktop computers are**
    - **Becoming as powerful as Unix boxes**
    - **More economical**
  - **More similarity of services and avenues for intrusions**
    - **Desktop systems have added TCP/IP for routing across Wide Area Networks (WANs)**
    - **Traditional network services now available on desktop systems**
  - **NT servers had 85% growth rate in 1996 (International Data Corporation)**

Introduction (continued)

- Windows NT appears to be hacker's next target
- Public announcements of attacks
  - Scriptors of Doom to hit NT
    - Announcement by editor of Phrack Magazine
  - Emerging NT newsgroups
    - Bug reports starting to show up
    - New NT bugtraq
- Hackers don't do cost benefit analysis but . . .
  - NT provides a new area of challenge to hackers
    - Encouraged by promotion of NT "security"
  - NT supports the traditional network services that have been so effective in hacking Unix machines

Specific intrusion types

- Intrusion model
- General intrusion paths on desktop systems
- Intrusion paths for Windows NT
- Intrusion paths for Macintosh
- Intrusion paths for Novell

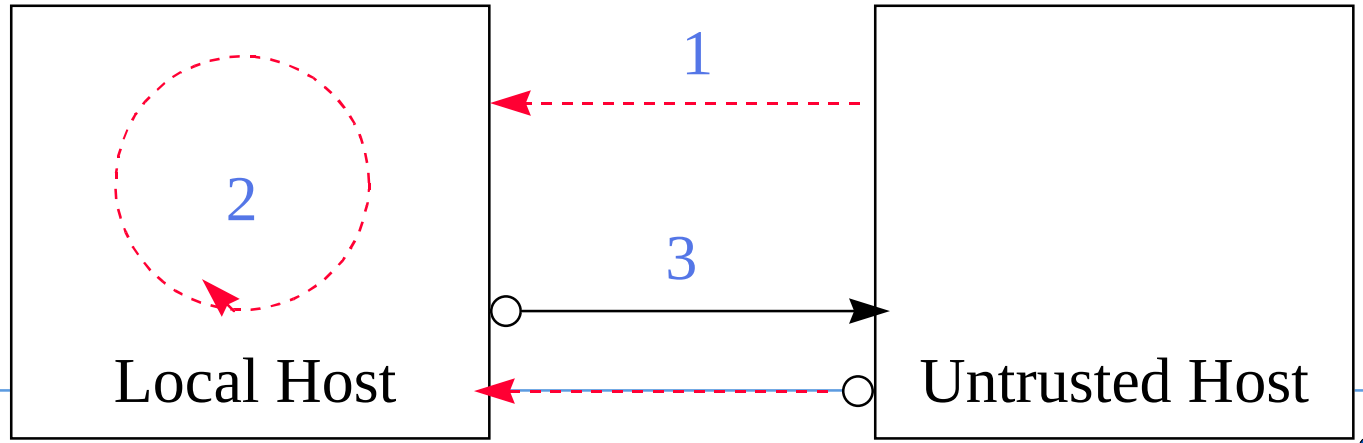
Intrusion model

Type 1: Attacks on network and dial-up services

Type 2: Physical attacks against a local system

- **Virus attacks using current privilege**
- **Non-privileged users attempting to gain privilege to view, alter, or control**

Type 3: Server attacks on client applications NEW



General intrusion paths on desktop systems

- Many intrusions are on client machines vulnerable to untrusted host connections via web browsers
- Adding third-party software on top of the operating system often introduces points for intrusion
  - End users install pre-released software with no notion of the security implications
  - Misconfiguration of software opens systems to attack
  - Word and Excel files allow macro viruses across platforms
- Some attacks on desktop systems use different vulnerabilities to provide similar intrusion opportunities as in Unix
  - phf attack --> Internet Information Server (IIS) ".." bug
  - Network File System (NFS) attack --> Apple public file servers misconfigured as writable

Intrusion paths for Windows NT

- Type 3 Intrusions
  - Internet Explorer 3.x (Windows NT and 95)
    - Five serious security bugs discovered in March, 1997
    - Malicious .url or .lnk files
    - Malicious icon can be embedded within a web page
    - Version 3.02 is now available and claims to fix these problems
  - Active X
    - ActiveX enabled browsers inherit capabilities of the local user, thus enabling an accepted malicious ActiveX control to execute arbitrary commands
  - Shockwave (Windows NT and 95)
    - Allows malicious webpage developers to create a Shockwave movie that will read through a user's e-mail and potentially upload it to their web server

Intrusion paths for Windows NT (continued)

- Type 2 Intrusions
  - Physical Access
    - Viruses have always been a problem on desktop systems
      - Master Boot Record can be infected on NT systems by booting off of an infected floppy disk or by running a “dropper” program from a DOS session
    - NTFSDOS.exe overrides the NTFS security
    - Running Password Dump utility which generates a hashed password file then running NT Crack to create dictionary attack
      - See CIAC Bulletin H-45 at http://ciac.llnl.gov

Intrusion paths for Windows NT (continued)

- Type 1 Intrusions
  - IIS
    - Older versions of IIS tend to be buggy
      - The “..” bug
      - .BAT and .CMD files
  - Denial of Service
    - A problem with Remote Procedure Call (RPC) services causes NT to consume 100% of CPU time

Intrusion paths for Macintosh

- Shockwave is a problem on Macs also
- Most commonly used intrusion paths:
  - Unsecured network services
  - Unsecured file sharing can allow for open access to what may be private information
- Seems to have no publically known “back doors” in locked down systems
  - Mac hack contest

Intrusion paths for Novell

- The intruder is typically an insider
  - Gains physical access to the console
  - Installs sniffer or other password grabber on the local network
- Default configuration for privileged accounts is wide open
  - "Out of the box" with no passwords on accounts for
    - Supervisor
    - Admin (Netware 4.x)
    - User_Template (Netware 4.x)
- Installation of software automatically creates [Root] and [Public] directories
  - Rights are inherited on files and directories created under those directories unless blocked

Intrusion detection

- **Windows NT**
  - **Auditing and logging**
    - **User account auditing**
    - **File and directory auditing**
    - **Registry auditing**
    - **Viewing audit logs**
    - **Managing audit logs**
  - **Native tools**
  - **Third party tools**
- **Macintosh**
  - **Tools**
- **Novell**
  - **Auditing and log files**
  - **Tools**

Windows NT - Auditing and logging

- **Types of Auditing**
  - **User Account**
    - **Tracks security events and puts entries in the server's security log**
  - **File and Directory**
    - **Tracks file system events**
  - **Registry**
    - **Tracks important registry files**

Windows NT - User account auditing

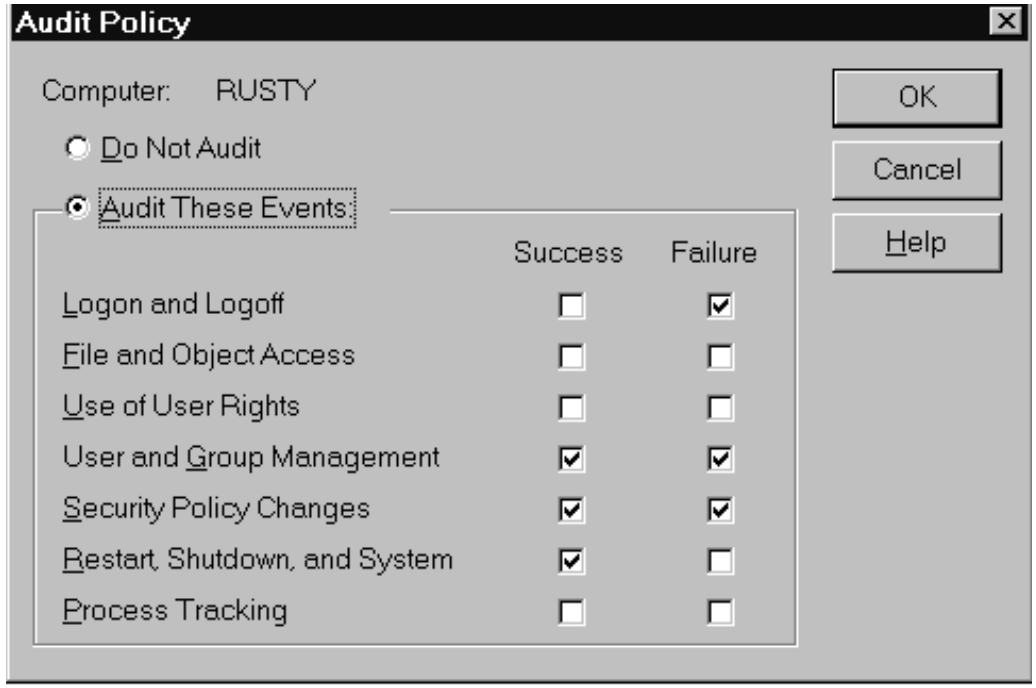
- User Manager's Audit Policy
  - What events should be audited?
    - Logon / Logoff
      - Reports users logging on or off or that have made a network connection
      - Track failures for unauthorized attempts to log on
    - File and Object Access
      - Reports user accessing a directory, file, registry, or printer
      - Track failures for attempted unauthorized access
    - User Rights
      - Reports when a user exercises a user right
      - Track failures
    - User and Group Management
      - Reports when a user account has been created or changed in some way
      - Track both successes and failures

Windows NT - User account auditing (continued)

- **Security policy changes**
  - **Reports changes to the User Rights, Audit or Trust Relationship policies**
  - **Track both successes and failures**
- **Restart, shutdown, and system**
  - **Reports when a user or an event occured to shutdown or restart the system**
  - **These events will probably not happen often, so it is safe to monitor both successes and failures**
- **Process tracking**
  - **Tracks information for events such as program activation and exits**
  - **Enable these events only when system is believed to be under attack**

Windows NT - User account auditing (continued)

- To access *Audit Policy* menu
  - Must be Administrator
  - User Manager->Policies->Audit

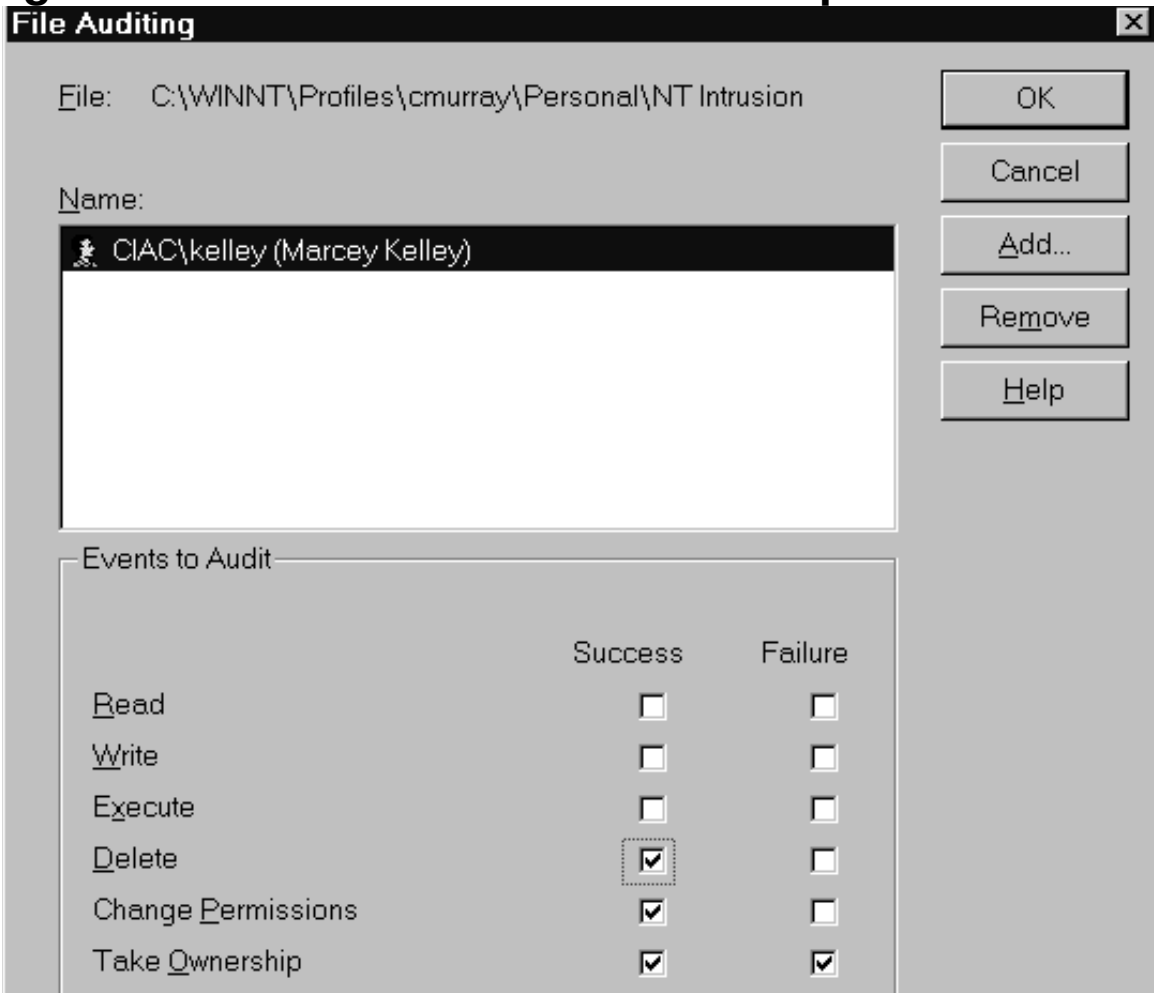


Windows NT - Directory and file auditing

- **Directory and File Auditing**
  - **Audit controls on files and directories log events only if *File and Object Access* is enabled in the User Manager's Audit Policy**
  - **Only items on logical disks formatted with NT File System (NTFS) have directory and file audit controls**
  - **NT sets audit controls on a newly created object to those of its parent directory**
  - **Types of auditable events are:**
    - **Read, Write, Execute, Delete, Change Permissions, and Take Ownership**

Windows NT - Directory and file auditing (continued)

- **To access *File Auditing* screen**
  - **Must be Administrator**
  - **Right mouse button on file icon->Properties->Security->Auditing**



Windows NT - Registry auditing

- **Some NT concepts**
  - **Windows NT Registry**
    - **A database of information replacing the INI files used in the Windows 3.x environment**
  - **Registry key**
    - **Is analogous to a directory in a file system**
  - **Registry subkeys**
    - **Are analogous to files**
  - **Rights**
    - **Privileges given to you by the system administrator**
  - **Access Control List (ACL)**
    - **A tag attached to each file or directory controlling which accounts can access the item to which the ACL is attached**
  - **Objects**
    - **All NT resources are referred to as objects**
      - **Threads, processes, files and directories**

Windows NT - Registry auditing (continued)

- Registry auditing
  - Query Value
    - System activity that attempts to read a value entry from a key
  - Set Value
    - System activity that attempts to set value entries in a key
  - Create Subkey
    - An attempt to create subkeys on a key
  - Enumerate Subkeys
    - Any event attempting to identify the subkeys of a key
  - Notify
    - Notification event from a key
  - Create Link
    - Events that attempt to create a symbolic link in a particular key

Windows NT - Registry auditing (continued)

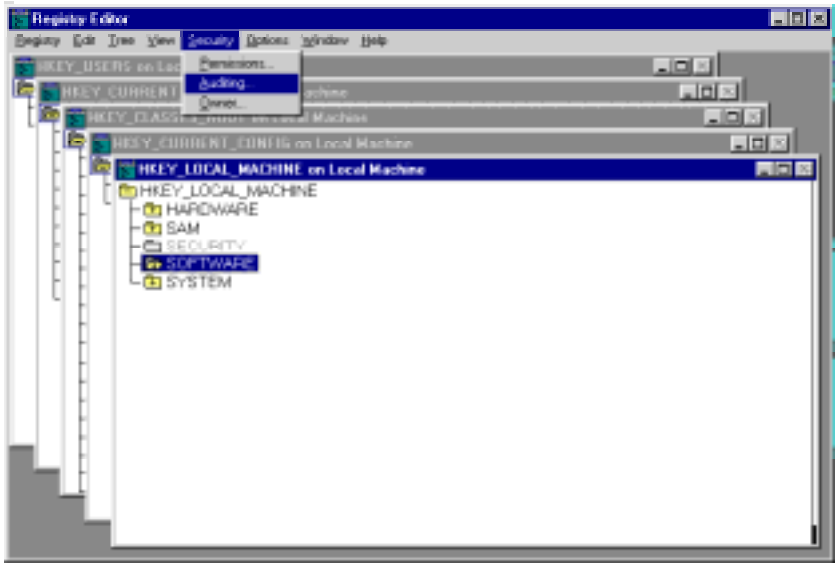
- Delete
  - Attempts to delete a key
- Write Discretionary Access Control (DAC)
  - An attempt to gain access to a key to write an ACL (assigning a permission)
- Read Control
  - Attempt to access the security assigned to a key

Windows NT - Registry auditing (continued)

- **Registry editor**
  - **Access failures are generally more valuable and far less frequent than successes**
    - **Can indicate attempt to access restricted keys**
  - **Audit controls on files and directories log events only if *File and Object Access* is enabled in the User Manager's Audit Policy**

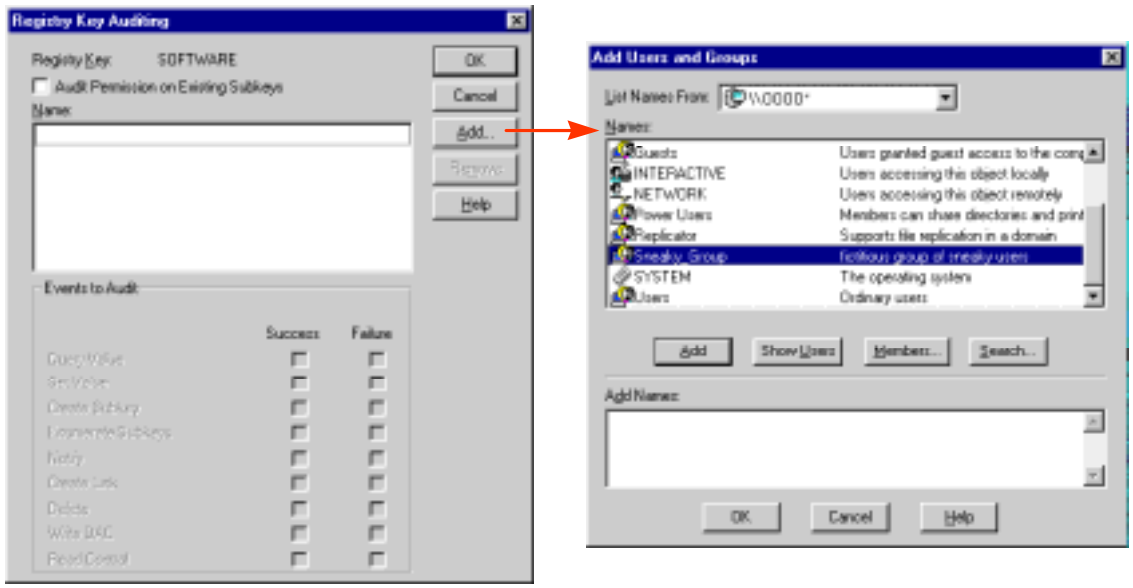
Windows NT - Registry auditing (continued)

- To start editor (REGEDT32)
  - Select Auditing in the Security Menu
  - Add users or groups you want to apply auditing to
  - Select types of events to be logged



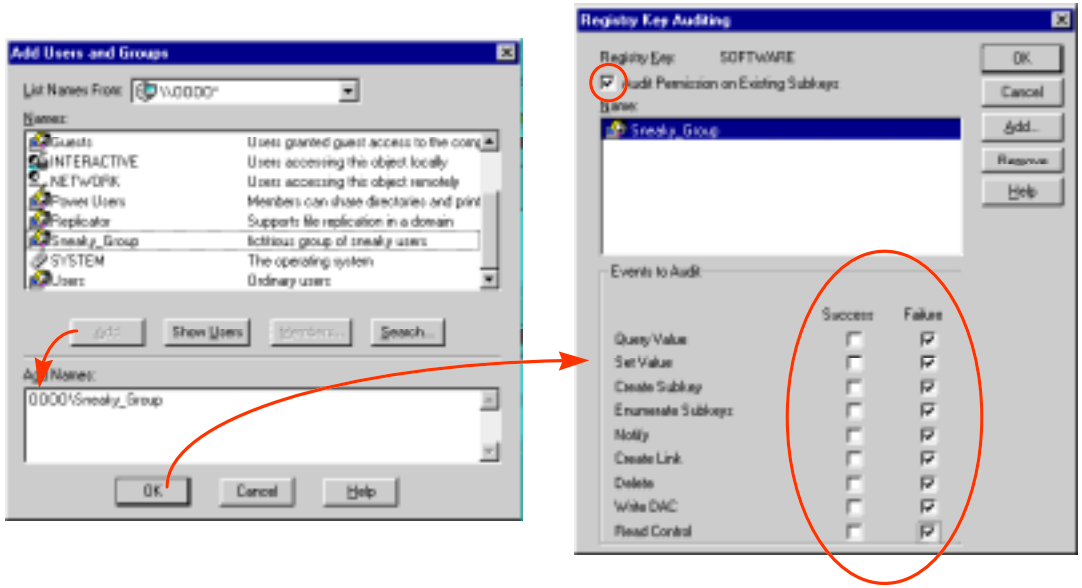
Windows NT - Registry auditing (continued)

- Carefully select groups and users for logging registry key events



Windows NT - Registry auditing (continued)

- Example of events to audit for a group of users
- Check *Audit Permission on Existing Subkeys* box to propagate auditing options to subkeys of the key selected



Windows NT - Viewing audit logs

- **Event Viewer**
  - **Can view all events, filter events, newest first, oldest first, or find a specific event**
  - **Administrative tools->Event Viewer->Log menu->Security**

Event Viewer - Security Log on \\RUSTY

Log View Options Help

Date	Time	Source	Category	Event	User	Computer
4/9/97	2:53:58 PM	Security	Logon/Logoff	538	cmurray	RUSTY
4/9/97	2:53:21 PM	Security	Logon/Logoff	538	Administrator	RUSTY
4/9/97	2:53:21 PM	Security	Logon/Logoff	528	Administrator	RUSTY
4/9/97	2:53:21 PM	Security	Logon/Logoff	528	Administrator	RUSTY
4/9/97	10:56:34 AM	Security	Logon/Logoff	528	cmurray	RUSTY
4/9/97	10:56:19 AM	Security	Logon/Logoff	538	Administrator	RUSTY
4/9/97	10:55:21 AM	Security	Logon/Logoff	538	Administrator	RUSTY
4/9/97	10:55:20 AM	Security	Logon/Logoff	528	Administrator	RUSTY
4/9/97	10:55:20 AM	Security	Logon/Logoff	528	Administrator	RUSTY
4/9/97	10:55:06 AM	Security	Logon/Logoff	529	SYSTEM	RUSTY
4/9/97	10:54:58 AM	Security	Logon/Logoff	529	SYSTEM	RUSTY
4/9/97	10:54:54 AM	Security	Logon/Logoff	538	Administrator	RUSTY
4/9/97	10:54:12 AM	Security	Policy Change	612	Administrator	RUSTY
4/9/97	10:53:17 AM	Security	Logon/Logoff	538	Administrator	RUSTY
4/9/97	10:53:17 AM	Security	Logon/Logoff	528	Administrator	RUSTY
4/9/97	10:53:16 AM	Security	Logon/Logoff	528	Administrator	RUSTY
4/7/97	9:06:33 AM	Security	Logon/Logoff	528	cmurray	RUSTY
4/2/97	4:41:26 PM	Security	Policy Change	612	Administrator	RUSTY
4/2/97	4:39:59 PM	Security	Policy Change	612	Administrator	RUSTY
4/2/97	4:38:39 PM	Security	Logon/Logoff	529	SYSTEM	RUSTY
4/2/97	4:38:33 PM	Security	Logon/Logoff	529	SYSTEM	RUSTY
4/2/97	4:36:03 PM	Security	Logon/Logoff	529	SYSTEM	RUSTY
4/2/97	4:26:59 PM	Security	Policy Change	612	Administrator	RUSTY

Windows NT - Viewing audit logs (continued)

Event Detail

Date:	4/2/97	Event ID:	529
Time:	4:36:03 PM	Source:	Security
User:	NT AUTHORITY\SYSTEM	Type:	Failure Audit
Computer:	RUSTY	Category:	Logon/Logoff

Description:

```
Logon Failure:
        Reason:                 Unknown user name or bad password
        User Name:              Administrator
        Domain:                 CIAC
        Logon Type:             2
        Logon Process:          User32
        Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
        Workstation Name:       RUSTY
```

Data: Bytes Words

Close | Previous | Next | Help

Windows NT - Managing audit logs

- Managing the audit logs
  - Base your audit selection criteria on perceived threats to your system
    - Do a threat analysis and develop auditing strategies to counter them
  - Choose Event Log settings carefully
    - Where possible, only audit failed access attempts
    - Try to audit at the directory level by placing items of high audit value in their own directory trees
  - Audit important system files
    - Registry, event log files, and user profiles are all stored in WINNT\SYSTEM32\config
  - Time and date changes
    - May want to remove the Right to change system time from Power Users

Windows NT - Managing audit logs (continued)

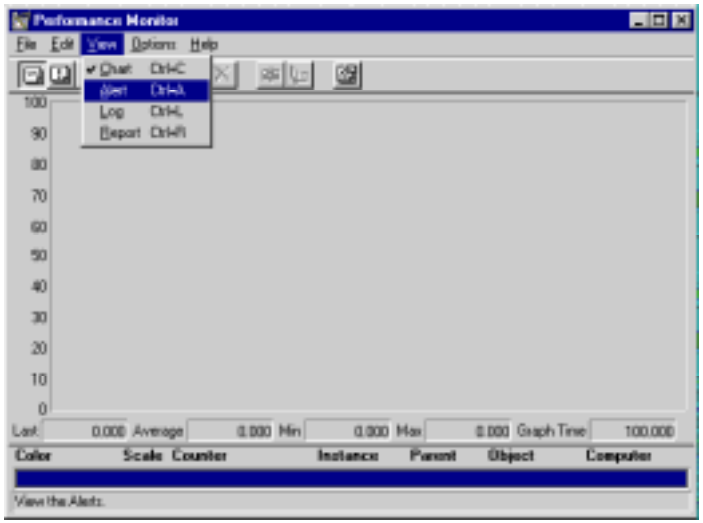
- Auditing requires planning and determining not only what needs to be monitored as well as what does not
- Target specific threats especially those you can only control by auditing
- Everything CANNOT be saved!
  - Consumes too much storage space
  - Impossible to distinguish between routine and suspicious events
- Use third party exception management tools

Native Windows NT tools - Performance Monitor

- **Performance Monitor (NT 4.0)**
  - Generates alerts when specified system values pass thresholds
  - Some values in the System category are
    - Error Access Permissions
      - Count of the number of times an attempt to open a file fails due to insufficient access permissions
    - Errors Granted Access
      - Count of the number of times attempts to access an open file fail
    - Errors Logon
      - Count of the number of failed logon attempts to the system

Native Windows NT tools - Performance Monitor (continued)

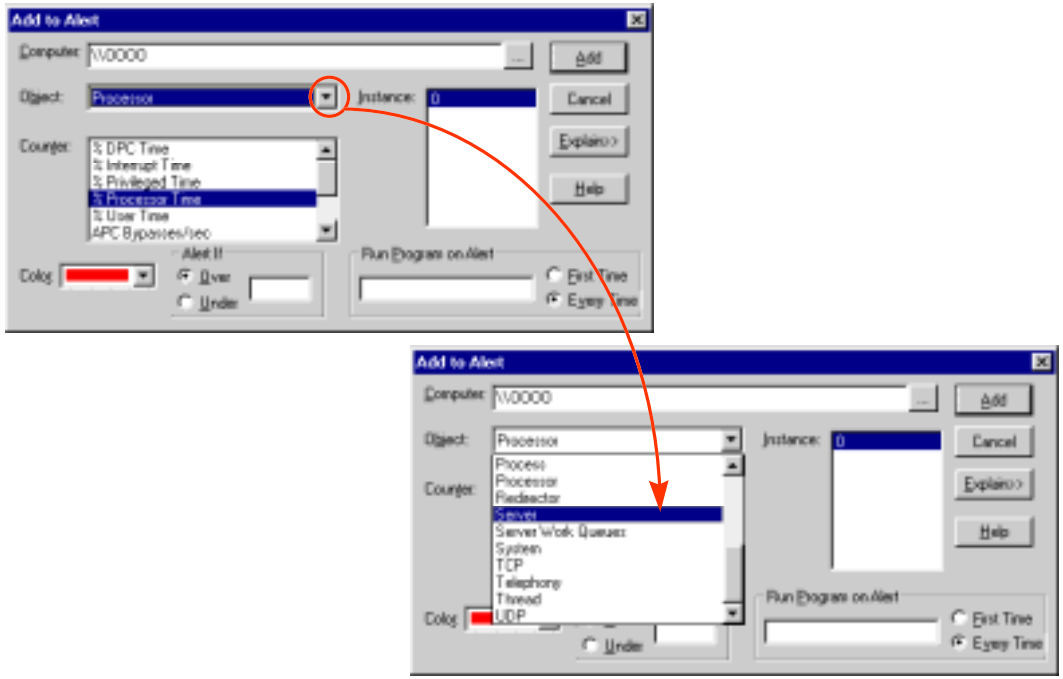
- To set an alert
  - Select Alert from the View Menu
  - Select event to be alerted
  - Set desired threshold value



Native Windows NT tools - Performance Monitor (continued)

- **Performance Monitor example**
  - **Adding an alert for specified number of failed logon attempts**
    - **Select *Add to Alert* from the Edit Menu of the Performance Monitor**
      - **Will bring up dialog box to define alerts based on system values set to be monitored**
    - **Select category of system values from which a specific value will be picked to be monitored**

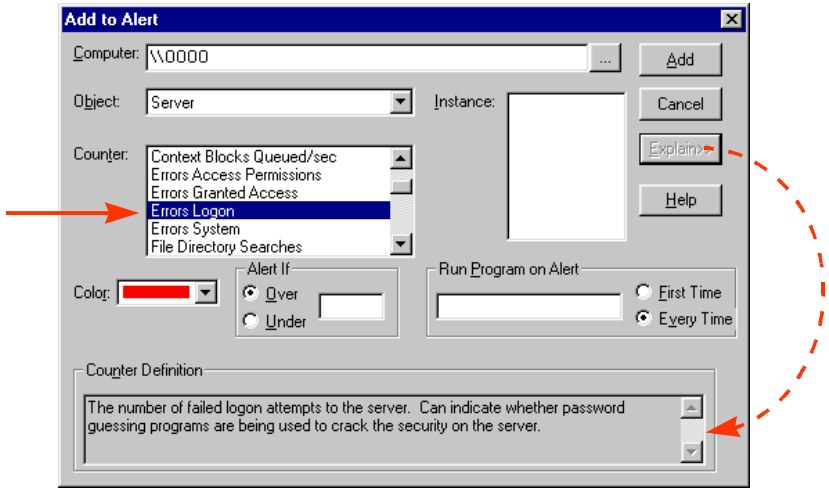
Native Windows NT tools - Performance Monitor (continued)



Native Windows NT tools - Performance Monitor (continued)

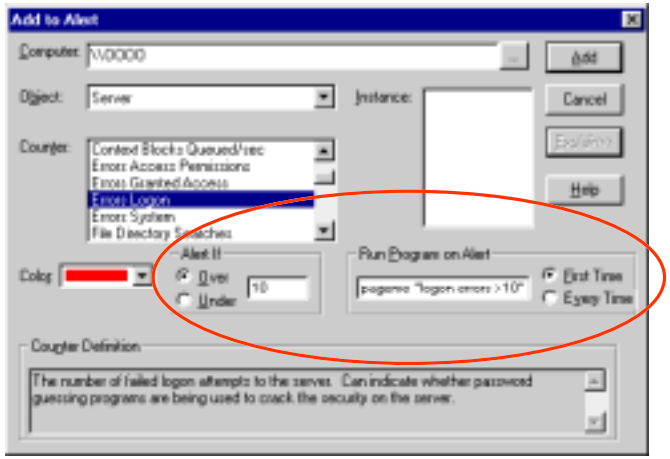
- **Explain button will provide a short explanation describing a Counter within an object**

NT 4.0 Performance Monitor Alerts



Native Windows NT tools - Performance Monitor (continued)

- Set threshold values in *Alert If* box
- To execute a command in the event of an alert
  - Specify program/command in *Run Program on Alert* box

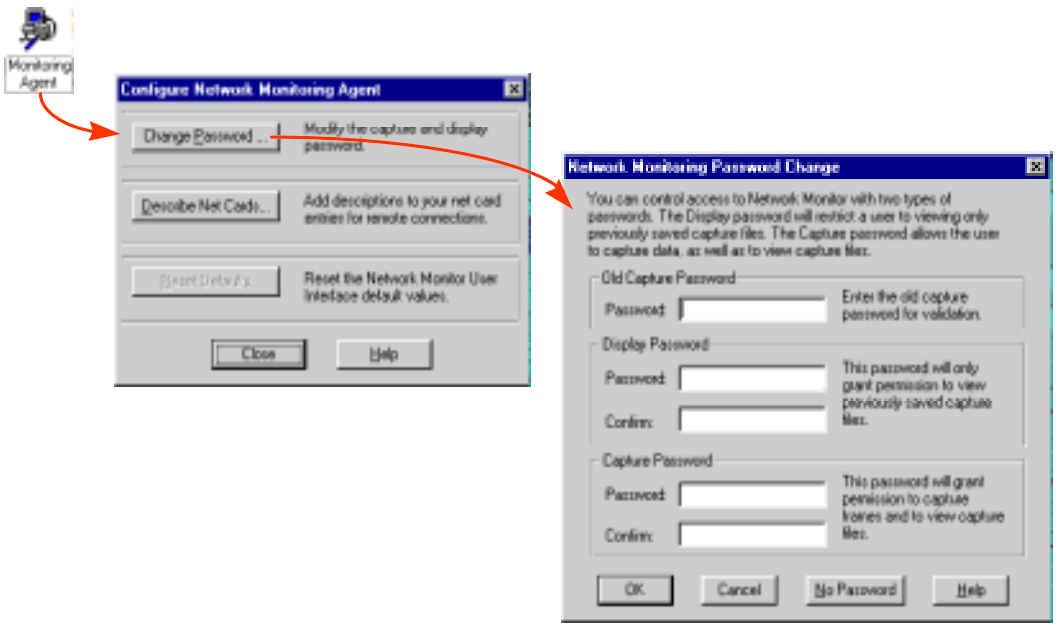


Native Windows NT tools - Network Monitor

- **Windows NT 4.0 Network Monitor**
  - **Packet sniffing program that allows authorized users to monitor traffic specific to the system where it is installed**
    - **Does not capture all network traffic on a given network segment**
  - **Can perform a variety of packet capturing tasks**
    - **May be configured to trigger execution of a command based on appearance of specific data in a packet**
    - **Using this feature, administrators can have a command executed that alerts them to suspicious packets or possible intrusive activities**

Native Windows NT tools - Network Monitor (continued)

- Access privileges to this tool should be restricted to protect against misuse
  - Need Administrator privileges
- Passwords should be set in the *Monitoring Agent Control Panel* to limit authorized users abilities
  - If no passwords are set, Network Monitor is available to all

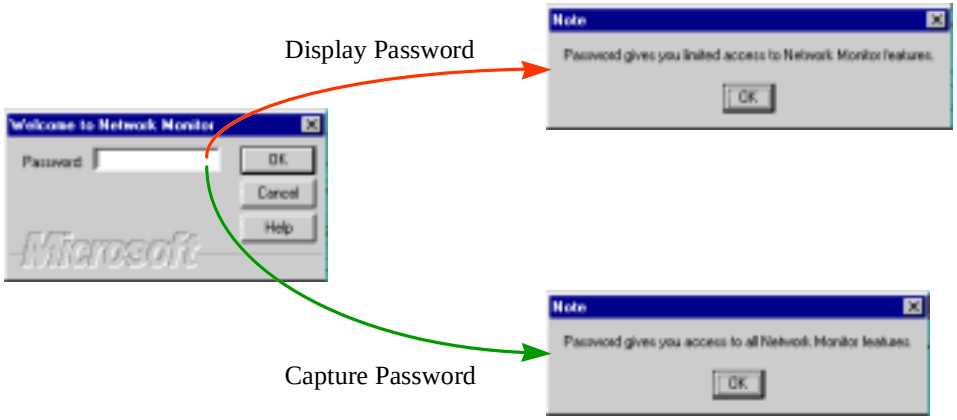


Native Windows NT tools - Network Monitor (continued)

- There are two levels of access that can be enabled
  - Display Password
    - Displays contents of a previously executed packet capture data file
  - Capture Password
    - Captures packets and stores results in a file

Native Windows NT tools - Network Monitor (continued)

- ***Display Password*** **provides limited use of the Network Monitor**
- ***Capture Password*** **enables all features of the Network Monitor**

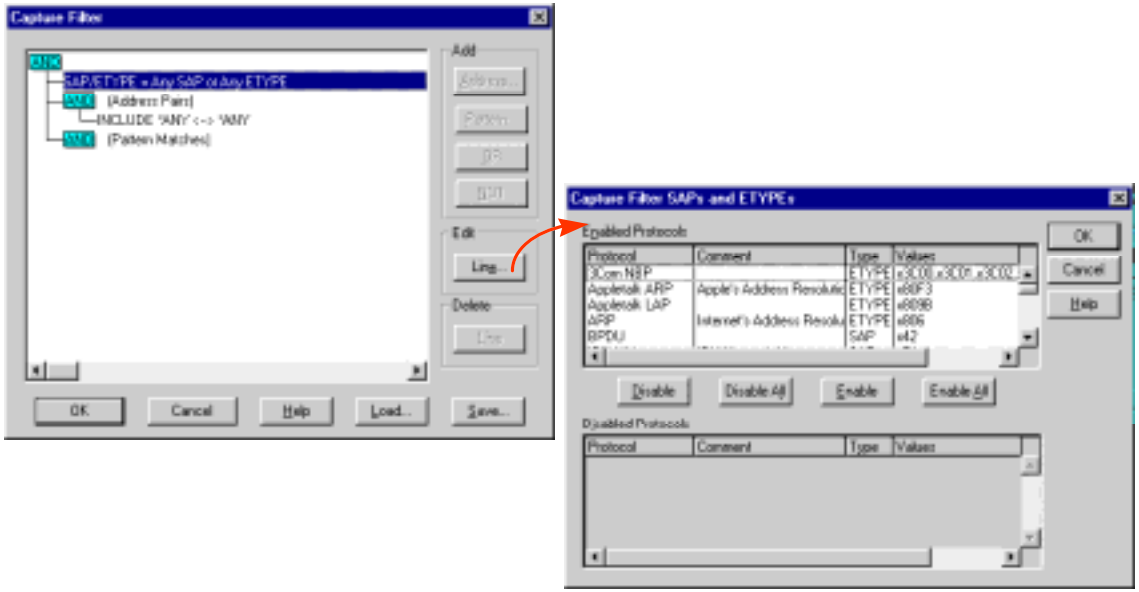


Native Windows NT tools - Network Monitor (continued)

- **Network Monitor example**
  - **Alerting to FTP (TCP port 21) connection attempts to server**
  - **Need to use *Capture Password***
  - ***Create Filter* to collect packets that are**
    - **IP protocol frames**
    - **Addresses to the target host 10.20.30.40**
    - **With a TCP destination of port 21 (0x0015 hex)**
  - **Setup trigger to report when specified connect attempts are detected**

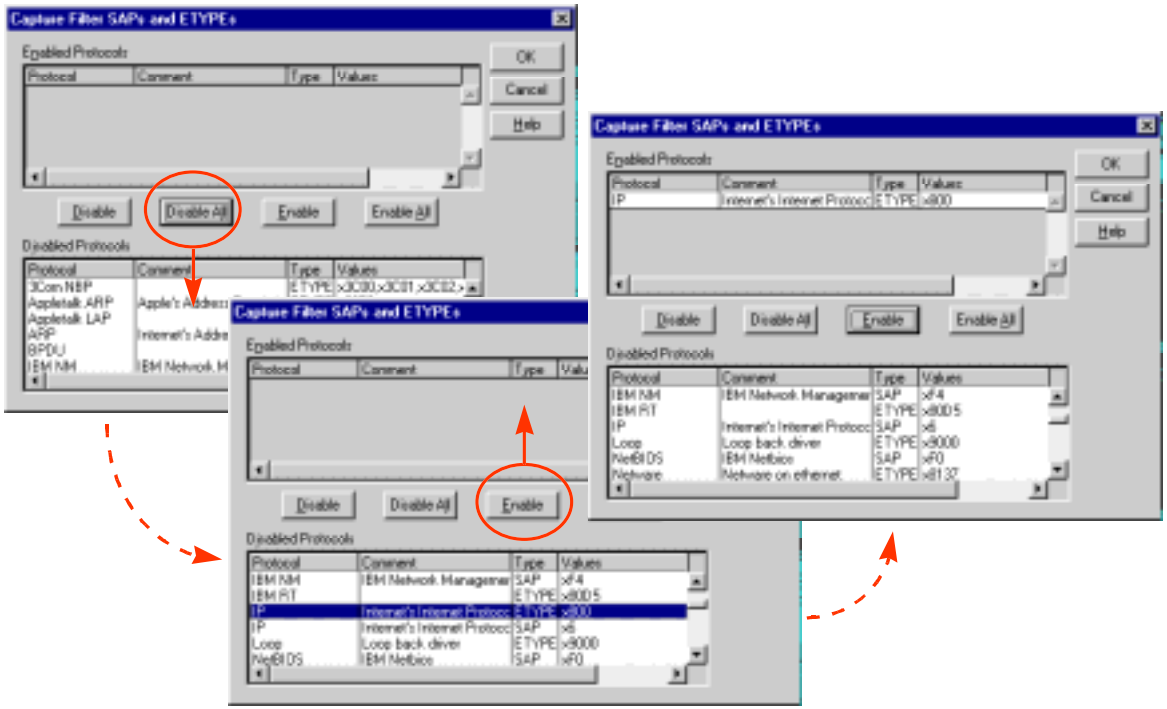
Native Windows NT tools - Network Monitor (continued)

- *Select Filter* from Capture Menu of Network Monitor main menu
  - Default settings capture of all types of packets from every location addressed to/from NT Server
  - Default restricts packet capturing to/from the NT Server that Network Monitor is running on
- Select *Edit Line* from the Capture Filter Dialog Box



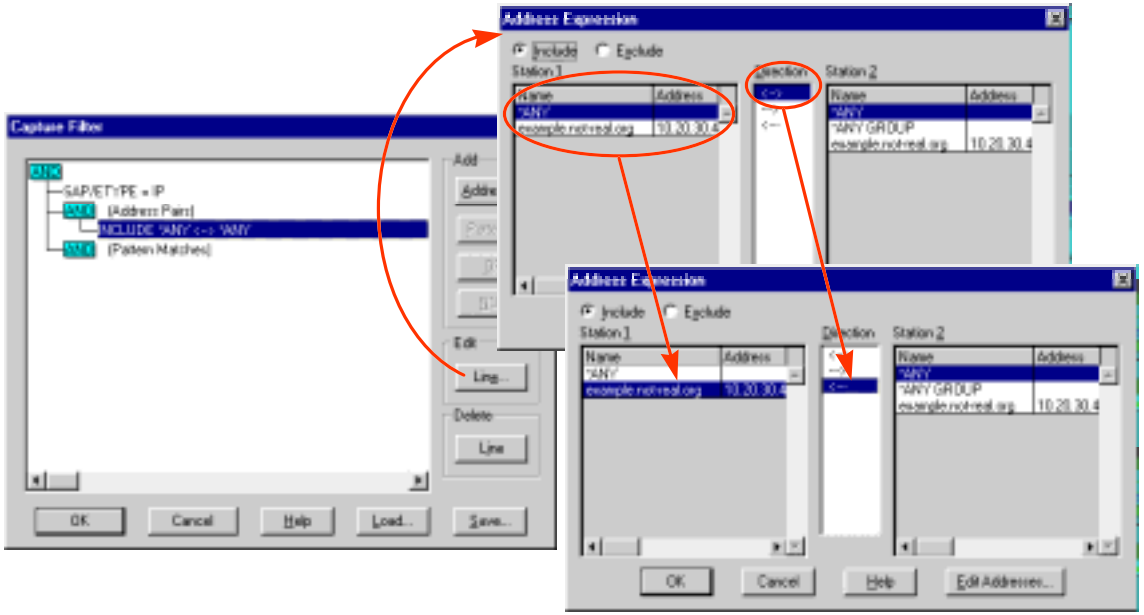
Native Windows NT tools - Network Monitor (continued)

- Capture Filter Service Access Points (SAP)s and Ethertypes (ETYPE)s show protocols that Network Monitor will recognize in the Enabled Protocols window
- To see packets that are not SAP packets
  - Disable all protocols and add back entry for IP (ETYPE)



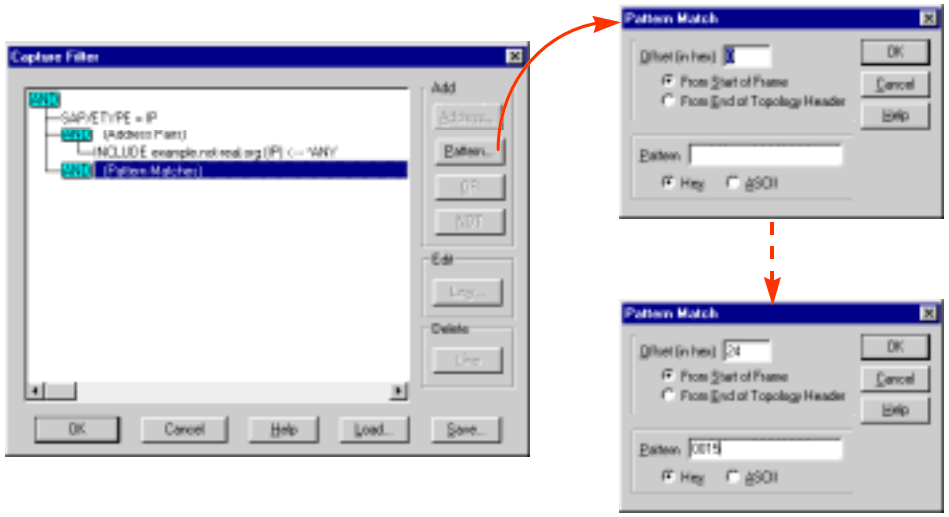
Native Windows NT tools - Network Monitor (continued)

- To include packets that arrive at example.not-real.org from any host



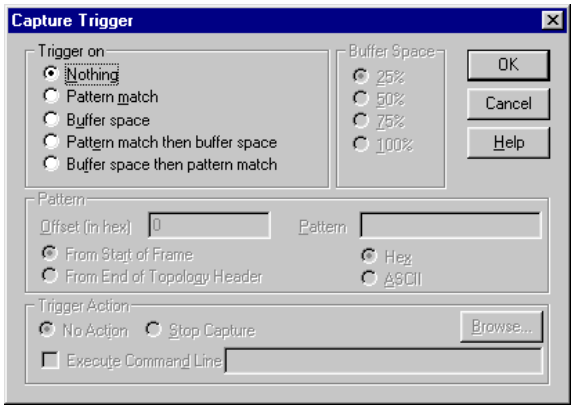
Native Windows NT tools - Network Monitor (continued)

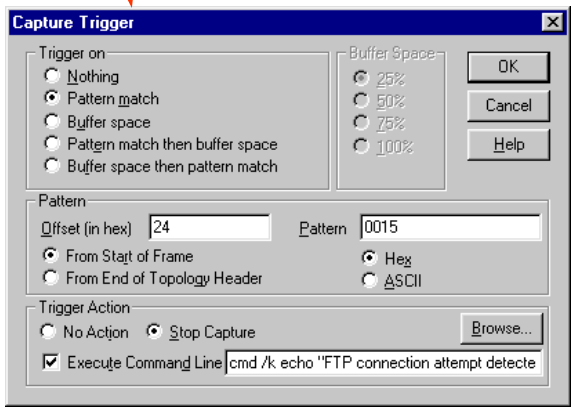
- Define the characteristic pattern in packet which represents an FTP connection request
  - Offset in IP packet of destination port is 24 (hex)
  - 16 bit value representing FTP connection is 015 (hex)



Native Windows NT tools - Network Monitor (continued)

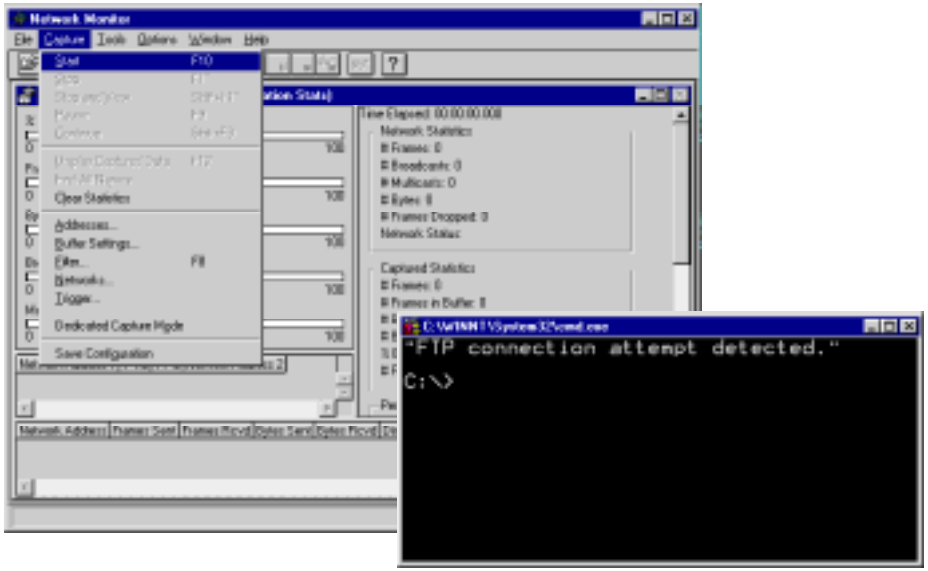
- Select *Trigger* from Capture menu of main menu
- Set pattern offset and pattern
- Trigger Action box
  - *No Action* will execute command specified for every match and continue to capture packets - BE CAREFUL
  - *Stop Capture* will stop capturing packets when match occurs





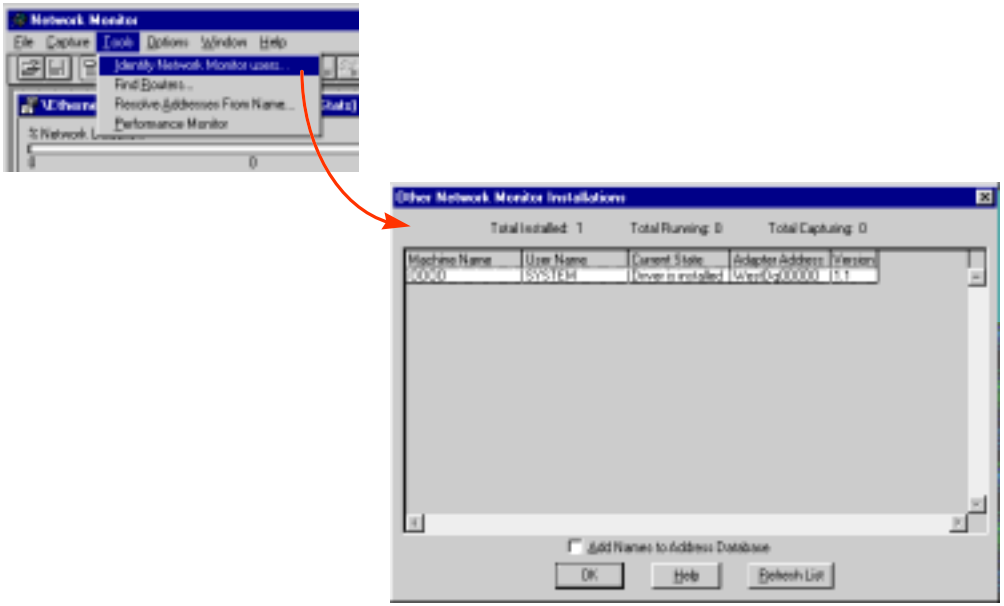
Native Windows NT tools - Network Monitor (continued)

– **Example output when capture occurs**



Native Windows NT tools - Network Monitor (continued)

- Can also identify other instances of Network Monitor running on the network



Native Windows NT tools - Password Filter

- **Password Filter (Passfilt.dll)**
  - Provides enhanced security against password guessing or dictionary attacks
  - Passwords must contain
    - More than six characters
    - A combination of alpha, numeric and non-alphanumeric characters
  - Passwords must not contain
    - Your user name or any part of your full name
  - Only available with Windows NT 4.0 Service Pack 2

Third party Windows NT tools

- **Windows NT Resource Kit**
  - **C2 Configuration Manager (C2CCONFIG.EXE)**
    - **Compares current security configuration of a Windows NT Workstation with the C2 level security requirements as defined by the National Computer Security Center (NCSC)**
  - **Crystal Reports Event Log Viewer**
    - **Full featured report writer**
      - **Allows viewing, sort/filter/group, save and print**
    - **Uses NT event logs from one or more systems**

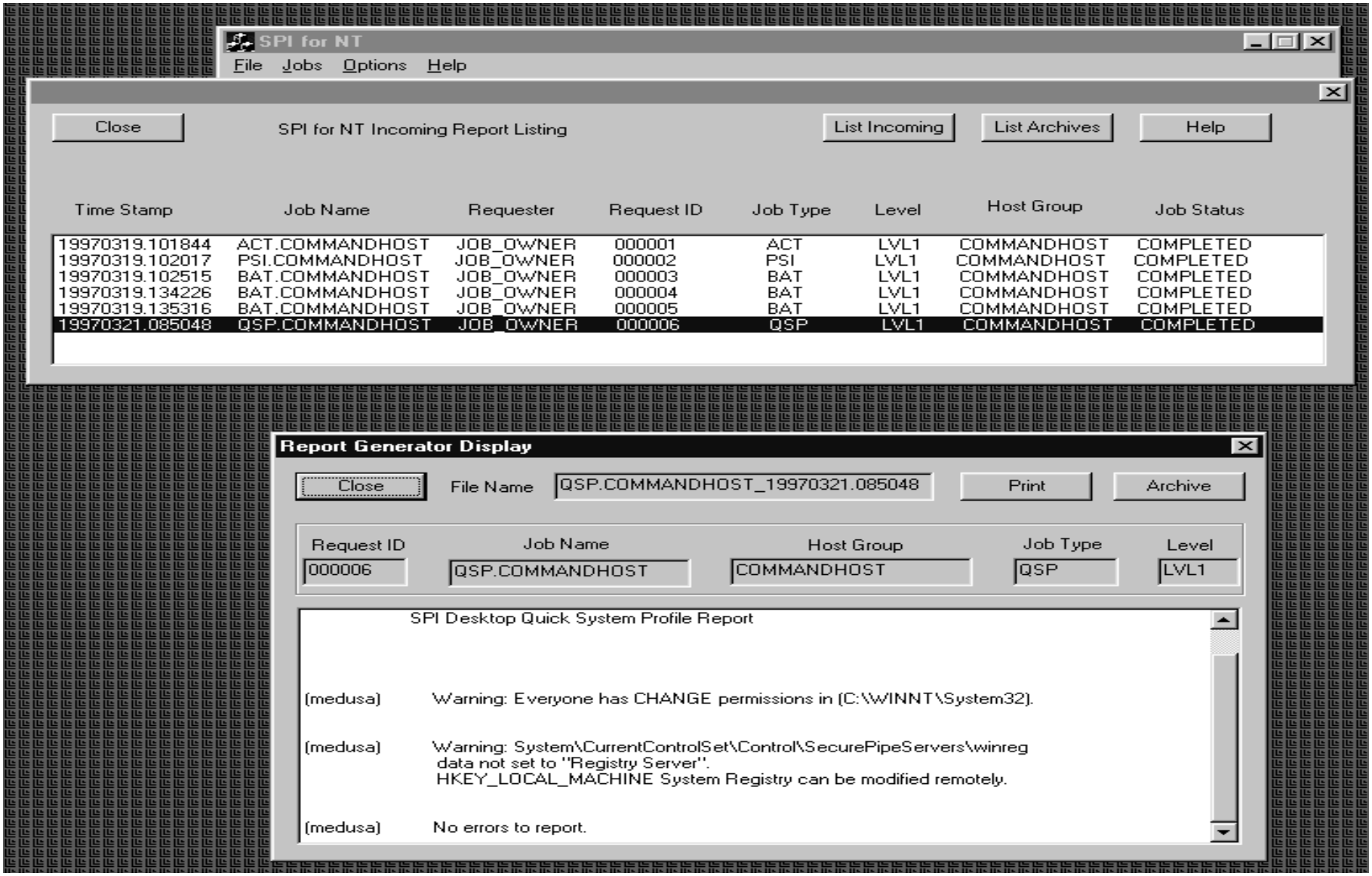
Third party Windows NT tools (continued)

- **SPI for NT**
  - **Employs a suite of five security tools:**
    - **Access Control Test (ACT)**
    - **Password Security Inspector (PSI)**
    - **Quick System Profile (QSP)**
    - **Binary Authentication Tool (BAT)**
    - **Change Detector Tool (CDT)**
  - **Hooks are included to incorporate an anti-virus tool into this package**
  - **Future releases will contain auxiliary hooks to incorporate other security tools**
  - **Available from http://ciac.llnl.gov/tools**

Third party Windows NT tools (continued)

- **QSP**
  - **Performs various checks of the system to determine vulnerabilities that exist**
  - **NT registry keys, system files and dynamically linked libraries are checked to ensure Guest group only has READ access**

SPI-NT QSP Report Example



Third party Windows NT tools (continued)

- **BAT**
  - Determines whether Service Packs need to be installed to keep system current
  - Reports if files are missing or don't match any known binary from the original distribution through the latest Service Pack
  - Binary authentication table is provided with installation
    - Table includes the filename and MD5 checksum value
    - Files that cannot be verified through a checksum may be trojaned

SPI-NT BAT Report

SPI for NT

File Jobs Options Help

Close | SPI for NT Incoming Report Listing | List Incoming | List Archives | Help

Time Stamp	Job Name	Requester	Request ID	Job Type	Level	Host Group	Job Status
19970319.101844	ACT.COMMANDHOST	JOB_OWNER	000001	ACT	LVL1	COMMANDHOST	COMPLETED
19970319.102017	PSI.COMMANDHOST	JOB_OWNER	000002	PSI	LVL1	COMMANDHOST	COMPLETED
19970319.102515	BAT.COMMANDHOST	JOB_OWNER	000003	BAT	LVL1	COMMANDHOST	COMPLETED
19970319.134226	BAT.COMMANDHOST	JOB_OWNER	000004	BAT	LVL1	COMMANDHOST	COMPLETED
19970319.135316	BAT.COMMANDHOST	JOB_OWNER	000005	BAT	LVL1	COMMANDHOST	COMPLETED

Report Generator Display

Close | File Name: BAT.COMMANDHOST_19970319.135316 | Print | Archive

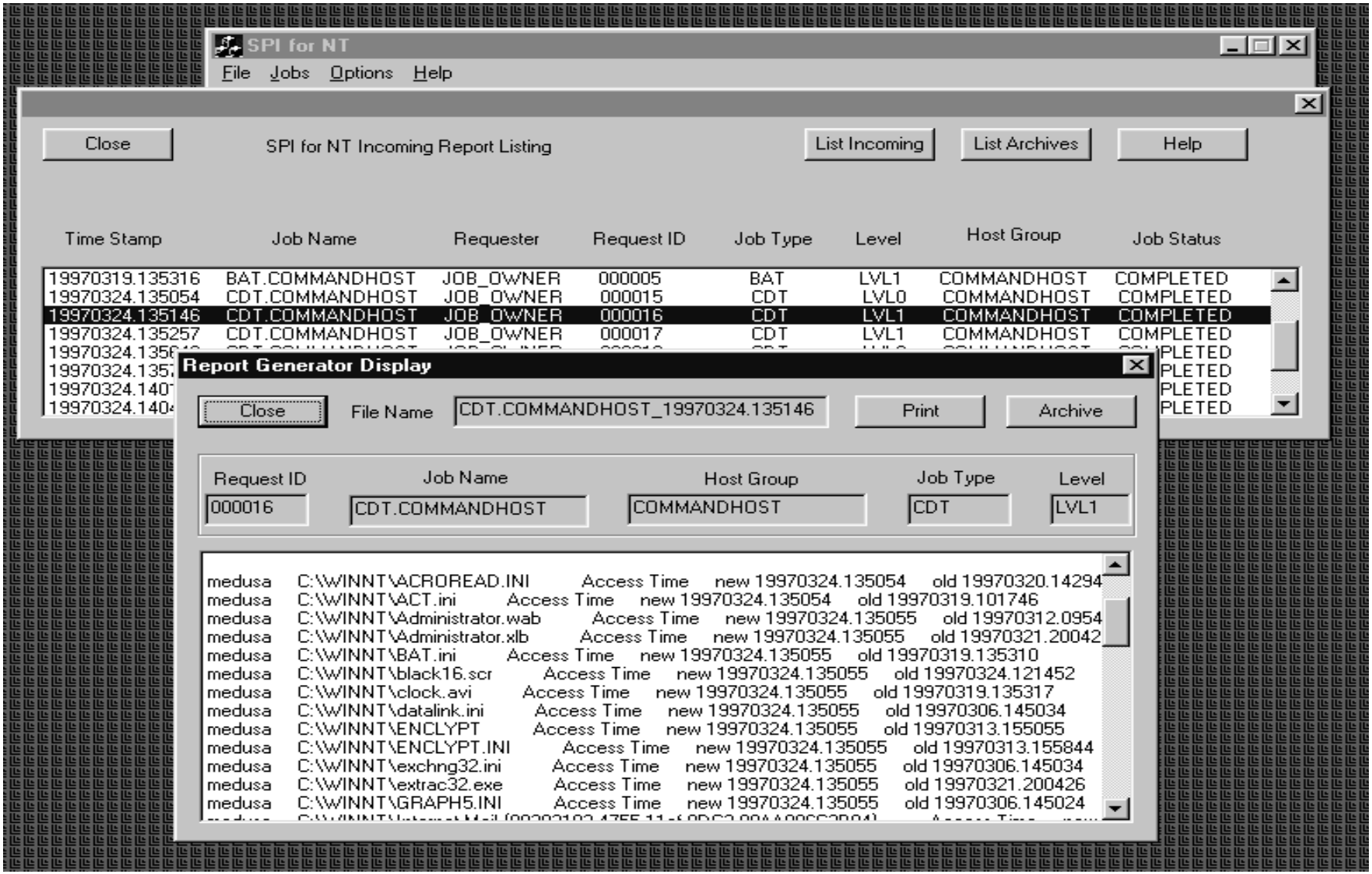
Request ID	Job Name	Host Group	Job Type	Level
000005	BAT.COMMANDHOST	COMMANDHOST	BAT	LVL1

```
Unrecognized Binaries Found

C:\WINNT\system.ini

    5685CAC9B3BA0538686FAC53EF600DF3 Current Check Sum
    EE600165C40F493305A7EE244D75FE76 Authentication Check Sum

C:\WINNT\system32\AUTOEXEC.NT

    34FD06063AEFF65D81025000B80D82F6 Current Check Sum
    85F4FB754F54014E8BF87B109E3D7589 Authentication Check Sum

C:\WINNT\system32\CONFIG.NT
```

Third party Windows NT tools (continued)

- **CDT**
  - Reports changes to a set of user selected files
  - After a “baseline” snapshot has been taken of the selected files
    - Future checks can be made to determine what files have been added, deleted or changed
  - Attributes checked to determine if files have changed
    - Owner
    - File size, mode
    - MD5 checksum
    - Checksum length
    - Permissions
    - Creation, modify, change and access time

SPI-NT CDT Report Example

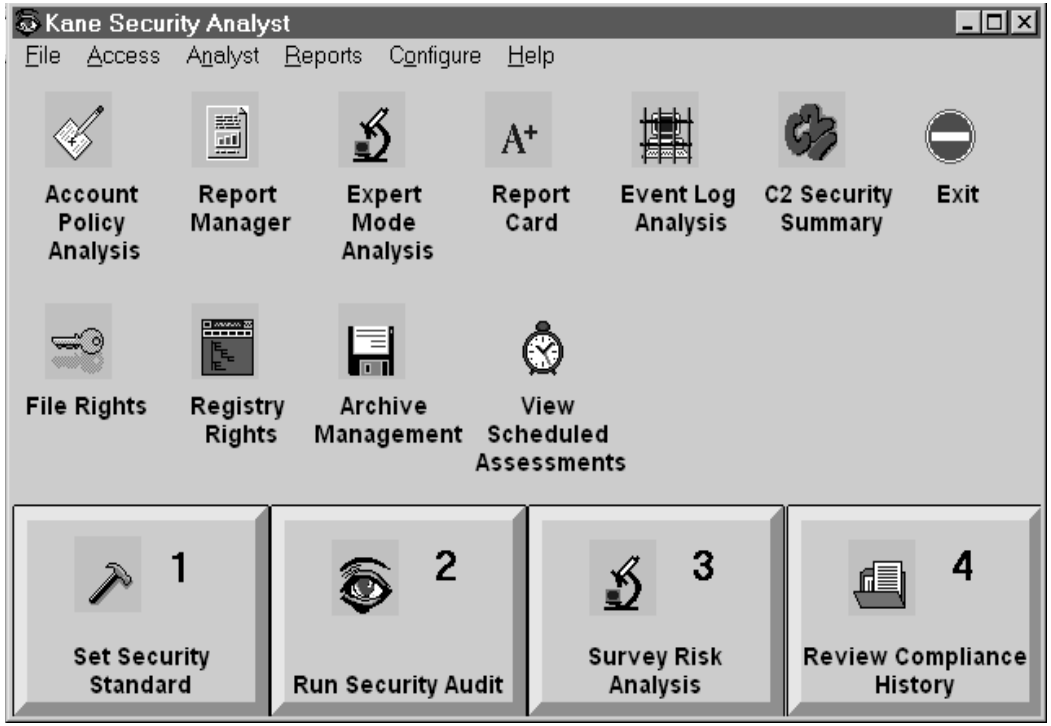


Third party Windows NT tools (continued)

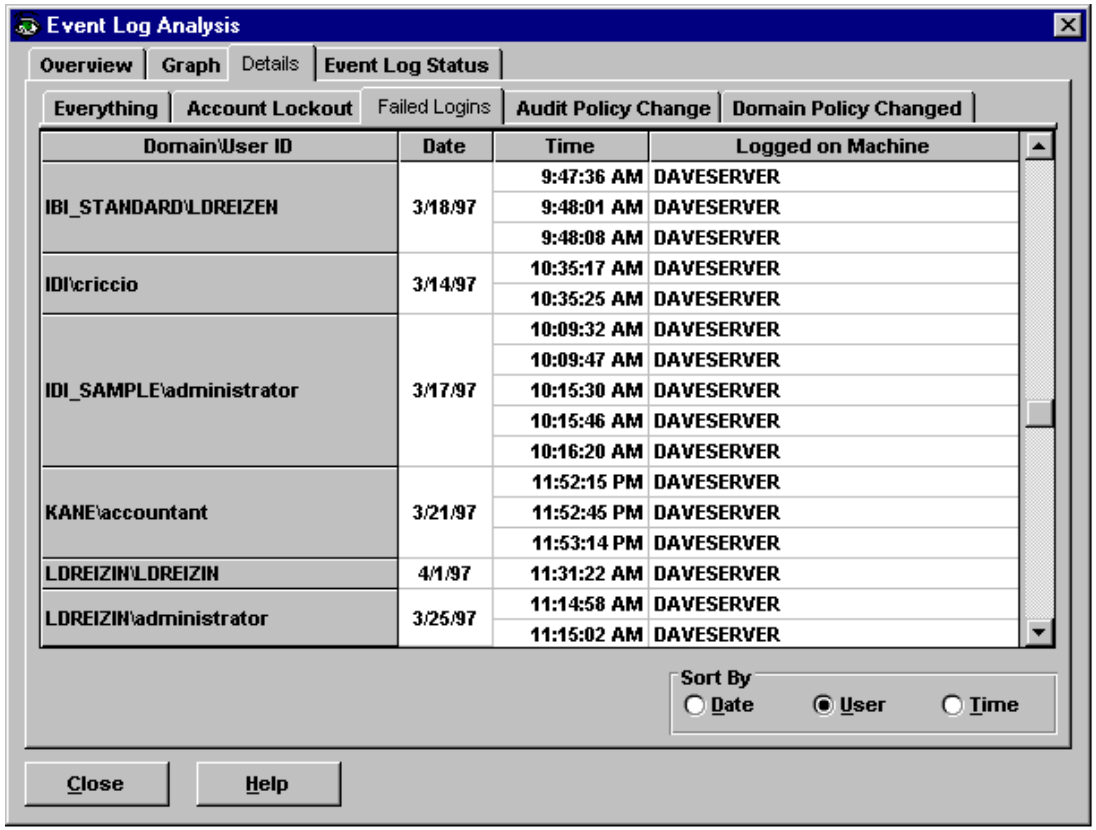
- **Kane Security Analyst**
  - Registry security settings
  - Trust relationships
  - Domain security
  - Auditing policies, Event Logs
  - Rights, permissions, and shares
  - Also available for Novell
  - Available from http://www.intrusion.com

Third party Windows NT tools (continued)

- **Kane Security Analyst**
  - Kane provides many security related functions
  - Most useful intrusion detection feature is the Event Log Analysis



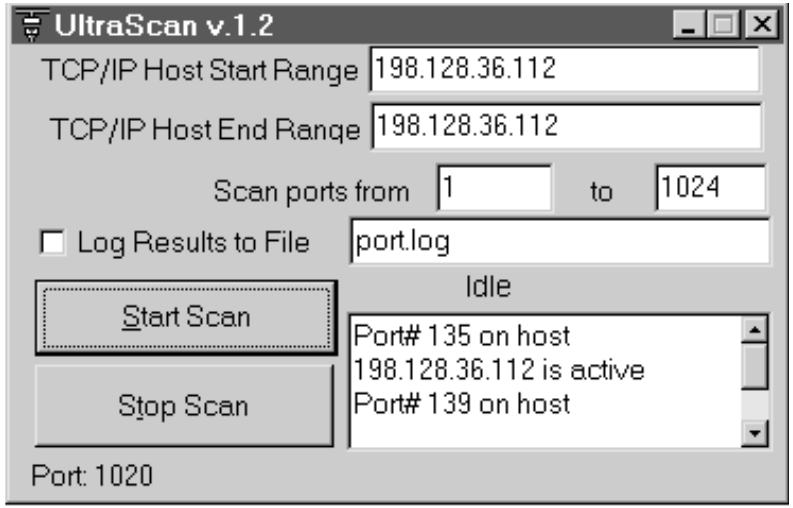
Third party Windows NT tools (continued)



Domain\User ID	Date	Time	Logged on Machine
IBI_STANDARD\LDREIZEN	3/18/97	9:47:36 AM	DAVESERVER
		9:48:01 AM	DAVESERVER
		9:48:08 AM	DAVESERVER
IDI\criccio	3/14/97	10:35:17 AM	DAVESERVER
		10:35:25 AM	DAVESERVER
IDI_SAMPLE\administrator	3/17/97	10:09:32 AM	DAVESERVER
		10:09:47 AM	DAVESERVER
		10:15:30 AM	DAVESERVER
		10:15:46 AM	DAVESERVER
		10:16:20 AM	DAVESERVER
KANE\accountant	3/21/97	11:52:15 PM	DAVESERVER
		11:52:45 PM	DAVESERVER
		11:53:14 PM	DAVESERVER
LDREIZIN\LDREIZIN	4/1/97	11:31:22 AM	DAVESERVER
LDREIZIN\administrator	3/25/97	11:14:58 AM	DAVESERVER
		11:15:02 AM	DAVESERVER

Third party Windows NT tools (continued)

- **UltraScan 1.2**
  - **Provides port status on a range of IP addresses and port numbers**
  - **Shareware**
  - **http://www.ntsecurity.net**



Third party Windows NT tools (continued)

- **NTRegmon**
  - **Displays all registry activity taking place on a Windows NT system**
  - **Advanced filtering capabilities keep log files helpful**
  - **http://www.ntsecurity.net**

NT Registry Monitor

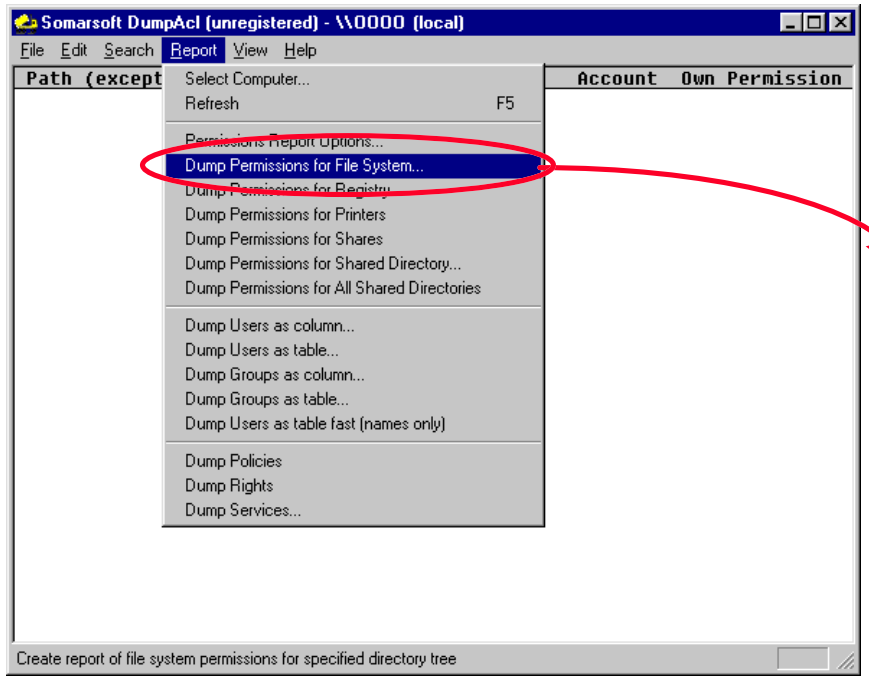
File Events Help

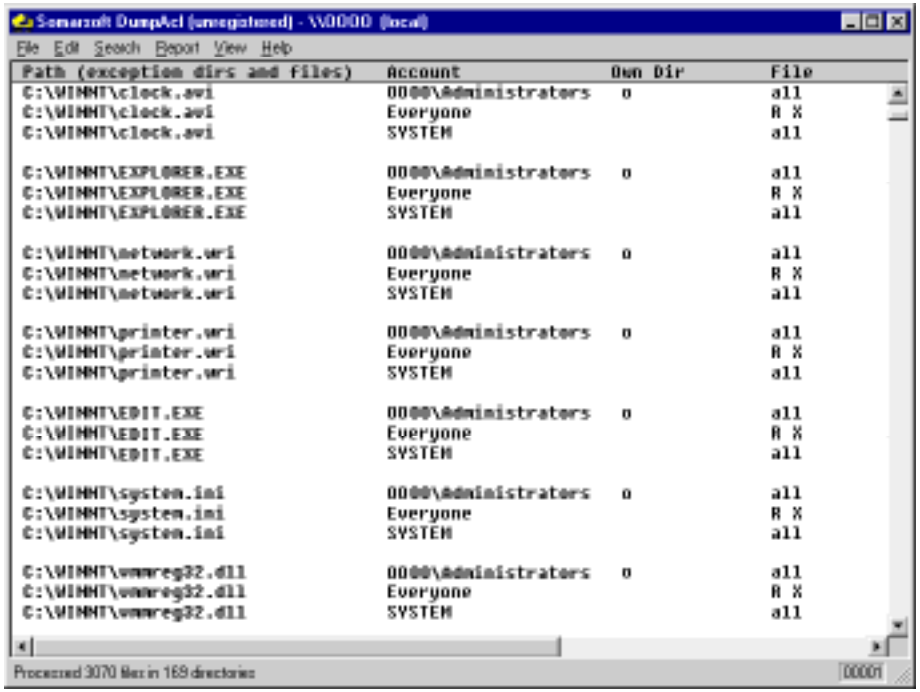
#	Process	Request	Path	Result	Other
146	calc.exe	CreateKey	USERS\S-1-5-21-1022309625-114961431-1233284464-1000\Software\Mic...	SUCCESS	Key: 0xE119CF20
147	calc.exe	OpenKey	MACHINE	SUCCESS	Key: 0xE119A200
148	calc.exe	CreateKey	MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	Key: 0xE1439880
149	calc.exe	OpenKey	USERS\S-1-5-21-1022309625-114961431-1233284464-1000\Software\Mic...	SUCCESS	Key: 0xE17B3F60
150	calc.exe	QueryValue	USERS\S-1-5-21-1022309625-114961431-1233284464-1000\Software\Mic...	NOTFOUND	
151	calc.exe	CloseKey	USERS\S-1-5-21-1022309625-114961431-1233284464-1000\Software\Mic...	SUCCESS	Key: 0xE17B3F60
152	calc.exe	QueryValue	USERS\S-1-5-21-1022309625-114961431-1233284464-1000\Software\Mic...	NOTFOUND	
153	calc.exe	OpenKey	USERS\S-1-5-21-1022309625-114961431-1233284464-1000	SUCCESS	Key: 0xE137BA20
154	calc.exe	CloseKey	USERS\S-1-5-21-1022309625-114961431-1233284464-1000	SUCCESS	Key: 0xE137BA20
155	calc.exe	OpenKey	USERS\S-1-5-21-1022309625-114961431-1233284464-1000\Control Panel...	SUCCESS	Key: 0xE137BA20
156	calc.exe	QueryValue	USERS\S-1-5-21-1022309625-114961431-1233284464-1000\Control Panel...	SUCCESS	"."
157	calc.exe	CloseKey	USERS\S-1-5-21-1022309625-114961431-1233284464-1000\Control Panel...	SUCCESS	Key: 0xE137BA20
158	perfmon.exe	OpenKey	0xE115D2C0\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib	SUCCESS	Key: 0xE137BA20
159	perfmon.exe	CloseKey	0xE115D2C0\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib	SUCCESS	Key: 0xE137BA20
160	calc.exe	CloseKey	ROOT\CLSID	SUCCESS	Key: 0xE15DFCE0
161	calc.exe	CloseKey	USERS\S-1-5-21-1022309625-114961431-1233284464-1000\Software\Mic...	SUCCESS	Key: 0xE119CF20
162	calc.exe	CloseKey	MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	Key: 0xE1439880
163	calc.exe	CloseKey	ROOT	SUCCESS	Key: 0xE13C8A20
164	calc.exe	CloseKey	USERS\S-1-5-21-1022309625-114961431-1233284464-1000	SUCCESS	Key: 0xE113D9E0
165	calc.exe	CloseKey	MACHINE	SUCCESS	Key: 0xE119A200
166	perfmon.exe	OpenKey	0xE115D2C0\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib	SUCCESS	Key: 0xE113D9E0
167	perfmon.exe	CloseKey	0xE115D2C0\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib	SUCCESS	Key: 0xE113D9E0

Third party Windows NT tools (continued)

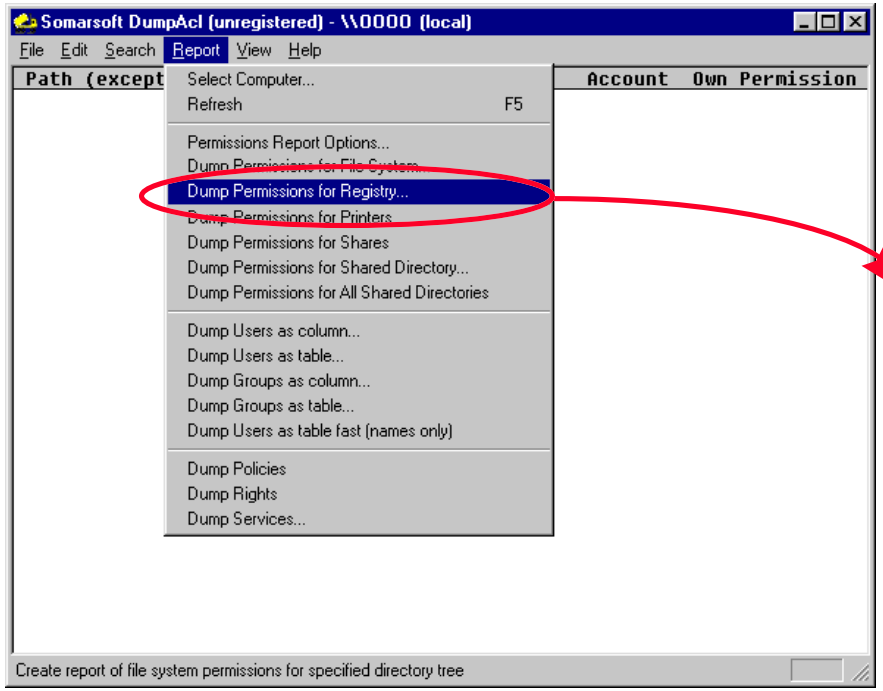
- **Somarsoft DumpACL**
  - **Provides a quick way to list information useful for system administration and security checks**
    - **Reports permissions for file system, Registry, shares, printers**
    - **Reports user/group information**
    - **Reports policies, rights, trusts, and other security information**
    - **Query capability**
    - **Reports on local and remote systems on a network**
  - **Available from http://www.somar.com**

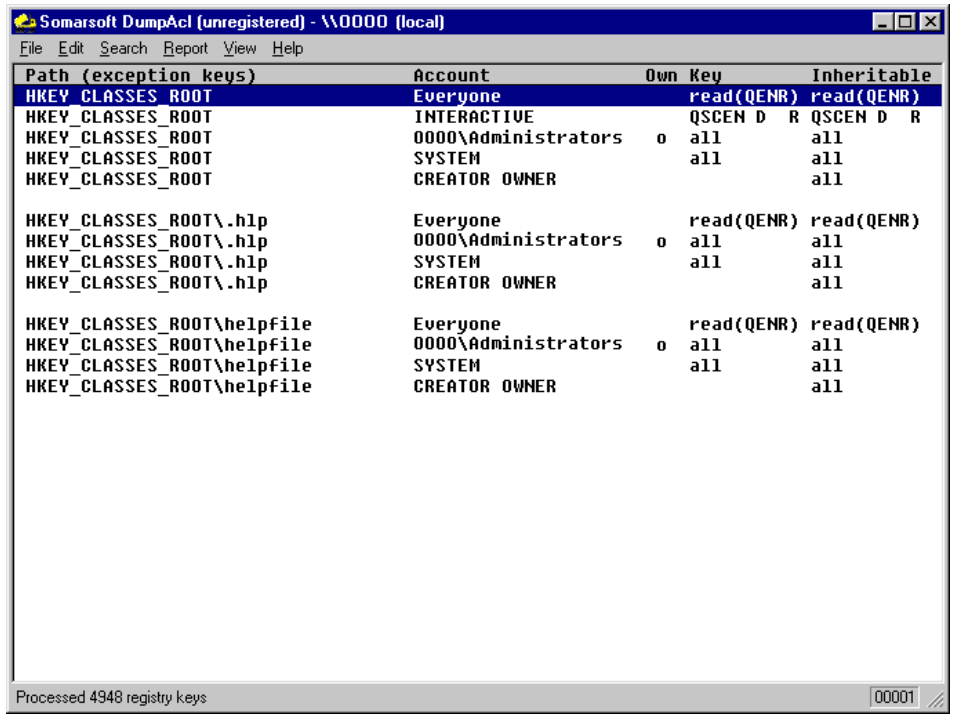
Third party Windows NT tools (continued)





Third party Windows NT tools (continued)





Third party Windows NT tools (continued)

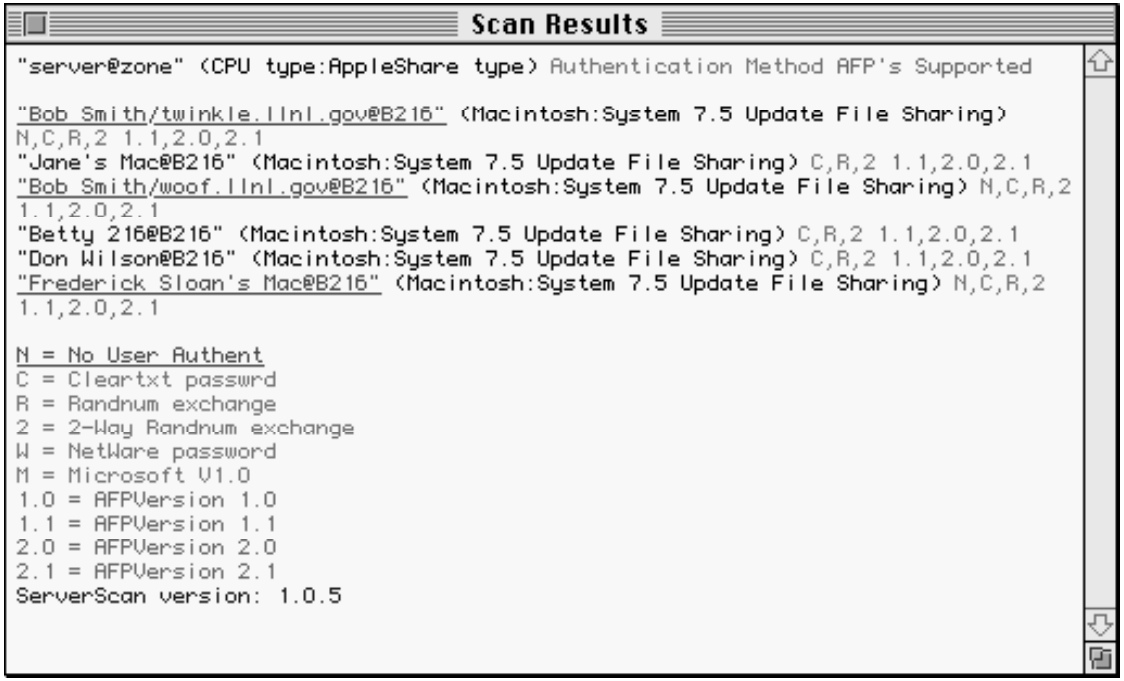
- **BindView**
  - Control domain rights permissions, and other critical system functions
  - Expose any active or potential security holes in your domains
  - Analyzes logged events on all NT machines across every domain
  - Reports across all domains without sacrificing security and regardless of trust relationships
  - Ensures that critical services and current service packs are running on all servers and workstations installed
  - http://www.bindview.com

Macintosh tools

- **Server Scan**
  - Appletalk network scanning tool
  - Scans zone(s) for Macintosh servers
  - Can be configured to crack user accounts and passwords
- **Nok Nok**
  - Control Panel that notifies, logs and limits sharing of local disks on an Appletalk network
- **Net Watchman**
  - Appletalk network scanning tool
  - Scans zone(s) for nodes and services
  - Notification of nodes appearing/disappearing
  - Visual mapping of zones, color coding alerts
  - All tools available from http://www.aggroup.com

Macintosh tools (continued)

- **ServerScan**
  - Shows a great deal of information about an Appletalk network
  - Appletalk hosts with “Guest” account enabled shown in red

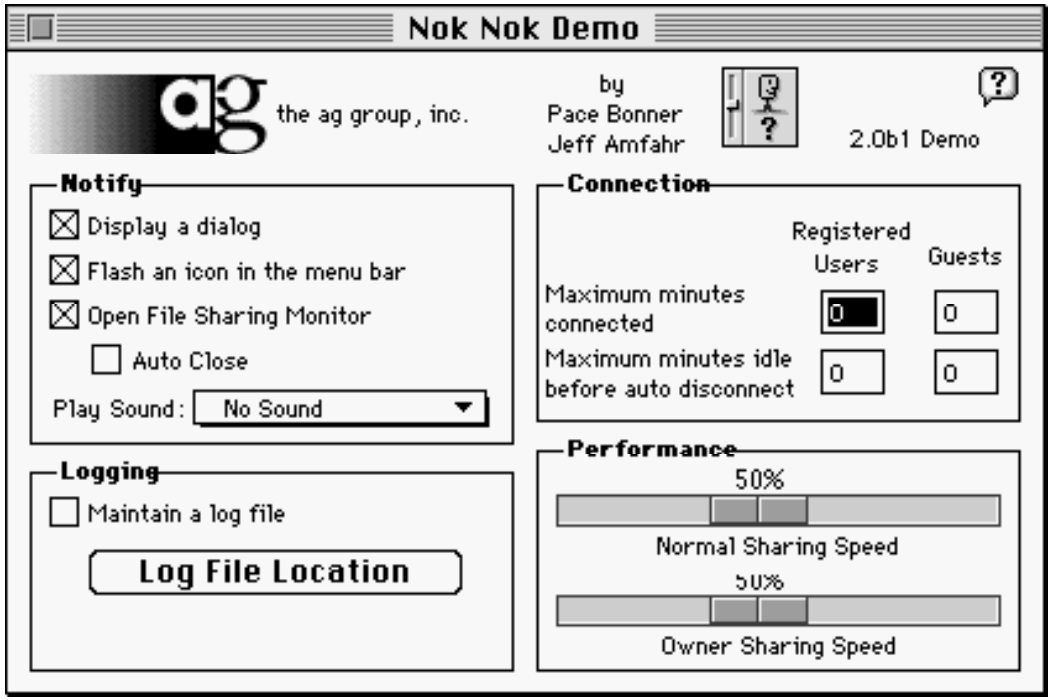


Scan Results

```
"server@zone" (CPU type:AppleShare type) Authentication Method AFP's Supported

"Bob Smith/twinkle.llnl.gov@B216" (Macintosh:System 7.5 Update File Sharing)
N,C,R,2 1.1,2.0,2.1
"Jane's Mac@B216" (Macintosh:System 7.5 Update File Sharing) C,R,2 1.1,2.0,2.1
"Bob Smith/woof.llnl.gov@B216" (Macintosh:System 7.5 Update File Sharing) N,C,R,2
1.1,2.0,2.1
"Betty 216@B216" (Macintosh:System 7.5 Update File Sharing) C,R,2 1.1,2.0,2.1
"Don Wilson@B216" (Macintosh:System 7.5 Update File Sharing) C,R,2 1.1,2.0,2.1
"Frederick Sloan's Mac@B216" (Macintosh:System 7.5 Update File Sharing) N,C,R,2
1.1,2.0,2.1

N = No User Authent
C = Cleartxt passwrd
R = Randnum exchange
2 = 2-Way Randnum exchange
W = NetWare password
M = Microsoft V1.0
1.0 = AFPVersion 1.0
1.1 = AFPVersion 1.1
2.0 = AFPVersion 2.0
2.1 = AFPVersion 2.1
ServerScan version: 1.0.5
```

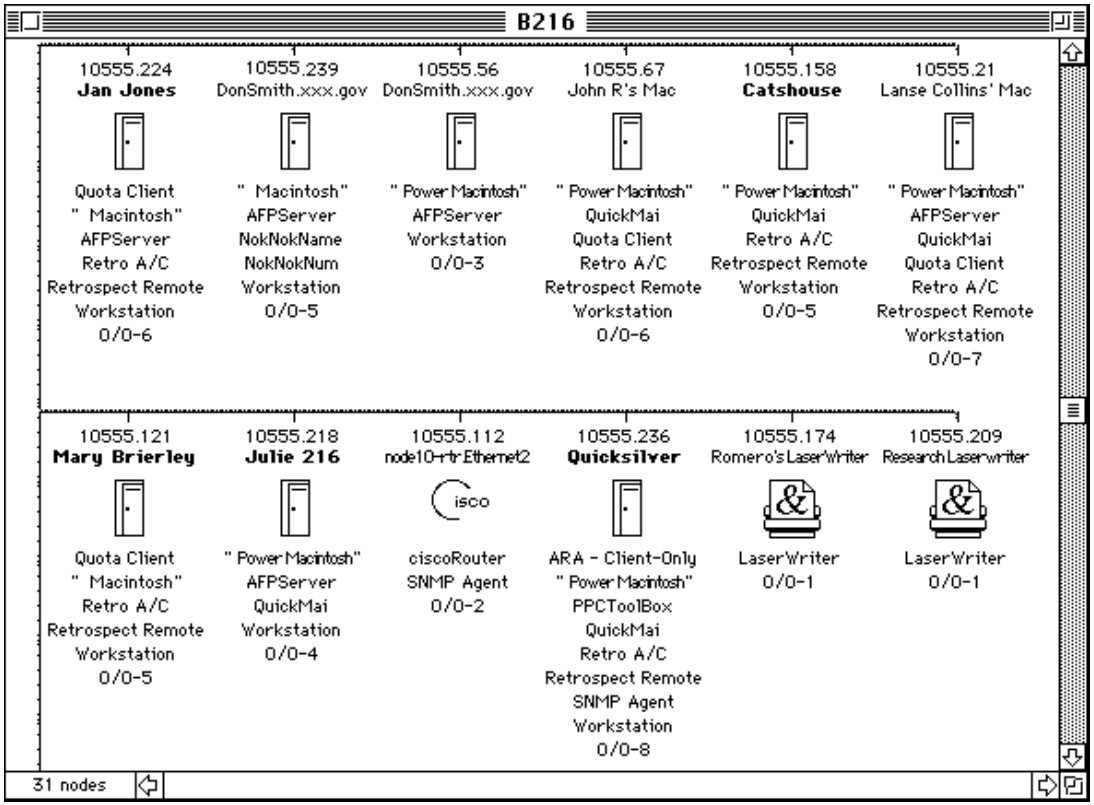
Macintosh tools (continued)

- **Nok Nok**
  - **Control Panel that notifies, logs and limits sharing of local disks on an Appletalk network.**



Macintosh tools (continued)

- **Net Watchman**
  - –Appletalk network mapping and change notification tool
  - –Notification of nodes appearing/disappearing
  - –Visual mapping of zones, color coding alerts



Novell important file information

- **Most important files**
  - **are located in SYS:_Netware directory (including bindery files).**
- **Other important directories**
  - **SYS:SYSTEM, SYS:PUBLIC, SYS:LOGIN**
- **Netware 3.x password and security files**
  - **located in SYS:SYSTEM directory. (NET$OBJ.SYS, NET$VAL.SYS, NET$PROP.SYS)**
- **Netware 4.x login names/password files**
  - **in SYS:_Netware: (PARTITION.NDS, BLOCK.NDS, ENTRY.NDS, VALUE.NDS)**

Novell log files

- The audit files are NET$AUDT.*; usually located in SYS:_Netware directory
  - auditing can be turned on or off
  - can be configured to capture log-in activity
- Novell's Accounting Feature"on"
  - Records changes in files such as
    - deleting
    - adding
    - other footprints
  - provides details to auditing files
- File Server Error log periodically
  - shows system downs, reboots, new system installations

Third party Novell tools

- **AUDIT**
  - for Netware 3.1x
  - Audit file analysis tool: filters important information
- **LOGIT**
  - Log chosen network events
- **EXPIRED**
  - search for unused (or expired) accounts
- **NECSEC**
  - check for bad or no passwords
- **http://www.best.com/~dmadden**

Native Novell tools

- CHKNULL.EXE
  - check for bad or no passwords
- Intrusion detection property
  - Password guessing alert-notifys sys admin when someone is guessing passwords
  - can be set to lock account when guessing is detected
- GRPLIST.EXE
  - Network configuration analyzers for weak or default accounts such as “guest”
- USERLST
  - Check for new/mysterious users
  - check privileges (especially supervisor)
- Bindfix
  - Checks for unaccounted changes in rights or privileges for users and container objects

Resources

- Books
- Websites
- Newsgroups

Books

- **Security Audit and Control**
  - Microsoft Press
- **Windows NT Security Handbook**
  - Tom Sheldon
  - Osborne McGraw-Hill
- **Windows NT Server 4.0 Professional Reference**
  - Karanjit Siyan
  - New Riders
- **The Complete Guide to Netware 4.1**
  - James Gaskin
  - Network Press
- **Novell's Netware Administrator's Handbook**
  - Kelley J.P. Lindberg
  - Sybex, Novell Press

Websites

- NT resources
  - Microsoft - http://www.microsoft.com
    - tools
    - knowledge base
  - NT Security - http://www.ntsecurity.net
  - NT FAQ - http://www.it.kth.se/~rom/ntsec.html
- Mac and NT resources
  - http://www.aggroup.com
  - http://www.macintouch.com
  - http://www.MacWEEK.com
- Novell resources
  - http://www.novell.com
  - http://www.best.com/~dmadden

Newsgroups

- **NT Bugtraq**
  - **e-mail to: listserver@rc.on.ca**
  - **in body of message: subscribe ntbugtraq <yourName>**
- **NT Security**
  - **e-mail to: majordomo@iss.net**
  - **in body of message: subscribe ntsecurity**
  - **for digest version: subscribe ntsecurity-digest**