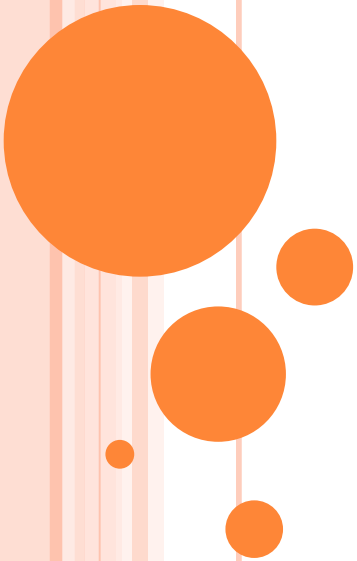


INVESTIGATING WINDOWS ENVIRONMENT---PART 4

CONDUCTING A WINDOWS INVESTIGATION.

- Review all pertinent logs.
- Perform keyword searches.
- Review relevant files.
- **Identify unauthorized user accounts or groups.**
- Identify rogue processes and services.
- Look for unusual or hidden files/directories.
- Check for unauthorized access points.
- Examine jobs run by the Scheduler service.
- Analyze trust relationships.
- Review security identifiers.

HANDLING UNAUTHORIZED USER ACCOUNTS OR GROUPS

- Use ***usrstat*** from the NTRK to view all domain accounts on a domain controller.

- Examine the **Security log** using Event Viewer

  Check for following event id's :

  - Id 632(adding new account)
  - Id626(user account enabled)
  - Id 636(changing account group)
  - Id 642(user account changed)

- Check for profiles directory

  Path *user account \ %systemroot% \ Profiles*

- If user acc **exits** and directory **not found** then **no user account has log on yet.**

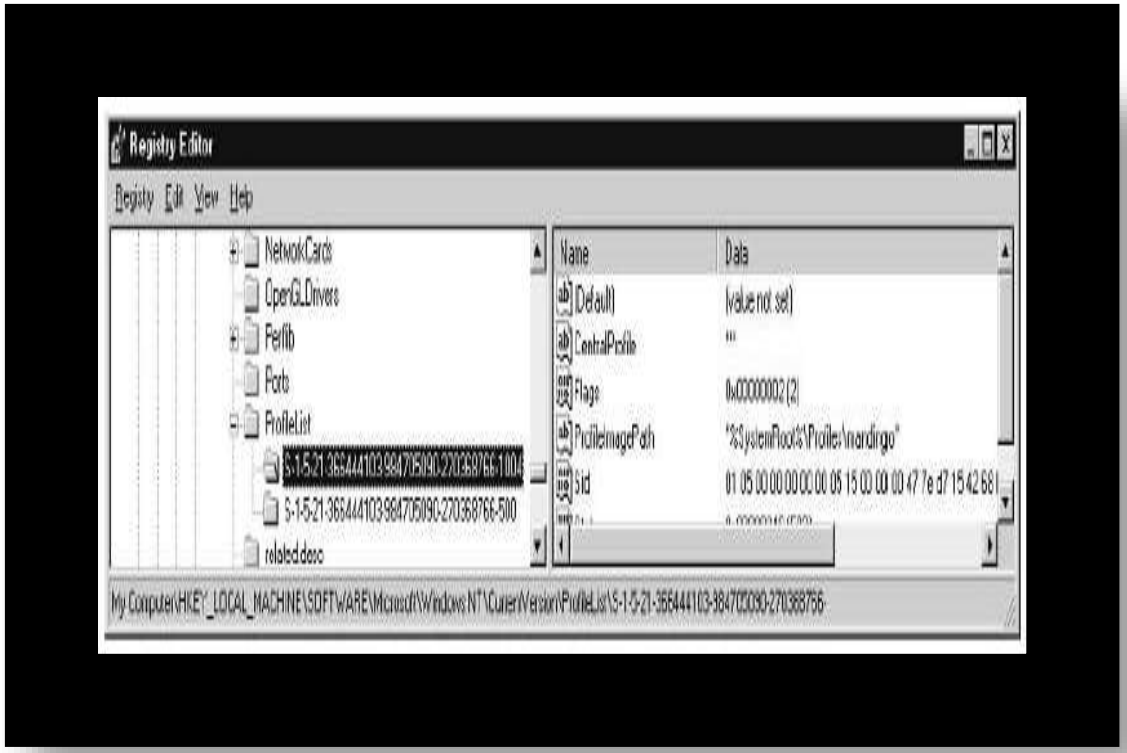
- **If** directory **found** and user account not listed in *Account \ Users \ Names* then user id exists at one time but no longer exists.

- Review SID's

- When a user account is deleted, respective Profile directory entry is **not** deleted, and the respective SID will **remain** in the Registry.

- ***Path*** *Microsoft \ Windows NT \ CurrentVersion \ ProfileList*

This allows you to trace which user IDs have been deleted over the course of a system's life.



CONDUCTING A WINDOWS INVESTIGATION.

- Review all pertinent logs.
- Perform keyword searches.
- Review relevant files.
- Identify unauthorized user accounts or groups.
- **Identify rogue processes and services.**
- Look for unusual or hidden files/directories.
- Check for unauthorized access points.
- Examine jobs run by the Scheduler service.
- Analyze trust relationships.
- Review security identifiers.

Identifying Rogue Processes

- Rogue means dishonest or spam
- Key is to run the most up-to-date virus scanner on the whole logical volume of evidence
- An excellent tool that identifies trojans, backdoors, keystroke loggers, and other "malware" is **PestPatrol**

CONDUCTING A WINDOWS INVESTIGATION.

- Review all pertinent logs.
- Perform keyword searches.
- Review relevant files.
- Identify unauthorized user accounts or groups.
- Identify rogue processes and services.
- **Look for unusual or hidden files/directories.**
- Check for unauthorized access points.
- Examine jobs run by the Scheduler service.
- Analyze trust relationships.
- Review security identifiers.

Looking for Unusual or Hidden Files

NEED

- Once an insider chooses to perform unauthorized or unacceptable deeds on his system, he may choose to make a few files “invisible.”

METHODS USED

- NTFS file streams can be used to hide data behind legitimate files
- Also to store multiple instances of file data under one file entry.
- These multiple data streams may be used to hide data as Windows Explorer does not indicate the presence of the additional streams.

IDEA TO HANDLE

HIDE THE FORENSIC TOOLS

- Netcat (nc.exe) can be hidden in a secondary data stream of a file called **logo.jpg** by using command

  cp nc.exe logo.jpg:nc.exe

- the nc.exe within the **logo.jpg** file entry is not reflected by the file size, but the time/date stamp is altered.

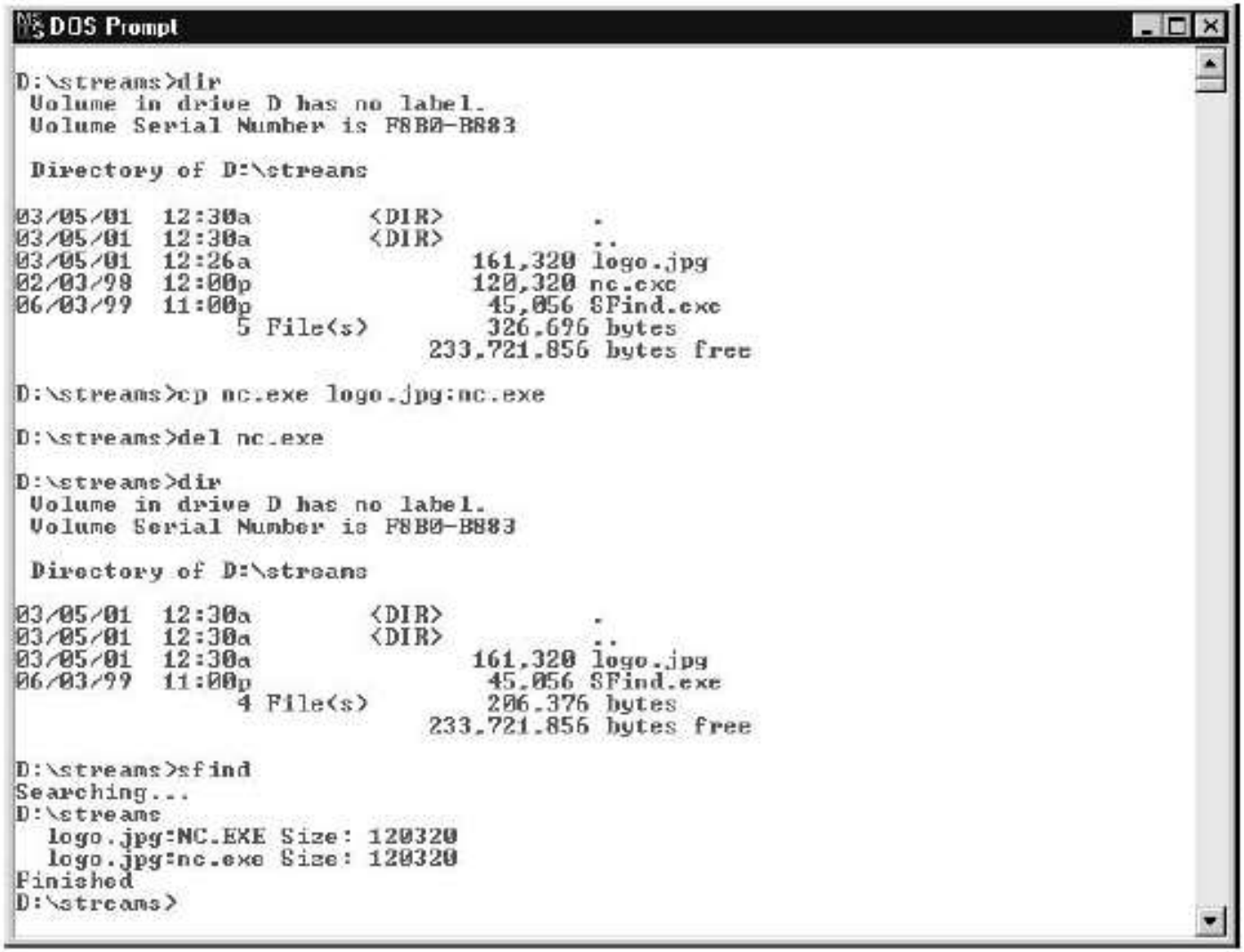


Figure 12-12. Using streams to hide a file

Other methods

- Changing the file extension or creatively naming the files to match those of important system files.

- This method can fool some popular automated forensic tools.

CONDUCTING A WINDOWS INVESTIGATION.

- Review all pertinent logs.
- Perform keyword searches.
- Review relevant files.
- Identify unauthorized user accounts or groups.
- Identify rogue processes and services.
- Look for unusual orhidden files/directories.
- **Check for unauthorized access points.**
- Examine jobs run by the Scheduler service.
- Analyze trust relationships.
- Review security identifiers.

Checking for Unauthorized Access Points

- **WHAT IS UNAUTHORISED ACCESS**
- Any service that allows some degree of remote access, could provide an entry point to unwanted intruders.

SERVICES INCLUDE

- Terminal server
- SQL/Oracle
- Third-party telnet daemons on Windows NT
- Windows 2000 Telnet Server
- Third-party FTP daemons
- Web servers (such as Apache and IIS)
- Virtual network computing (TCP port 5800) and PC Anywhere (TCP port 5631)
- Remote-access services (PPP and PPTP)
- X Servers

TOOLS USED

- **netstat**
- **Fport**

PURPOSE

- They use API calls to read the contents of kernel and user space TCP and UDP connection tables.
- you will need to allow the restored image to boot

Remote Control and Remote Access Services

- **REMOTE CONTROL**

  Applications such as PC Anywhere, AT&T's Virtual Network Computing (VNC) and Reach Out

- **ALLOWS WHAT?**

  Absolute control over the system, including the keyboard, screen, and mouse

- **DISADVANTAGE**

  allow only a single remote user to control the system at a time.

TOOLS USED TO FIND THE OPEN PORTS

netstat
Fport
PsList

REMOTE ACCESS

- Aceess where multiple remote users can simultaneously connect to the system via a modem connection.(ex. Windows RAS)
- Windows NT Server is capable of handling 256 incoming RAS connections right out of the box

TOOL(S) USED

rasusers to list all the user accounts that have the privilege to log in to the RAS server

COMMAND USED

net start

-to view all the running services.

CONDUCTING A WINDOWS INVESTIGATION.

- Review all pertinent logs.
- Perform keyword searches.
- Review relevant files.
- Identify unauthorized user accounts or groups.
- Identify rogue processes and services.
- Look for unusual orhidden files/directories.
- Check for unauthorized access points.
- **Examine jobs run by the Scheduler service.**
- Analyze trust relationships.
- Review security identifiers.