INVESTIGATING WINDOWS ENVIRONMENT
PART 5

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.

MEANING

- There is a possibility for any attacker to connect to the victim’s system by examining the jobs running at the VICTIM’S system

METHOD TO TRACK

remote /s "cmd.exe" batman5

If this command is running at a specific time on a machine ,any other system can connect to it by a command

remote /c <hostname> batman5

The <hostname> is the NetBIOS name of the remote system, and batman5 is the key
phrase to connect. The person can now execute any commands desired.

CONT…

- Mostly jobs are scheduled using “at” or “soon” utility.
- At command(with no arguments) will show any jobs that have been scheduled.

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.

ANALYZE TRUST RELATIONSHIPS.

- **WINDOWS NT**
- supports ***nontransitive/one-way trust***(*access and* services are provided in one direction only).
- If your NT PDC trusts another domain, it doesn't need to trust your PDC. Therefore, users on the trusted domain can use services on your domain, but not vice versa.
- **WINDOWS 2000**
- provide a two-way, or *transitive, trust relationship*.
- *Domains located* within an Active Directory forest require two-way trusts to communicate properly.

Contd…..

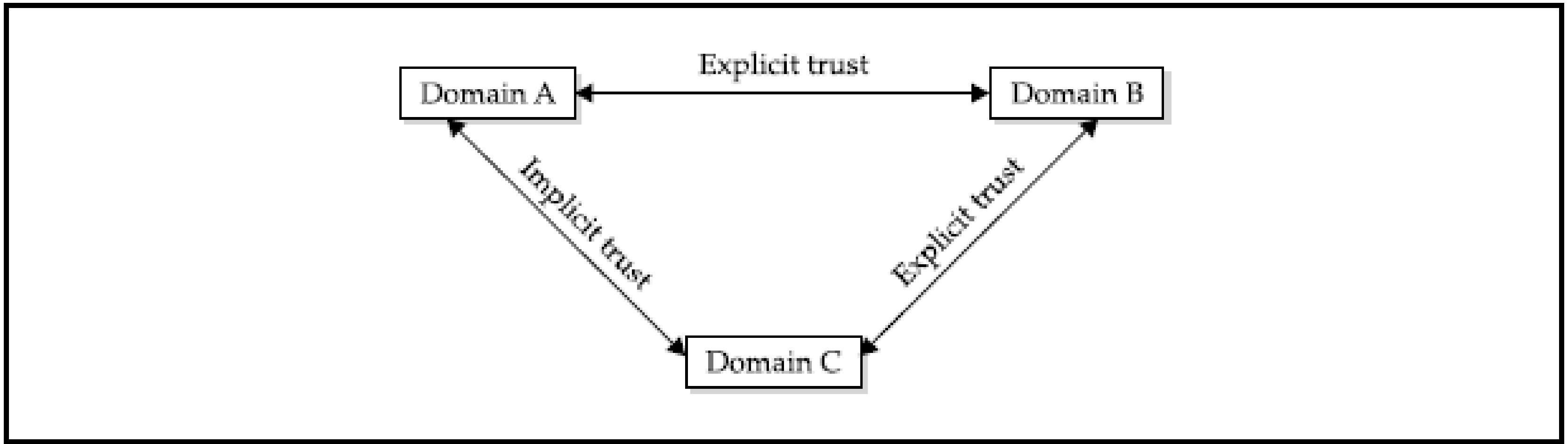


Figure 12-14. Windows 2000 trust relationships

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.**

Review security identifiers.

- The SID is used to identify a user or a group uniquely.
- Each system has its own identifier and each user has his own identifier on that system.
- The computer identifier and the user identifier are combined to make the SID.
- Thus, SIDs can uniquely identify user accounts.
- SIDs do not apply to share security.
- SIDs do apply when remote access to a domain is provided.
- SIDs can be the digital fingerprints that prove that a remote system was used to log on to a machine and access a domain.

CONTD..

- SID example
- S-1-5-21-917267712-1342860078-1792151419-500

EXPLANATION

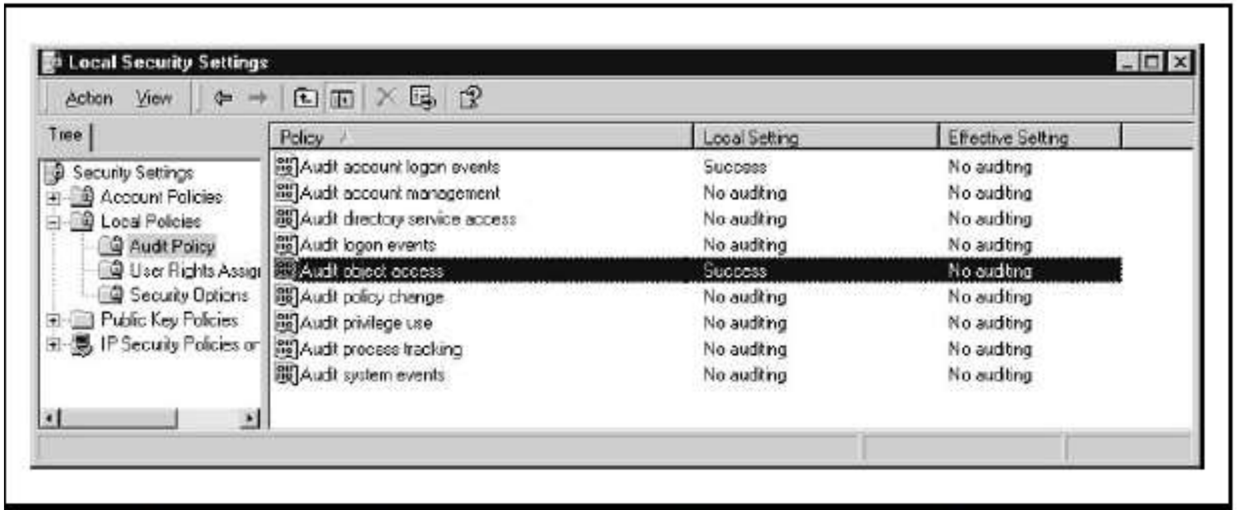
▪The **S** denotes the series of digits as a SID.
▪The 1 is the revision level,
▪ The 5 is the identifier-authority value, and
▪ 21-917267712-1342860078-1792151419 includes the subauthority values.
▪The 500 is the relative identifier.

FILE AUDITING AND THEFT OF INFORMATION

- If you need to identify who has placed unauthorized files on a server.

STEP1
use a network-based sniffer to monitor access to
the file server, or implement host-based logs using standard
Windows file-access auditing.

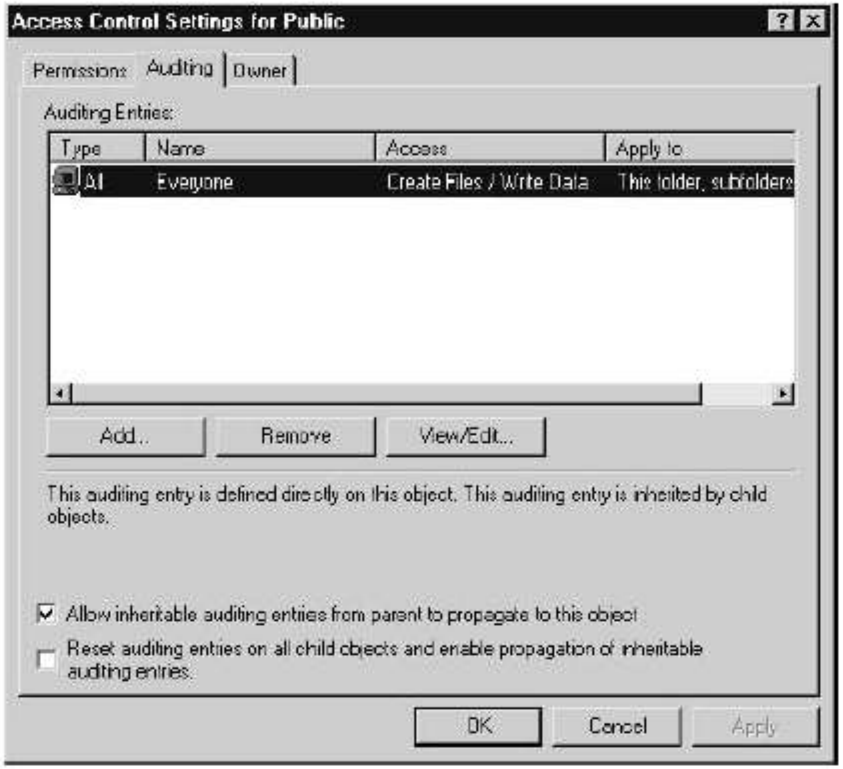
NOTE
if the file server is not running NTFS, you will not be
able to audit file and directory access easily.



Policy	Local Setting	Effective Setting
Audit account logon events	Success	No auditing
Audit account management	No auditing	No auditing
Audit directory service access	No auditing	No auditing
Audit logon events	No auditing	No auditing
Audit object access	Success	No auditing
Audit policy change	No auditing	No auditing
Audit privilege use	No auditing	No auditing
Audit process tracking	No auditing	No auditing
Audit system events	No auditing	No auditing

Figure 12-15. Using the Local Security Settings to audit object access in Windows 2000

- If file server is running then use local security auditing
- ***Figure*** shows the Local Security Settings window in a Windows 2000 system,which indicates that object access is being audited for successful access


Access Control Settings for Public

Auditing Entries:

Type	Name	Access	Apply to
All	Everyone	Create Files / Write Data	This folder, subfolders

This auditing entry is defined directly on this object. This auditing entry is inherited by child objects.

☑ Allow inheritable auditing entries from parent to propagate to this object

□ Reset auditing entries on all child objects and enable propagation of inheritable auditing entries

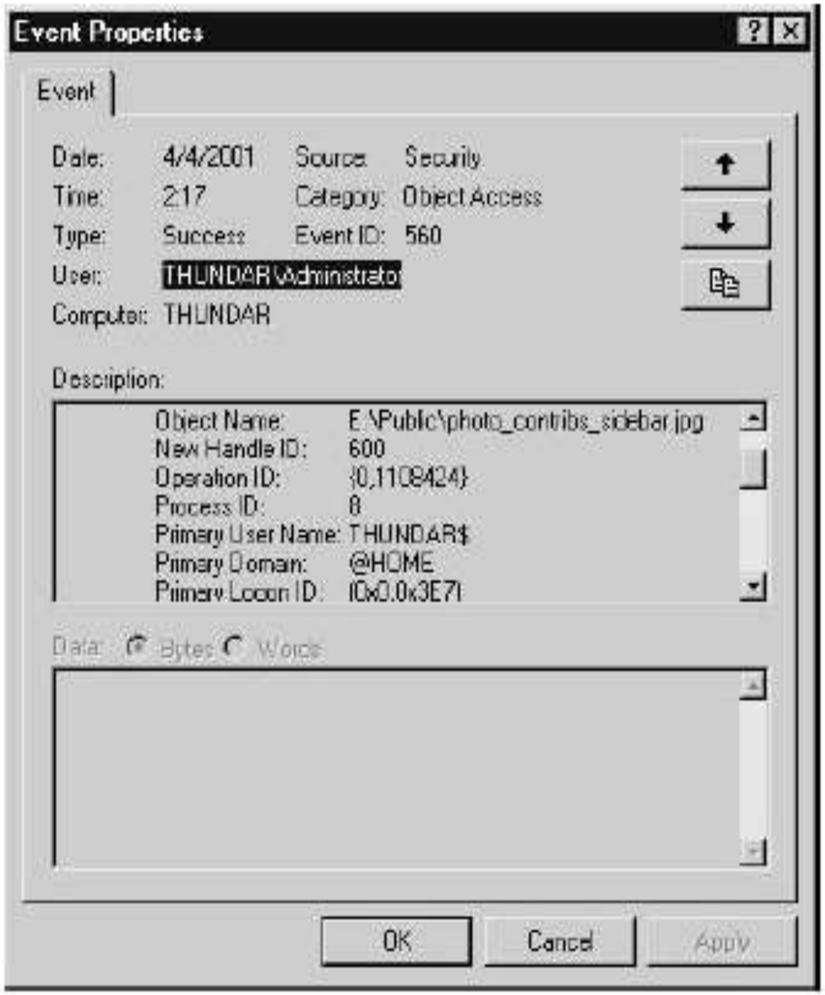
Figure 12-16. Auditing file writes to a directory on Windows 2000

- **STEP2**
- The next step is to select the directory to be monitored and choose the appropriate auditing.
- Figure 12-16 shows an example of the Public directory being audited, so that any user who writes a file to the Public directory will be logged

- If you enable success-and-failure auditing of the File and Object Access category of the audit policy, you will enable the following events:
- 560 Object Open
- 561 Handle Allocated
- 562 Handle Closed
- 563 Object Open for Delete
- 564 Object Deleted

Windows 2000 the File and Object Access category also includes these events:

- 565 Object Open
- 566 Object Operation



Date: 4/4/2001 Source: Security
Time: 2:17 Category: Object Access
Type: Success Event ID: 560
User: THUNDAR\Administrato
Computer: THUNDAR

Description:

```
Object Name:       E:\Public\photo_contribs_sidebar.jpg
New Handle ID:     600
Operation ID:      {0,1108424}
Process ID:        8
Primary User Name: THUNDAR$
Primary Domain:    @HOME
Primary Logon ID:  (0x0,0x3E7)
```

Data: ● Bytes ○ Words

Figure 12-17. The event detail showing the name of the file placed on the file server