

WINDOWS NT SECURITY AUDIT PROGRAM

1. Use table below and compare actual Windows NT settings with Standard or recommended settings.

FEATURE	DEFAULT SETTING	RECOMMENDED VALUE
PASSWORDS		
Maximum Age	30 days	60 days*
Minimum Age	14 days	1 day*
Minimum Length	6 characters	5 characters*
Uniqueness	Prevent users from using their last 3 passwords	8 characters for sensitive ID (Admins)* Prevent users from using their last 8 passwords*
After hours Disconnection	Don't Disconnect	Disconnect
Built-In Accounts		
Guest	No Password, Account Enabled	Disable and rename guest, assign password
Administrator	No Password, Account Enabled	Rename administrator, assign password
USER PROPERTIES		
Change Password at next logon	Selected	Selected
User Cannot Change Password	Not Selected (Except Guest)	Not Selected (Except Guest)
Password never expires	Not Selected	Not Selected
Account Disabled	Not Selected	Selected for Guest; selected on a case by case basis for all other accounts.
Full name and description fields	Blank	Should be filled in with user name and description
Home Directory	Blank	Should be specified if a user requires it.
USER PROFILES		
Disable RUN on File Menu	Not Selected	Select
Disable saved settings menu item and never save settings	Not Selected	Select
Show common program groups	Selected	Select
Logon Scripts	No default script	All user should have one

Feature	Default Settings	Recommended Value
HOME DIRECTORIES	None	Set up one per user
GROUPS Local Global	7 No users assigned	Assign Users to Groups
File/Directory Permissions	Full Control	Use NTFS Restrict permissions according to “principle of least privilege”.
Directories Shared Files/Directories Across the Network Printers	Full Control No Share Not shared can only be created by Administrator	Use NTFS Restrict permissions according to “principle of least privilege”. Create share, grant permissions according to “principle of least privilege”. Share printers
FILE STRUCTURES NTFS FAT HPFS	No default file structure “ ” “ ” “ ” “ ”	Use NTFS “ ” “ ”
OTHER Registry Replication Legal Notice Audit Policy File and Directory Printers Clipboard page Remote Access Server Security Event Logging Network Alerts	Not enabled “ ” “ ” “ ” “ ” “ ” “ ” “ ” “ ” Overwrite Events as Needed Not enabled	Enable where appropriate “ ” “ ” Enable with Unauthorized Access is Prohibited” message Enable all events Enable Enable where appropriate Enable Not enabled Enable Do not overwrite events (Clear Log Manually) Enable for excessive Log Failures

Source: Windows NT 3.5 Guidelines for Security, Audit and Control

* Corporate Standard (Use your company standards)

V. EXPLANATIONS

NTFS

1. Windows NT File System is a system designed for use specifically within the NT OS.
2. It supports file system recovery, extremely large storage media and various features for a subsystem, such as multitasking.
3. It supports object oriented applications, treating all files as objects with user and system defined attributes.

FAT

4. File Allocation Table file system.
5. Maintained by the OS to keep track of various segments of disk space used for file storage

HPFS

6. High Performance File System.
7. Primarily used with OS/2 OS.
8. It supports long file names, but does not provide security.

Registry

9. think of a bride's registry at a store.
10. a database repository for information about a computer's configuration, including the hardware, software environment settings and other information.
11. Includes user profiles.
12. It's a read only file

Replication

13. The copying of a master set of directories from a server.
14. It simplifies a task of maintaining identical files on multiple computers because only one set has to be maintained.

NT Security Audit Program

HDWAT is "How do we Assure that"

1. HDWAT anyone can not use the system without being explicitly authorized?
 - a. Does a "no trespassing sign" greet everyone without authorization?
 - b. Do trusted relationships exist? In other words, can a user log on to another network and if so, what domains?
 - c. Have guest and administration accounts, as well as groups of the same names, been renamed and do the ids require passwords?
 - d. Does account policy define p/w age = 90days, p/w minimum length = 6 characters
 - e. Can administrator log on through the network or must be at the server console?
 - f. Is multiple log on allowed by anyone?
 - g. Identify all ids with administration privileges.

2. HDWAT anyone can not access system or application files without being explicitly authorized?
 - a. Are all file structures NTFS?
 - b. Can DOS be IPL'd which would provide access to all files and bypass NTFS?
 - c. Obtain copies of ACLs for each file or directory.

3. HDWAT anyone can not access resources without being explicitly authorized?
 - a. Review shares between systems and permissions for each.
 - b. Review security settings for the registry.

4. HDWAT anyone can not change access rules without being explicitly authorized?
 - a. Review all accounts with authority to change accounts and ACLs
 - b. Determine whether these are properly assigned and sufficiently restricted

5. HDWAT there is an adequate separation of duties among the three security functions?
 - a. Obtain written procedures for approving/applying/reviewing access privileges
 - b. If no separation, what compensating controls exist?

6. HDWAT the OS is protected against unauthorized modifications?
 - a. Who has the authority to modify the OS? Obtain ACLs for NT directories
 - b. Determine which accounts have the rights to the OS.
 - c. What services do these allow?

Supplement to NT Audit Program

1. Identify NT server and workstation version level.
2. Is the OS/2 and POSIX subsystems disabled (to disable go to Resource Kit)?
3. Verify if lockout feature is enabled (lockout after at most 5 bad login attempts).
4. Determine if access restrictions after off-hours is implemented.
5. Verify if screensaver feature is activated (activates after at most 20 minutes of inactivity)
6. Determine if existent formal procedures to tell operators and administrators who to contact and what action to take in the event of a security breach. (If yes, get copy)
7. Verify if there is a backup controller (BDC) for each primary controller (PDC).
8. Verify adequacy of access permissions for sensitive directories (including Event Log, etc.)
9. Review the security log in Event Viewer, and verify if action were taken for any unusual activity.
10. Obtain copies of system logon script and review. (standard approved scripts)
11. Verify when a new user ID is created, the logon script for new user account is replicated from standard approved scripts.
12. Verify that access to change NT registry from remote location is restricted.

13. Determine if virus scanners are used for workstation and server (should be set to run automatically) and how virus scanners is updated.
14. Verify if existent backup schedule procedures, if existent get copies.
15. Document which groups and users have each of the following sensitive administrative rights that can affect or bypass normal system security. Consider whether these rights are appropriate to that group or user:

Restore Files and Directories

Manage auditing and security log

Backup files and directories

Take ownership of files and other objects

Bypass traverse checking

Log on as a service

16. Determine if access to network monitoring devices, such as sniffers, is restricted to authorized individuals.