



Jack Schmidt
MS120
Schmidt@fina.gov

OSS/PCS

D0 NT Security Review



*Computer Security Review of the
DZERO NT Domain*

November 22, 1999
Greg Cisco
Mark Kaletka
Jack Schmidt

·
·
·
·
·
·
·

D0 NT Security Review

Computer Security Review of the DZERO NT Domain

Background

Computer security has been and is an important aspect of support by the lab. The Windows NT operating system along with sharing popularity in the operating system market has become the object of computer hacking worldwide. This plan documents present day practices followed by the D0 PC Support group in the DZERO NT domain as well as outlining new policies to be recommended. The computer security field is ever changing and it is the belief of the authors that this plan should be reviewed semi-annually and any necessary changes be made.

The number of people involved in PC support at D0 is 1.5 FTE's. The D0 Support group is responsible for maintaining 6 servers (one running Microsoft's Terminal Server), and providing various levels of support for 189 workstations. Universities own many of the workstations and the D0 Support group has very restricted access to these systems.

The D0 PC Support group has actively been working to tighten up security issues at D0. New servers have been purchased and the core services for D0 users have been expanded and separated. Key improvements are:

- The IIS server (Web Services) now resides on a simple server instead of being part of a domain controller.
- More storage has been added to allow users to store information on the server instead of on their desktop workstation.
- Virus scanning is present on all file servers.

The recommendations in the review are broken up into sections; desktop standardization, physical security, file system, registry entries, password and account policies, auditing services, monitoring, updating security, and tools.

Desktop Standardization

The most complicated problem that the D0 NT support group faces is providing a working desktop model. While the servers have been, in the most part, well secured the workstations are very vulnerable to attack.

In order for them to maintain a stable and secure working environment it is the recommendation of this committee that workstations in the D0 domain meet certain criteria. A checklist has been developed that addresses both D0 Supported workstations as well as

Experimenter provided systems. Before a system is added to the DZERO NT domain the Workstation owner must agree to the requirements set down by the D0 PC Support group

Desktop Systems:

Permanent systems are those defined as systems that require access to D0 domain resources on a regular basis. These systems may be owned by FNAL or by a university.

1. The default Administration permissions on workstations is that Domain Users have no Local Administrator privileges. A user can be added to the Local Administration *group* of a workstation and inherit the local administration group permissions, if the user agrees that in case of a problem the workstation system disk will be reformatted and the basic D0 Workstation configuration installed. At *no* time will a user be given the password for the Local Administrator *user account* for a Fermilab owned machine. University users must maintain their own Local Administrator account and password. If they require an additional program to be installed on their system then they will work with the D0 PC Support team.
2. Workstations will be configured to store documents in the user's area on the D0 NT servers. D0 Users will NOT create shares on their local systems.
3. Workstations will not be configured to run ftp, www or telnet servers. Users are required to use the departmental www and ftp server.
4. D0 Users are not allowed to install or operate any type of 'admin' program such as Back Orifice or security programs such as Lophtrcrack or tripwire.
5. D0 Unix Users are allowed to access PC software and files via the D0 terminal server or installing the Samba client on their desktop system. The Samba clients must meet the D0 PC Support configuration requirements. *At no time is a D0 Unix user allowed to install Samba Server on their desktop system.*
6. Virus checking software will be installed and maintained on each workstation.
7. All permanently installed NT systems at D0 must adhere to the above rules.

Laptops:

Laptops (whether D0 supported or a visitor system) that need access to D0 resources must meet the following criteria:

1. These systems are not allowed to have a domain machine account.
 - a. NOTE: This does not affect the ability to access the domain resources.
2. Laptops will be configured to store documents in the user's area on the D0 NT servers. Laptop Users will NOT create shares on their local systems.
3. Owners of laptop systems are not allowed to install or operate any type of 'admin' program such as Back Orifice or security programs such as Lophtrcrack or tripwire.

4. D0 Unix Users are allowed to access PC software and files via the D0 terminal server or installing the Samba client on their desktop system. The Samba clients must meet the D0 PC Support configuration requirements. *At no time is a D0 Unix user allowed to install Samba Server on their desktop system.*
5. Virus checking software will be installed and maintained on each laptop.

Physical Security

Physical security is one of the simplest but most overlooked security precautions that can be taken. Servers under the care of the D0 PC Support group are maintained in the D0 Detector Building. The relay racks holding the servers are accessible by anyone. Desktop systems are spread across the D0 complex.

Server Specific Recommendations:

1. It is recommended to secure servers in each relay rack by cable and lock obtainable by the lab security office. The D0 Support group will be responsible for maintaining the keys in a secure area.
2. It is recommended to install the flopplock program from the NT resource kit to disable access to the floppy drive from everyone but the local Administrator, or use BIOS passwords to disable access to the floppy drive and CDROM drive.
3. It is recommended that server backups be performed on a regular basis. Backup tapes should be stored in a locked cabinet away from the servers. Only members of the D0 PC Support group should have access to the backup tapes.

Workstation Specific Recommendations:

1. Physical workstation security is the responsibility of each person at the lab. It is recommended that each workstation be in a locked office or locked down using security kits provided by the lab security office.
2. All monitors will display the DOE required logon sticker.

Registry Settings

The Registry provides many useful security settings for System Administration. Though there are many numerous options regarding security in the Registry only a few pertain to security requirements at the lab. The following registry settings will be made to systems in the D0 domain. They are divided into entries that are specific to servers, workstations or both systems.

Server Specific Recommendations

1. NT Allows anonymous access connections to list NT account names. Any anonymous access to the FNAL NT domain should be removed unless otherwise specified.
 Hive: HKEY_LOCAL_MACHINE\SYSTEM
 Key: \CurrentControlSet\Control\Lsa\RestrictAnonymous
 Type: REG_DWORD
 Set value to 1

2. Secure Event Log (Make the registry setting below and secure permissions on the system directories to be Admin and System only. Files are in %systemroot%\system32 directory)
 Hive: HKEY_LOCAL_MACHINE\SYSTEM
 Key: \CurrentControlSet\Services\EventLog\[LogName]\RestrictGuestAccess
 Type: REG_DWORD
 set value to 1.

3. Restrict Access to the AT job command. This can be set to 0 or 1, where 0 allows only admin access and 1 allows only admin and server operators
 Hive: HKEY_LOCAL_MACHINE\SYSTEM
 Key: \CurrentControlSet\Control\Lsa\SubmitControl
 Type: REG_DWORD
 Set Value to 0 – Allows only Administrator to submit AT jobs.

Workstation Specific Recommendations:

none

Both Recommendations:

1. Remove Username from the login box. The default is to display the username of the last person to log into the system. This setting will prevent the name from being displayed.
 Hive: HKEY_LOCAL_MACHINE\SOFTWARE
 Key: \Microsoft\WindowsNT\CurrentVersion\Winlogon\DontDisplayUserName
 Type: REG_DWORD
 Value Of 1 – The username field will be blank.

2. Enable display of the DOE sanctioned logon message. The Computing Division can provide the D0 PC Support group with a program that can perform this function.

Passwords and Account Policies

Password Guidelines

NT provides limited individual account settings. NT provides few tools for manipulating and gathering account information. This is one area that third party tools can be helpful. The following recommendations are made until NT can participate in the Strong Authentication plan created by the Fermilab Security team (these recommendations can be applied to both domain accounts and user accounts on individual computers):

New Accounts

When creating a new account, always check the *change password on first login* box. Never check the *Password never expires* box.

Terminated Account

When a member of the D0 domain leaves the lab his/her NT user account should be deleted. Access to the user's files will be determined by the FNAL Policy on Computing.

Domain Account Policies

The D0 NT domain account standards are set in User Manager |Policies|Account. Recommended default settings are:

Maximum Password Age = 180 days (6 months). This is the length of time before a password expires.

Minimum Password Age = 3 days. Once a user changes their password, they must wait at least three days before changing it again.

Minimum Password Length = 8 characters. Macintosh computer restrictions used to require the minimum password length be limited to only six characters. Since there is no longer Macintosh support at D0, a stronger password length of at least 8 characters is to be used.

Password Uniqueness = 3. A user in the D0 NT domain cannot reuse a password for at least three changes.

Account Lockout = lockout after 3; reset after 10 minutes. Incorrect attempts to log in to a domain account will lock the account out after three attempts.

Lockout Duration = 15 minutes. Once an account is locked out the user must wait 15 minutes before attempting to login again- or notify a system admin to reset their account.

User Must Logon To Change Password = yes (can cause problems on Citrix servers).

Enable Admin Lockout and Rename Admin Account

Use the passprop.exe utility found in the NT4 Resource kit to lockout the Administrator account after numerous network attempts. Note that the Administrator is not logged out from a console login. Many security documents suggest that the Administrator account be renamed and that account be used for admin purposes. Then they suggest that a decoy Admin account be created and the account be audited. It is recommended that D0 follow these suggestions.

SysAdmin Privs

System Administrators in the D0 NT domain will have standard user accounts with normal privileges. To perform Administrator work it is recommended that they log on using the Domain Admin account or make use of the SU command (much like the Unix SU command- allows process to run at a higher privilege level) available in the NT resource kit.

Secure Admin password (PGP file)

It is recommended that passwords for systems maintained by the D0 PC support group be kept in a PGP encrypted file on a floppy in a locked area.

Restrict Everyone Account Privileges and disable Guest Account

The guest account should be disabled on all servers in the D0 NT domain. The everyone account privileges should not be modified to include more than initially given.

Restrict Privileges to Non-Administrators

Members of the D0 PC Support group will refrain from assigning full Administrator privileges to users. It is recommended that the PC Support group identify the needed privileges/rights of each user.

Avoid shared accounts

Whenever possible, members of the D0 PC Support group will avoid creating shared accounts in the D0 NT domain (this policy is already in effect at D0).

Assign permissions to groups instead of users

Whenever possible D0 NT Administrators should assign permissions to groups instead of individual users. Group names should be created to help identify the support area they were created for.

Domain Admin

Weekly the Domain administration global group should be examined for any modifications.

DC SAM Encryption

The D0 PDC (Primary Domain Controller) SAM should have 128bit encryption applied to it.

Audit Logging on Servers

NT provides the ability to audit file access, account access, user right changes, system shutdown and restart. Specific ACL auditing can be done by the Security setting for the file. The general auditing events are set using the User Manager with the ability to log both Success and Failure events. It is recommended that servers in the D0 NT domain have auditing enabled for:

Event	Success	Failure
Logon and Logoff	No	Yes
File and Object Access	No	No
Use of User Rights	No	Yes
User and Group Management	No	Yes
Security Policy Changes	Yes	Yes
Restart, Shutdown, and System	Yes	Yes
Process Tracking	No	Yes

It is recommended that a central audit server be created and maintained by the D0 PC Support group. The NT resource kit provides simple tools for log examination or a third party tool can be purchased.

Monitoring

Monitoring of server event logs, IIS logs and group permissions is an important part of NT security. It is recommended that the D0 PC Support group monitor this information on a regular basis. Third party tools are available for this task or simple tools available from the NT resource kit can be used. Presently the Computing Division Support group uses tools

available in the NT resource kit to dump event logs and search for specific events. This set up can be made available to the D0 PC Support group.

Updating Security

Application of patches for the operating system and applications is extremely important.

OS Recommendations:

Identifying applicable service packs and patches are the responsibility of the system administrators. The D0 PC Support group can identify their own guidelines or follow those offered by the Computing Division PC Support group. Patch and hot fix information can be downloaded from Microsoft or taken from the CD PCKITS system.

Application Recommendations:

Care should be paid to security updates from application providers. Some third party security tools check for application (Office, IE) deficiencies.

Virus Prevention Recommendations:

Anti-virus prevention software is only as effective as the list of viruses it checks for. It is recommended that the anti-virus software on the D0 servers be configured to automatically update anti-virus information.

Recommended Tools

SPQuery

Maintaining a large numbers of servers and workstations at the proper service pack and hot fix configurations can be a daunting task. To help administrators at the lab the Computing Division PC Support group has purchased a site-wide license for SPQuery. SPQuery is a useful tool for:

- Reporting Service pack and hotfix information for an entire domain or a select group of machines.
- Downloading of hotfixes from Internet for NT, IIS, Exchange, SQL and Site Server to a central repository
- Applying Workstation/Server hotfixes to remote machines

It is recommended that the D0 PC Support group be allowed to use this tool.

STAT

The Computing Division PC Support group uses STAT (Security Testing and Analysis Tool) to help maintain computer security. STAT is useful for

- Detecting Vulnerabilities from NT3.51 to NT4 SP5

- Can Examine specific machine, multiple machines or Entire Domain
- Automatic Vulnerability Fix
- Configuration Templates available
- Password Strength testing

The security team recommends that D0 be allowed to run STAT against the D0 systems. STAT does come with a simple password `cracking' tool that is run against a system as part of the vulnerability checks. STAT can be configured NOT to use this feature if the Fermilab Security team desires. STAT must be purchased by D0. Fermilab does not have a site license for this product.

LOPHTCRACK

Lophtrcrack is a password cracking tool available for NT systems. The Computing Division PC Support group owns a copy of this tool. D0 requests the Computing Division to run l0phtcrack (dictionary check only) on the SAM database on the D0 Domain Controller(s) at a regular interval.

NT4 Resource Kit

The Microsoft resource kit for NT provides many valuable programs for checking security from dumping event logs to examining shares. It is recommended that the D0 PC support group install the resource kit on their servers and system administration desktops.

The Computing Division PC Support group owns a site-wide license for the NT4 Resource Kit.

ShareChk

This utility was written by Mark Kaletka to test for NT shares that allow access by anyone. It is recommended that the D0 PC Support group use this tool to check share permissions in the DZERO NT domain.

Overall Recommendations

Members of the D0 collaboration have met to review and comment on the recommendations made in this document. Overall the D0 PC Support group has made great advances in improving security of their NT workstations and servers. To help fully meet the recommendations of this plan the Review Committee feels that the D0 PC Support group be given permission to use the tools listed in the previous section. Reports generated from these tools can be mad available to the Computer Security team at FNAL.

The Review Committee strongly recommends that D0 increase the amount of personnel and security tool resources involved with supporting PCs.