Security Vulnerabilities in NT Server

Steven Weber
Technology Risk Services
PricewaterhouseCoopers LLP
Columbus, Ohio USA
steven.weber@us.pwcglobal.com

PRICEWATERHOUSECOOPERS

NT Threats and Vulnerabilities

Abstract:

And you thought your networks were secure! During this revealing presentation you will learn the threats to Microsoft Windows NT, how they work, where they can be found, and what you can do to minimize exposures. Such threats as physical security to the file server, information discovery, password cracking, and malicious services will be discussed. Come to this presentation to learn the security threats lurking in your Windows NT networks and the countermeasures you can take to protect your information assets from them.

PRICEWATERHOUSECOOPERS

Steven Weber CISSP CPA
Technology Risk Services Senior Consultant
PricewaterhouseCoopers LLP

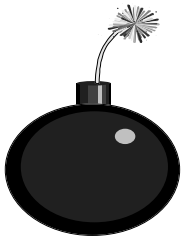
Biography:

Steven M. Weber is a Senior Consultant of Technology Risk Services for PricewaterhouseCoopers LLP in Columbus, Ohio. He has presented seminars relating to Novell and Windows NT security for various professional and training organizations. He has assisted clients through the United States in developing, maintaining, and assessing their overall security positions. His background includes a degree from the Ohio State University Max M. Fisher College of Business and he is a Certified Information Systems Security Professional and a Certified Public Accountant.

Steven can be reached through the Internet at steven.m.weber@us.pwcglobal.com or by phone at (614) 225-8830.

Agenda

- Overview
- Risks and Exposures
- Security Threats to NT
- Identification and Authorization
- Password Capture and Interception
- Defense and Prevention
- Reference Materials



Objectives

- Maintain an informal and interactive atmosphere
- Understand the security threats of Windows NT
- Learn the countermeasures needed to reduce the risks associated with the Windows NT environment
- Understand a set of minimal baseline security controls for the Windows NT environment

PRICEWATERHOUSECOOPERS

Why Be Concerned with Network Security?

- Used to process financially significant production applications and data
- Stores confidential, sensitive, or business critical information
- Networks are the connectivity between multiple platforms
  - Weakest Link Theory

PRICEWATERHOUSECOOPERS

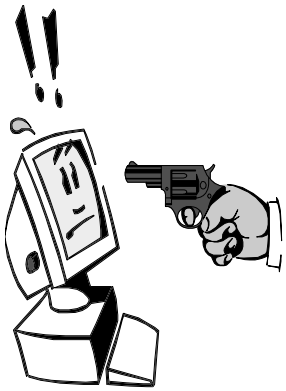
Risks and Exposures

- Physical access
- Privileged user access
- Technical vulnerability exploits
- Social engineering
- Network transmission analysis
- External connectivity
- Information discovery
- Information disclosure

PRICEWATERHOUSECOOPERS

Security Threats to Windows NT

- Physical Access
- NTFSDOS
- FAT vs. NTFS
- Backup Media
- GetAdmin
- NetBus
- C2MYAZZ
- Anonymous Logon
- NBTSTAT



PRICEWATERHOUSECOOPERS

Physical Access

Description: If an unauthorized individual has physical access to a Windows NT Server, there are a number of methods that could be used to obtain system privileges or direct access to the information contained on the server. In addition, as with any computing device, physical access means a person could shut down or damage the computer system regardless of the operating system in use.

Countermeasures:

- Control physical access to servers
- Control access to other critical devices
  - (e.g. routers, hubs, etc.)
- Control physical access to backup media

PRICEWATERHOUSECOOPERS

Physical Access - NTFSDOS

Description: NTFSDOS is an executable program developed by Mark Russinovich and Bruce Cogswell which allows access to NTFS partitioned file systems when a Windows NT server is booted using DOS. This program allows direct access the information stored on an NTFS partition, bypassing all access control features of the file system.

Countermeasures:

- Load only one operating system (do not install DOS on a separate partition)
- Require a valid login to occur before system reboot
- Use hardware power on passwords

PRICEWATERHOUSECOOPERS

Physical Access - FAT

Description: A disk partition that has been formatted using FAT (File Access Table) does not provide any security. There is no support for any of the access control features of an NTFS file system. If a Windows NT server is booted locally using DOS, access to any FAT partitions will be unrestricted.

Countermeasures:

- Use the NTFS format for all disk partitions

PRICEWATERHOUSECOOPERS

Backup Media

Description: Depending on the backup method and software used, the data written on the backup media may be stored in an unencrypted form. This means that the media could potentially become accessible to an outsider by restoring the data on a different machine.

Countermeasures:

- Prevent access to the media storage facility and transport it in locked containers.
- The encryption features of the backup software and devices should be enabled.

PRICEWATERHOUSECOOPERS

GetAdmin

Description: When executed it inserts an unprivileged user account into the local Administrators group. That user account is then able to function as an administrator on the system. The user does have to be logged on interactively (locally) or via a telnet session in order to execute the program. Any valid user account may be added to the local Administrators group.

Countermeasures:

A patch was released on the Microsoft website to address this technical vulnerability. However, a second version of GetAdmin was released which still takes advantage of this technical vulnerability even after the first patch. A supplementary patch was released to address the new version of GetAdmin. Therefore, both patches need to be implemented to protect Windows NT.

PRICEWATERHOUSECOOPERS

NetBus

Description: Remote administration utility utilized to remotely control a Windows 95 or Windows NT workstation or server over a TCP/IP network. NetBus allows a remote user to perform just about any function on the infected machine including controlling the keyboard, mouse, and video.

Countermeasures:

- Perform a port scan of each system to determine if the system is listening on port 12345 which is the default NetBus IP port.
- Run an updated anti-virus package to determine if the system is infected with NetBus.

PRICEWATERHOUSECOOPERS

C2MYAZZ

Description: When a Microsoft networking client creates a new connection to an NT Server, it is possible for another computer on the same physical network to “spoof” the Microsoft client into sending a clear-text password to the NT Server, bypassing all password encryption and allowing the client's clear-text password to be discovered by any other device on the same physical network.

Countermeasures:

NONE!

PRICEWATERHOUSECOOPERS

Anonymous Login

- Windows NT may be configured to support anonymous user access for specific purposes--usually as a web or FTP server
- Another concept known as an anonymous connection presents a significant threat to Windows NT
  - Anonymous Logon
    - Rights are derived from the rights assigned to the Everyone group
    - This allows certain system and account configuration details to be obtained by a remote NT workstation or NT server using the IPC$ administrative share
      - net use \\servername\ipc$ “” /user: “”

- Can be utilized to gain other detailed information from the Windows NT registry as well

PRICEWATERHOUSECOOPERS

NBTSTAT

- Native command of NT that can be used to display the contents of the remote computer's NetBIOS name table
- The information that is listed in the NetBIOS name table can be used to determine the Domain name or workgroup the machine is in and the currently connected users
  - The information may also be used to uncover the administrator, due to the fact that active connections are displayed in the name cache

PRICEWATERHOUSECOOPERS

Identification and Authorization

As the front line defense in any computer system, identification and authentication is an essential component of the Windows NT security architecture. The basic concept of authentication begins with the user's login name and password. Most of the threats in this environment relate to the password: is it too weak, does it exist at all, can it be compromised in some way? User accounts with easily guessed passwords can be used to gain unauthorized access to a Windows NT environment and can be the starting point of a more serious security compromise.

PRICEWATERHOUSECOOPERS

Identification and Authorization (Continued)

- Weak or easily guessed user passwords are one of the most common ways to attack computer security. If users are not required to have a password or can have passwords of inadequate length or strength, the risk that a user account may be compromised increases significantly. Conversely, forcing passwords to be too complex becomes self-defeating when users write the passwords down in order to remember them.
- Default passwords created by vendors when installing software or products and the accounts and passwords created by automated software installation tools also pose a serious threat to Windows NT security.
  - (e.g. backup, UPS, and virus scanning software)

PRICEWATERHOUSECOOPERS

Identification and Authorization (Continued)

- Password Cracking
  - Brute force and dictionary attacks
  - Programs exist that can be used to quickly identify user accounts without passwords assigned or passwords that are commonly used
  - Several programs, some are freely available, while others must be purchased
  - (e.g. NTCrack, L0PHT Crack, etc.)

PRICEWATERHOUSECOOPERS

Password Capture and Interception

- Network sniffing and packet capture can be used to capture sensitive network transmissions from other platforms that in turn can be utilized to compromise Windows NT security
- Network Monitor tool that is available with SMS for Windows NT is a common tool for watching network traffic
  - Many others available

PRICEWATERHOUSECOOPERS

Password Capture and Interception (Continued)

- Passwords may be cached in the registry during the logon process on a local machine--this cache is potentially available to collect passwords
- Another method of password capture involves intercepting the plain text password during the password change process. This requires a form of Trojan Horse program to operate within the normal password processor
- Standard TCP/IP networking services such as Telnet and File Transfer Protocol (FTP) are available for Windows NT. While these services provide additional functionality and interoperability, they use a weak authentication protocol
  - When a user authenticates using either of these services, their password is transmitted from the network in clear text

PRICEWATERHOUSECOOPERS

Password Capture and Interception (Continued)

- NetBIOS commands, the most common of which is “NET USE”, may require a password to be transmitted over the network
  - If authentication has been previously accomplished to the server or to the domain containing it, then the password is not required
- Passwords may also be captured from the on-line directories that store registry data
  - These directories include the %systemroot%/repair and %systemroot%/system32/config
- The default Administrator account cannot be locked out by the intruder detection feature, which is an intended function of Windows NT Server
- The Auto Admin Logon function of Windows NT Server allows a server to automatically logon upon system startup
  - The user account name and password are stored in the registry in clear text

PRICEWATERHOUSECOOPERS

Denial of Service Attacks

- Ping-of-Death and Ping-of-Death 2
  - Sending ping packets that are not the standard 64k size
- SYN Flood Attack
  - Spoofing packets with unknown IP addresses so that the server continues to respond with SYN packets
- Out-of-Band Attack
  - Sending data outside of the normal scope of Windows NT to ports such as 139 (NetBIOS) and 53 (DNS)

PRICEWATERHOUSECOOPERS

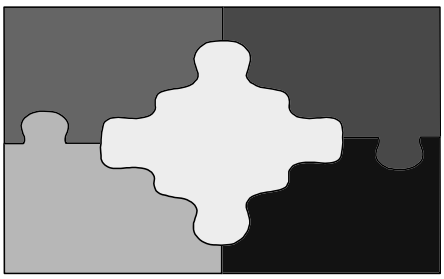
Denial of Service Attacks (Continued)

- Telnet to Unknown Ports
  - Telnet to ports other than 23 (Telnet) such as 135 (RPC), 53 (DNS), 1031 (inetinfo)
- Land Attack
  - Source and destination SYN packets have the same address and port
- Teardrop and Teardrop 2
  - Sending fragmented UDP datagram packets to the server

PRICEWATERHOUSECOOPERS

Denial of Service Attacks Defenses

Implementing latest service packs and system patches to address these specific attacks

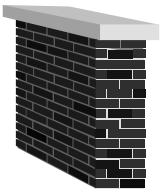


PRICEWATERHOUSECOOPERS

Defense and Prevention

The following outlines several steps to be taken to help secure an NT environment:

- A determination of the business purpose of each and every Windows NT system
- Disable access to the Server Message Block (SMB) protocols that operate on NetBIOS over TCP/IP. The communications protocol ports for this process include tcp/udp/ ports 137, 138, and 139
- Disable the Computer Browser service on servers other than domain controllers
- Unbind the NetBIOS and NetBEUI protocols from any external network interface card
- Ensure that the registry contains strong enough permissions to prevent members of the Everyone group from creating or writing to key values



PRICEWATERHOUSECOOPERS

Defense and Prevention (Continued)

- Disable the hidden administrative shares (C$, D$, Admin$, etc.) by changing the following key in the registry for a server:

  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters

  Name: AutoShareServer

  Value Type: REG_DWORD

  Value: 0 (off) or 1 (on)

- Or for a workstation:

  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters

  Name: AutoShareWks

  Value Type: REG_DWORD

  Value: 0 (off) or 1 (on)

PRICEWATERHOUSECOOPERS

Defense and Prevention (Continued)

- Install Service Pack 3 or greater and insert the following key into the registry:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

  Name: RestrictAnonymous

  Value Type: REG_DWORD

  Value: 1

- This key addition will prevent the Anonymous Logon connection and will require authentication in order to list account names and enumerate share names when using the Graphical User Interface tools native to Windows NT
- Ensure that remote editing of the registry is restricted by verifying the presence of the following registry key (default in NT Server 4.x but not NT Workstation 4.x or NT Server/Workstation 3.x):

  HKEY_LOCAL_MACHINE\CurrentControlSet\Control\SecurePipeServers\winreg

PRICEWATERHOUSECOOPERS

Defense and Prevention (Continued)

- A good password policy that is both enforceable and reasonable is a requirement
  - Set account policies to require passwords of adequate length and enforce a regular change interval
  - Enforce stronger password controls by implementing PASSFILT.DLL, available from service pack 2 onward. PASSFILT.DLL enforces strong passwords by requiring the use of three of the four following characteristics: lower case, upper case, numeric, and special (*, &, etc.) characters. PASSFILT.DLL can be implemented as follows:
    - HKEY_LOCAL_MACHINE\System\CurrentControlSet\LSA
    - Name: NotificationPackages
    - Value Type: REG_SZ
    - Value: PASSFILT

PRICEWATERHOUSECOOPERS

Defense and Prevention (Continued)

- Consider enabling strong encryption of the SAM database by using SYSKEY.EXE (see Microsoft Knowledge Base Documentation Q143475 for more details), which stores the password hash values
- Disable the LAN Manager authentication process (assuming only NT is used with the environment) using lm-fix from service pack 3 and implementing this key:
    - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA
    - Name: LMCompatibilityLevel
    - Value Type: REG_DWORD
    - Value: 2

PRICEWATERHOUSECOOPERS

Defense and Prevention (Continued)

- Restrict the access to the LSA key so that the permissions allow only Administrators write access to the key
- Limit the use of legacy services that send passwords in clear text. Use anonymous logon access for legacy protocols, if appropriate
- Rename the built-in Administrator account to a name less obvious and change the account description
    - Consider creating a decoy account named “Administrator” and revoke all sensitive access
    - Monitor attempted access to the decoy “Administrator” account to help identify potential intruders

PRICEWATERHOUSECOOPERS

Defense and Prevention (Continued)

- Protect the registry directories from unauthorized access and possible theft of data
  - Restrict permissions on the %systemroot%/repair directory to the Administrator group only
  - Restrict permissions on the %systemroot%/system32/config directory so that the Everyone group has List access. In addition, the Everyone group should have Read permissions for the files within this directory
- System services run underneath the system context by default
  - Consider running third party system services with specific user accounts rather than the System context when appropriate

PRICEWATERHOUSECOOPERS

Baseline Security Standards Passwords

Security Features	Default	Recommended
Maximum Age	42 Days	30 Days
Minimum Age	Allow changes immediately	1 Day
Minimum Length	Permit blank passwords	8 Characters
Uniqueness	Do not keep password history	Prevent users from using their last 8 passwords
After Hours Disconnection	Don't forcibly disconnect	Consider Disconnect

PRICEWATERHOUSECOOPERS

Baseline Security Standards
Installation Defined User Accounts

Security Features	Default	Recommended
Guest	No Password, Account Disabled	Assign Password and Keep Disabled
Administrator	Password Assigned During Installation, Account Enabled	Rename Account Name, Assign Difficult to Determine Password

PRICEWATERHOUSECOOPERS

Baseline Security Standards
User Properties

Security Feature	Default	Recommended
Change Password at Next Logon	**Selected**	**Selected**
User Cannot Change Password	**Not Selected (except Guest Account)**	**Not Selected (except Guest Account)**
Password Never Expires	**Not Selected (except Guest Account)**	**Not Selected (except Guest Account)**
Account Disabled	**Not Selected (except Guest Account)**	**Not Selected (except Guest Account)**
Full Name and Description Fields	**Blank**	**Should be filled in with user name and description**
Home Directory	**Blank**	**Should be specified**

PRICEWATERHOUSECOOPERS

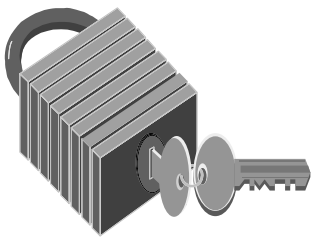
Baseline Security Standards
User Profiles

Security Feature	Default	Recommended
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	Selected
Logon Scripts	No Default Logon Script	As Needed

PRICEWATERHOUSECOOPERS

Windows NT Audit & Security Tools

Audit and Security Tools



- BindView Enterprise Management System for NT
- Kane Security Analyst for NT
- Axent ESM for NT
- ISS and RealSecure for NT
- Somarsoft's DumpACL, DumpEVT, DumpReg
- SCANNT, NTCrack, L0PHT Crack (Password Crackers)

PRICEWATERHOUSECOOPERS

Windows NT v5.0 Features

Some of the shortcomings relating to the Windows NT domain structure will be addressed with the implementation of the Active Directory structure in Windows NT v5.0. The new version of Windows NT is expected to include the following new features:

- A new GUI that will incorporate the Internet Explorer v4.0 front-end with Active Desktop.
- New X.500-style directory services called Active Directory, where each domain controller stores the entire directory database for the domain. Active Directory combines DNS and LDAP style directory information to create a hierarchical directory system.
- A Distributed File System that will enable multiple volumes on different machines to appear as a single logical volume.
- Windows NT v5.0 will implement Kerberos security using passwords and private encryption keys to protect the domain tree.
- Support for Plug and Play and for Advanced Power Management (APM).
- Common device drivers that will work on both Windows NT and Windows 98.

Reference Materials

Windows NT 4.0 Security Sites

The Microsoft Security Home Page at http://www.microsoft.com/security

Home Page includes the PricewaterhouseCoopers LLP. Security White Paper on how to secure Windows NT (http://www.microsoft.com/NTServer/security/techdetails/prodarch/CoopersLybrand.asp)

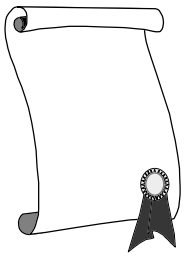
NTSecurity Web Site at http://www.ntsecurity.net

NTBugTraq Mailing List

The NTBugTraq is the Windows NT counterpart of the

BugTraq mailing list that is mainly for UNIX related bugs with impact on security.

Subscribe by sending a mail to LISTSERV@RC.ON.CA with the mail body of “SUB NTBUGTRAQ <e-mail address>”



Reference Materials (continued)

Windows NT Security Books from Microsoft Press

Windows NT 3.5 Guidelines for Security, Audit, and Control

Coopers & Lybrand L.L.P., Citibank, IIA, and Microsoft

ISBN 1-55615-814-9

Microsoft Windows NT 4.0 Security, Audit, and Control (Microsoft Technical Reference)

Coopers & Lybrand L.L.P. and Microsoft

ISBN 157231818X

http://www.amazon.com/exec/obidos/ASIN/157231818X/qid%3D917466678/002-2561692-2046839

http://mspress.microsoft.com/prod/books/1548.htm

Windows NT 5.0 Guidelines for Security, Audit, and Control

PricewaterhouseCoopers LLP and Microsoft

To be released after the release of Windows NT 5.0

PRICEWATERHOUSECOOPERS

Reference Materials (continued)

Windows NT 4.0 Security Books

Windows NT Security Handbook

Tom Sheldon

ISBN 0-07-882240-8

Internet Security with Windows NT

Mark Joseph Edwards

ISBN 1-882419-62-6

Windows NT Security Guide

Stephen A. Sutton (Trusted Systems Services, Inc.)

ISBN 0-201-41969-6

Windows NT Security

Charles B. Rutstein

ISBN 0-07-057833-8

PRICEWATERHOUSECOOPERS

In Conclusion

- Windows NT "hacking" programs are readily available
- Companies must evaluate business risks and implement appropriate countermeasures based on cost
- Do NOT assume your network is secure!

PRICEWATERHOUSECOOPERS

Questions and Answers

PRICEWATERHOUSECOOPERS