# Chapter 4 Windows NT/2000 Overview

# NT Concepts

#### Domains

- A group of one or more NT machines that share an authentication database (SAM)
- Single sign-on to access resources and services on various machines within domain
- Primary domain controller (PDC)
- Backup domain controller (BDC)
- Workgroups
- Network File Shares
  - C: net use \\ [IP address or hostname] \ [share name]
     [username]:[password]
- Service Packs (SP) and hot fixes

#### Windows NT System



### Windows NT Architecture

## Security Subsystem

- Aka Local Security Authority (LSA)
  - User mode subsystem verifying validity of user logon attempts
- Security Accounts Manager (SAM) database
  - Each line contains user name, SID, LM password representation, NT password hash
  - $C:\winnt\system 32\config\SAM$

### User Accounts

- Default Accounts
  - Administrator
  - Guest
- Securing Accounts
  - Renaming administrator account
  - keep guest account disabled
  - Create non-privileged account named Administrator to act as decoy

# Groups

- Local Groups
  - Administrator
  - Account Operators
  - Server Operators
  - Backup Operators
  - Print Operators
  - Replicator
  - Users
  - Guests
- Global Groups
  - Domain Administrators
  - Domain Users
- Principle of Least Privilege



Account Policy		×
Computer: EDWORKSTATION Password Restrictions Maximum Password Age O Password Never Expires O Expires In 90 Days Minimum Password Length O Permit Blank Password O At Least C Characters	Minimum Password Age Allow Changes Immediately Allow Changes In Days Password Uniqueness Do Not Keep Password History Remember Resword Sources	OK Cancel <u>H</u> elp
<ul> <li>○ No account lockout</li> <li>○ Account lockout</li> <li>Lockout after</li> <li>5 → bad logon</li> <li>Reset count after</li> <li>30 → r</li> <li>Lockout Duration</li> <li>○ Forever (until admin unlocks)</li> <li>○ Duration</li> <li>30 → minu</li> </ul>	attempts minutes tes	

Users must log on in order to change password

#### Figure 4.3 Account Policy for Windows NT

# Windows NT DomaintTrust Models

- No Trust
- Complete Trust
- Master Domain
  - Accounts Domain
  - Resource Domain
- Multiple Master Domain
  - multiple Accounts Domain



Audit Policy			×
Computer: EDWORKSTATION			ОК
C <u>D</u> o Not Audit			Cancel
Audit These Events:			
	Success	Failure	Help
Logon and Logoff			
Eile and Object Access			
Use of User Rights			
User and <u>G</u> roup Management			
Security Policy Changes			
<u>R</u> estart, Shutdown, and System			
Process Tracking		V	

Seven audit categoriesEvent log



#### Windows NT Supported File Systems

FAT
 – No access control

NTFS

- Supports access control



# **NTFS** File Permissions

- No access
- Read access
- Change
- Full control

### **NTFS Share Permissions**

- Used for remote access to file systems
- Based on Server Message Block (SMB) protocol (aka CIFS)
- Share Permissions types
  - No access
  - Read access
  - Change
  - Full control
- Null sessions
  - Remote SMB sessions requiring no username/password

#### Windows NT/2000 Network Security

- Supports challenge-response authentication
- Securing NT: A Step-by-Step Guide at www.sans.org
- Windows 2000 Security Checklist at <u>www.securityforum.org</u>
- VPN using Microsoft PPTP

## Remote Access Service (RAS)

- Allows remote dial-in of Windows clients
- RAS servers rely on SAM database for user authentication
- War dialers

### Windows 2000 Features

- Windows NT 5.0
- Kerberos server (KDC) for user authentication
- ♦ IPSec
- Layer 2 Tunneling Protocol (L2TP)
- Encryption File System (EFS)
- Mixed Mode vs Native Mode
- Authoritative domain controllers (no BDC)
- Active Directory

### Tree vs Forest Domain

#### ♦ Tree

- A linking of domains via trust resulting in a continuous name space that supports locating resources easily via Active Directory
- Root domain
  - Topmost domain
  - Name of child domain ends with the parent domain name

#### Forest

 Produces a non-contiguous name space by cross-linking domains via trus



# **Active Directory**

- Based on Lightweight Directory Access Protocol (LDAP)
- Massive data repository
  - Account info
  - Organization units (OU)
  - Security policies
  - Files/Directories
  - Printers
  - Services
  - Domains
  - Inheritance rules
- Supports Dynamic DNS (DDNS)
- User account passwords stored in file **ntds.nit** 
  - grabbed by pwdump3 and cracked via L0phtCrack

# Windows 2000 Security

- install Active Directory in separate partition
  - C: Boot and system files
  - D: Active Directory
  - E: User files and applications
- Physically secure Kerberos authentication server (Key Distribution Center)

Local Security Settings			_O×
$ Action View   \Leftrightarrow \Rightarrow   \textcircled{1}   \times $	6		
Tree	Policy 🔺	Local Setting	Effective Setting
Security Settings  Account Policies  Account Policies  Constraint Policy  Constraint Policy  Constraint Policy  Constraint Policy  Constraint Policies  Con	Image         Image	0 passwords remem 42 days 0 days 0 characters Disabled Disabled	0 passwords remem 42 days 0 days 0 characters Disabled Disabled

#### Figure 4.8 Windows 2000 security settings

# Securing Windows 2000

- Windows 2000 Security Configuration Tools GUI
- secedit command-line tool
- \%systemroot%\security\templates contains nine templates to set system security to highly secure, secure or basic
- ♦ 3 security groups
  - Domain Local (access restricted to resources within same local domain)
  - Global (allows resources in one domain to be accessed by users from another domain)
  - Universal (can contain users and groups from any domain in any forest)

**Organizational Units (OU)** Supports delegation of privileges Each OU can be assigned a level of privileges Inheritance of rights in OUs Children OUs below the parent can never be given more rights than the parent has Three levels of OUs should be maximum for optimal performance





Local Security Settings				기×
Action View				
Tree	Policy 🛆	Local Setting	Effective Setting	
B Security Settings	Access this computer from the net	Everyone,Users,Po	Everyone, Users, Power Users, Ba	
Account Policies	Act as part of the operating system			
E- 📴 Local Policies	BB Add workstations to domain			
庄 🛄 Audit Policy	Back up files and directories	Backup Operators,	Backup Operators, Administrators	
🖅 🚇 User Rights Assigr	Bypass traverse checking	Everyone,Users,Po	Everyone, Users, Power Users, Ba	,
E Gecurity Options	Change the system time	Power Users,Admini	Power Users, Administrators	
Public Key Policies	BB Create a pagefile	Administrators	Administrators	
∃ - 3 IP Security Policies on	聞Create a token object			
	Create permanent shared objects			
	BBDebug programs	Administrators	Administrators	
	Deny access to this computer from			
	BBDeny logon as a batch job			
	- Deny logon as a service			
	- 떒Deny logon locally			
	Enable computer and user account			
	题Force shutdown from a remote sy	Administrators	Administrators	
	Generate security audits			
	Increase quotas	Administrators	Administrators	
	Increase scheduling priority	Administrators	Administrators	
	Load and unload device drivers	Administrators	Administrators	
	腾Lock pages in memory			
	Log on as a batch job			
	腾Log on as a service			
	j;;;Elog on locally	*5-1-5-21-1275210	*5-1-5-21-1275210071-158081	
	Manage auditing and security log	Administrators	Administrators	
	题Modify firmware environment values	Administrators	Administrators	
	Beile single process	Power Users,Admini	Power Users, Administrators	
	题Profile system performance	Administrators	Administrators	
	Remove computer from docking st	Users, Power Users,	Users, Power Users, Administrators	
	Replace a process level token			
	Restore files and directories	Backup Operators,	Backup Operators, Administrators	
	Shut down the system	Users,Power Users,	Users,Power Users,Backup Oper	
	Synchronize directory service data			
↓ >	题 Take ownership of files or other o	Administrators	Administrators	

#### Figure 4.10 User Rights in Windows 2000

#### RunAs command in Windows 2000

 Allows privileged users to execute programs in a non-privileged context

Link in	🖾 Command Prompt
No. And And	Microsoft Windows 2000 [Version 5.00.2195] (C) Copyright 1985-2000 Microsoft Corp.
	C:\>runas RUNAS USAGE:
	RUNAS [/profile] [/env] [/netonly] /user: <username> program</username>
	<pre>/profile if the user's profile needs to be loaded /env to use current environment instead of user's. /netonly use if the credentials specified are for remote access only. /user {UserName} should be in form USER@DOMAIN or DOMAIN\USER program command line for EXE. See below for examples</pre>
	Examples: > runas /profile /user:mymachine\administrator cmd > runas /profile /env /user:mydomain\admin "mmc %windir%\system32\dsa.msc" > runas /env /user:user@domain.microsoft.com "notepad \"my file.txt\""
	NOTE: Enter user's password only when prompted. NOTE: USER@DOMAIN is not compatible with /netonly.
	C:\>_

### Windows 2000 Trust

- Based on Kerberos instead of challengeresponse in NT
- When new domain is added to tree or forest, that domain automatically trusts all other domains and is trusted by all other domains within that tree or forest

#### Windows 2000 Encrypted File System (EFS)

- Automatically and transparently encrypts any stored files using DES encryption
- Files transmitted over the network are not encrypted
- DES encryption algorithm old

### Network Security in Windows 2000

- Windows NT PPTP
  - For Windows 2000 Mixed mode
  - Described in <u>www.counterpane.com/pptp-paper.html</u>
- Windows 2000 PPTP
  - For Windows 2000 Native mode
  - Not interoperable with other PPTP implementations

#### ♦ IPsec

Works only from Windows 2000 host to Windows 2000 host