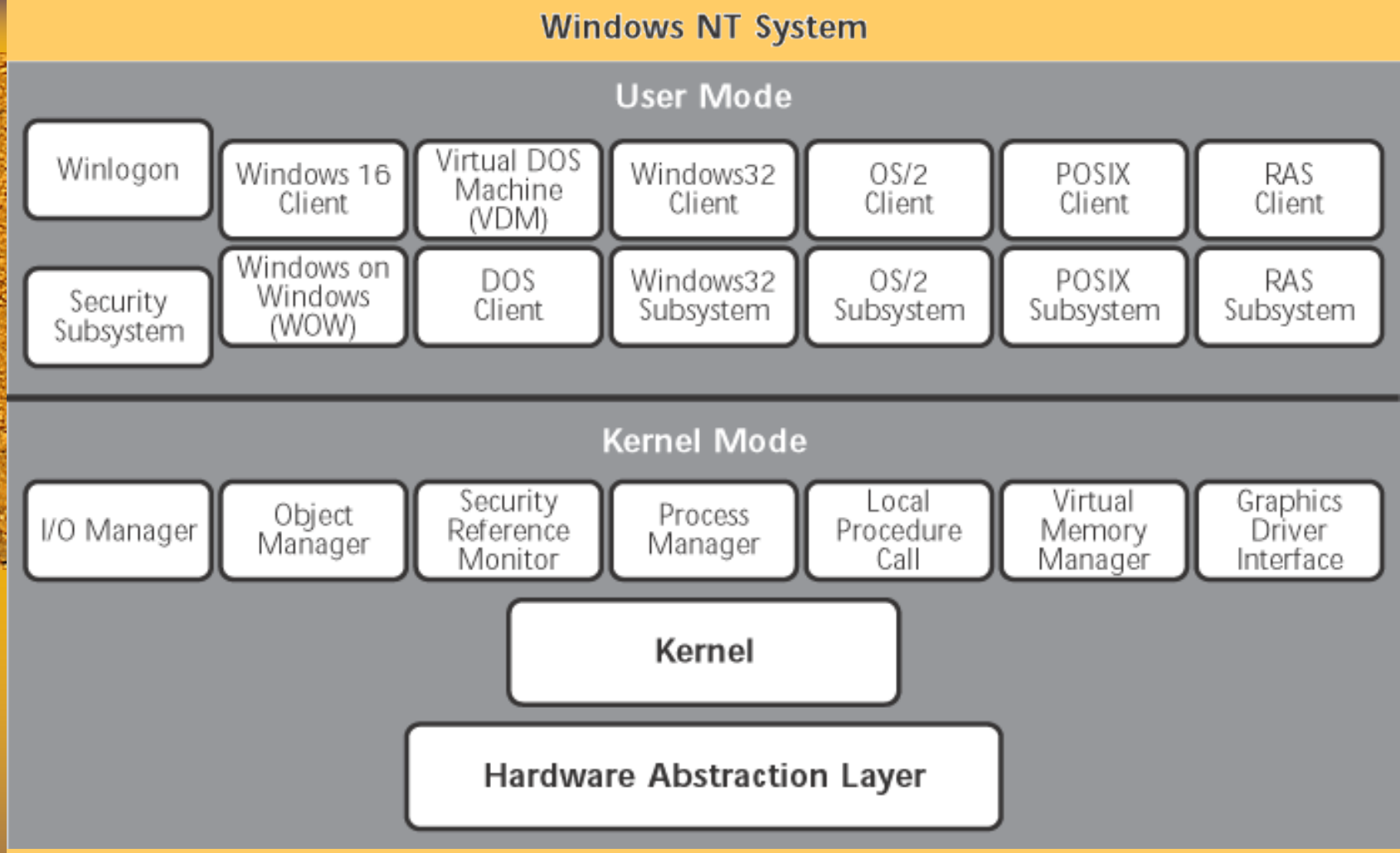
Chapter 4 Windows NT/2000 Overview

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 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\system32\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

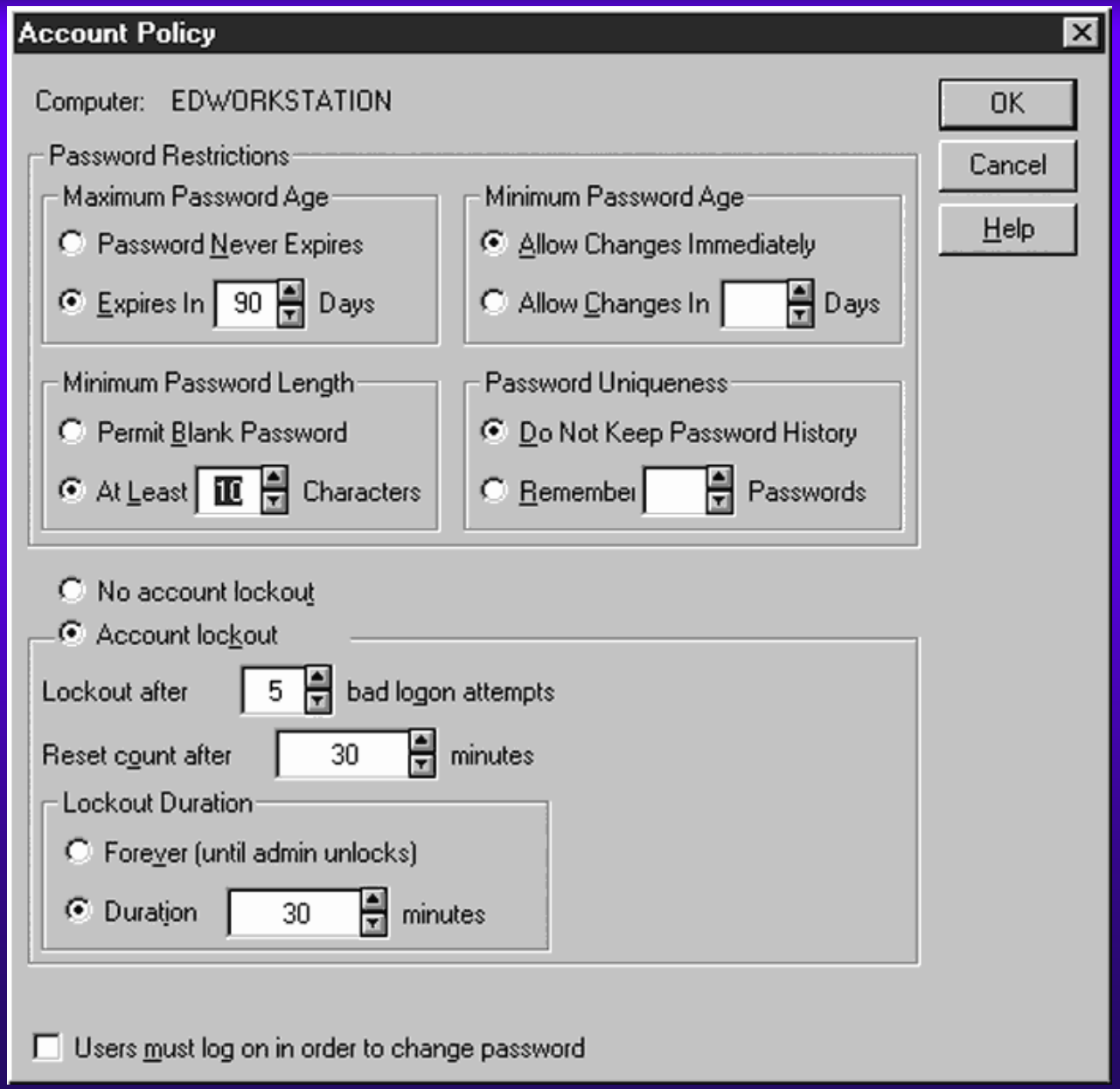
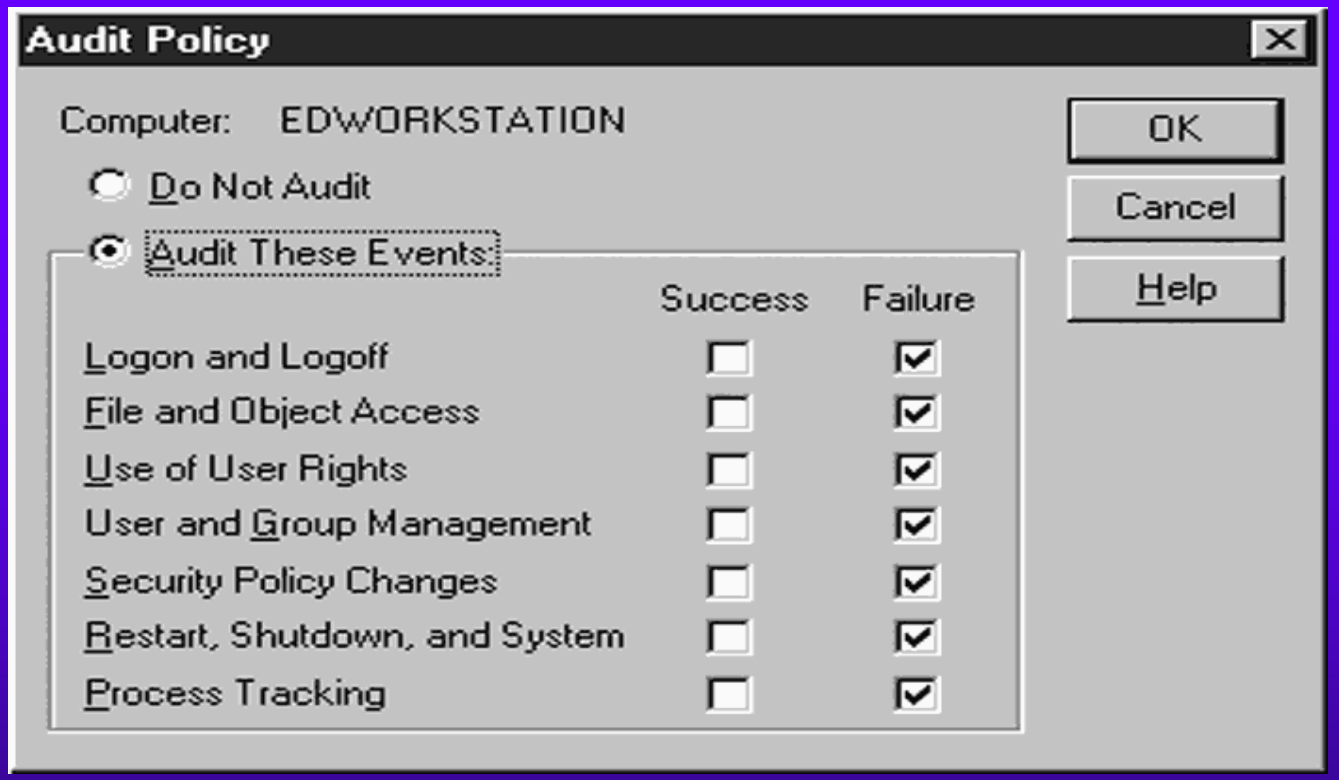


Figure 4.3 Account Policy for Windows NT

Windows NT DomaintTrust Models

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

Auditing



- Seven audit categories
- Event 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 www.securityforum.org
- 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

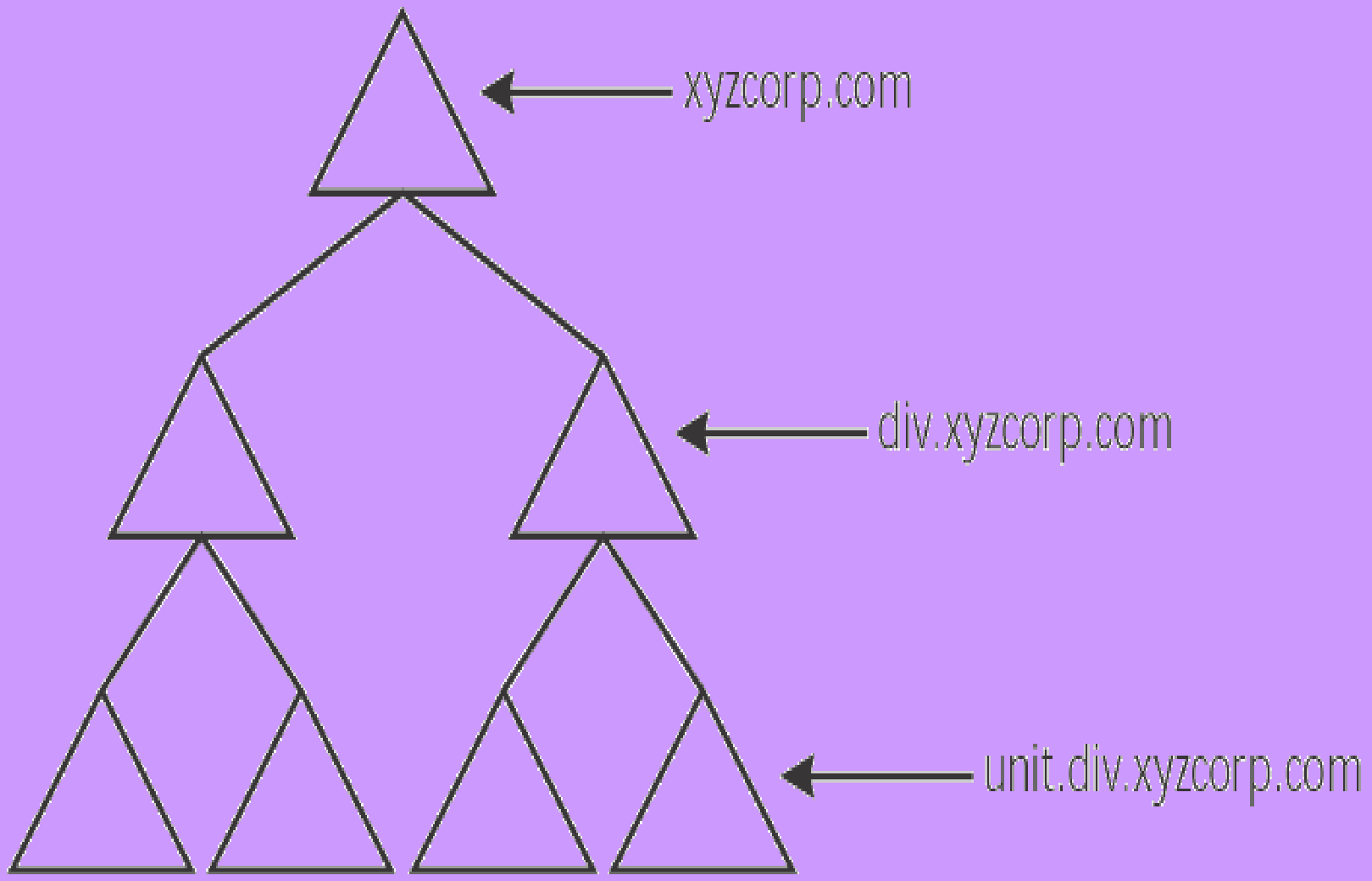
Windows 2000 Features

- 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

Figure 4.7 Depiction of a Windows 2000 tree



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)

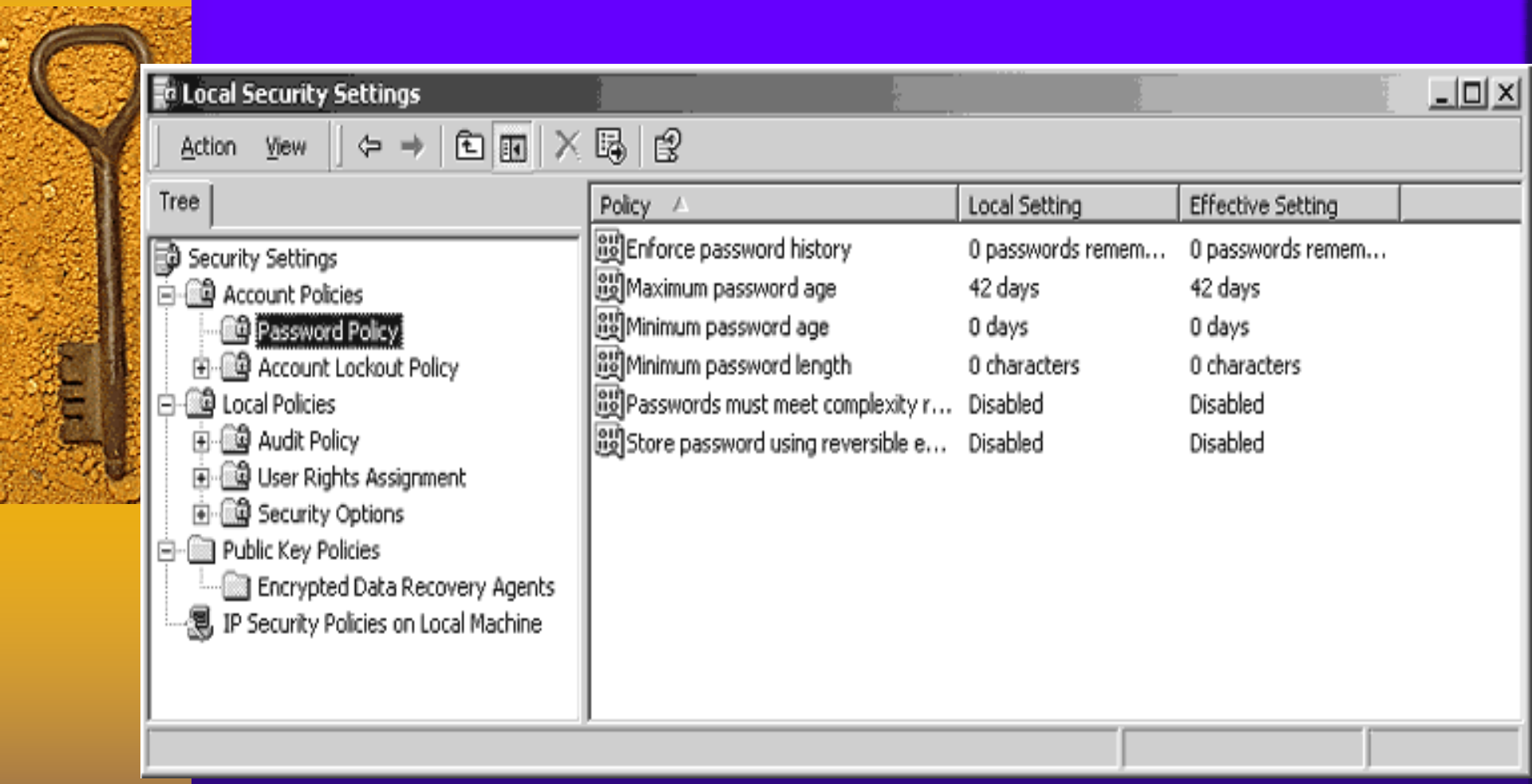


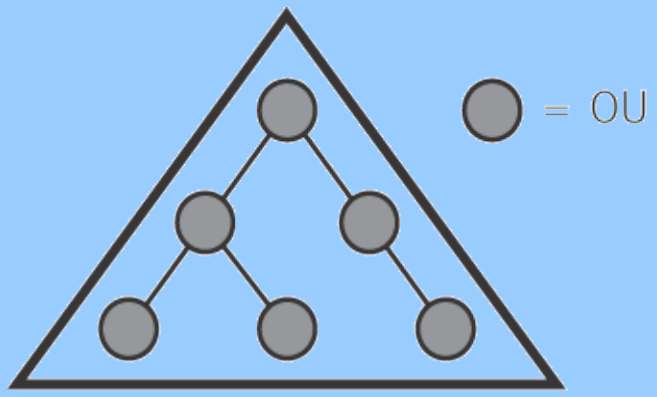
Figure 4.8 Windows 2000 security settings

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

Action View

Tree

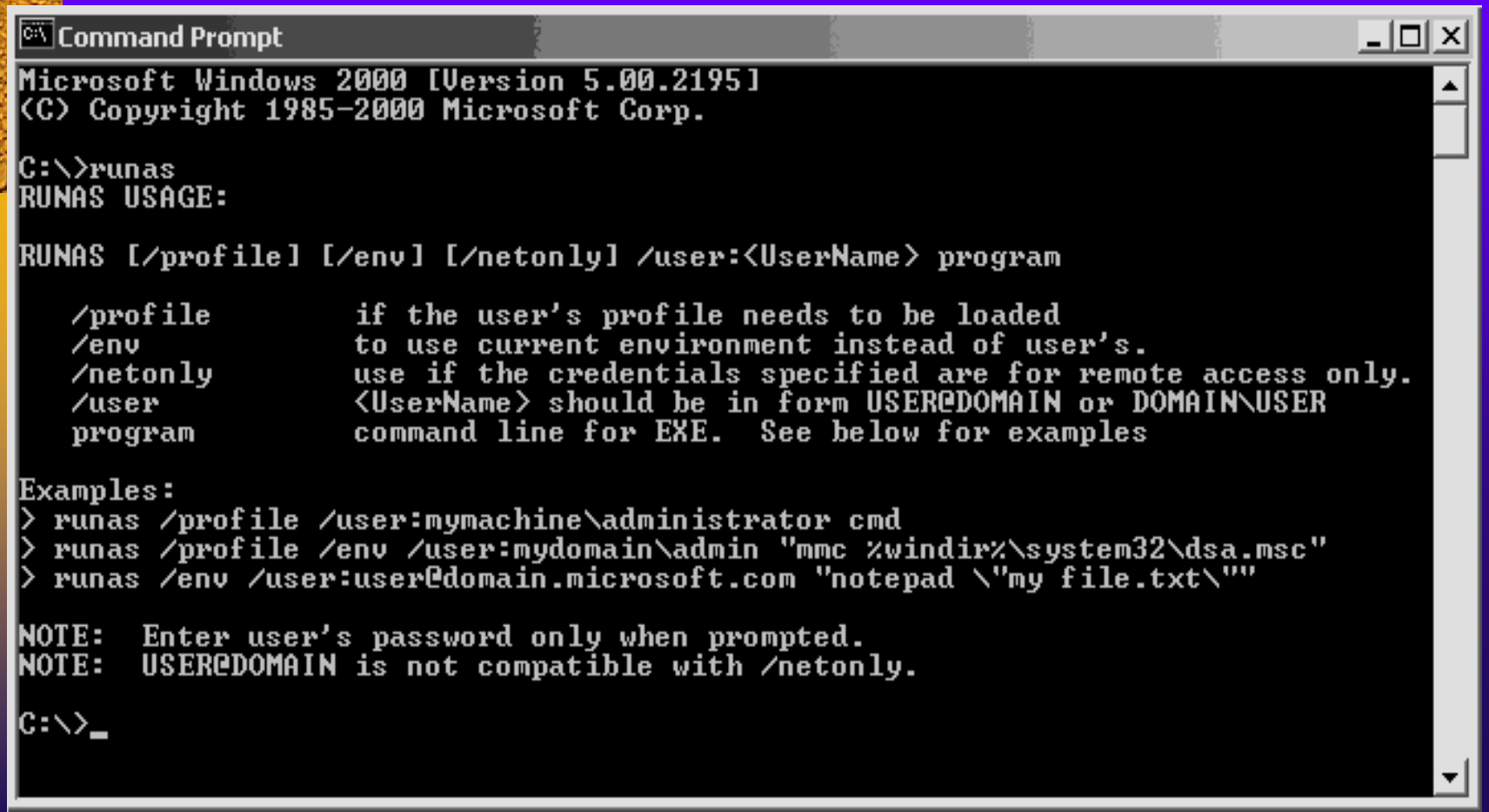
- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assigr
    - Security Options
  - Public Key Policies
  - IP Security Policies on

Policy	Local Setting	Effective Setting
Access this computer from the net...	Everyone,Users,Po...	Everyone,Users,Power Users,Ba...
Act as part of the operating system		
Add workstations to domain		
Back up files and directories	Backup Operators,...	Backup Operators,Administrators
Bypass traverse checking	Everyone,Users,Po...	Everyone,Users,Power Users,Ba...
Change the system time	Power Users,Admini...	Power Users,Administrators
Create a pagefile	Administrators	Administrators
Create a token object		
Create permanent shared objects		
Debug programs	Administrators	Administrators
Deny access to this computer from...		
Deny logon as a batch job		
Deny logon as a service		
Deny logon locally		
Enable computer and user account...		
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
Lock pages in memory		
Log on as a batch job		
Log on as a service		
Log on locally	*S-1-5-21-1275210...	*S-1-5-21-1275210071-158081...
Manage auditing and security log	Administrators	Administrators
Modify firmware environment values	Administrators	Administrators
Profile single process	Power Users,Admini...	Power Users,Administrators
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		
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



Windows 2000 Trust

- Based on Kerberos instead of challenge-response 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 www.counterpane.com/pptp-paper.html
- 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