

IT Service Delivery And Support Week Four - OS

IT Auditing and Cyber Security

Fall 2016

Instructor: Liang Yao

What is an Operating System (OS)?

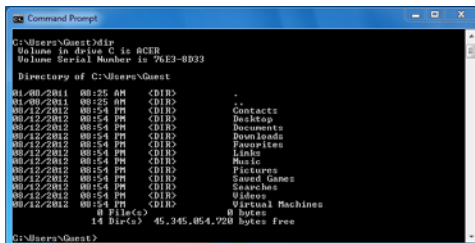
- * OS is a software that designed to run on specific hardware
- * OS controls hardware
 - * Input/Output
 - * Storage
 - * External devices
- * OS interfaces between the applications and hardware
 - * User interface (command Line or GUI)
 - * Application support
 - * communications

OS Layers

- * User Interface
- * File Management System
- * Input / Output
- * Memory Management
- * The Kernel

OS Layers (continue)

- * User Interface: is the software layer which allows the user to interact directly with the operating system
- * Command Line: “C:\ dir windows /p” (e.g. MS-Dos)
- * GUI: Parameters and switches are replaced by **dialogue boxes**, check-box, radio button, drop-down list box, etc. (Windows, Mac OS)

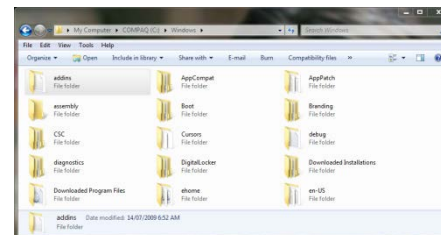


```
Command Prompt
C:\Users\Guest>dir
Volume in drive C is RCEB
Volume Serial Number is 76E3-8D33

Directory of C:\Users\Guest

01/08/2011  08:25 AM    <DIR>      .
01/08/2011  08:25 AM    <DIR>      ..
01/12/2012  08:54 PM    <DIR>      Contacts
01/12/2012  08:54 PM    <DIR>      Desktop
01/12/2012  08:54 PM    <DIR>      Documents
01/12/2012  08:54 PM    <DIR>      Downloads
01/12/2012  08:54 PM    <DIR>      Favorites
01/12/2012  08:54 PM    <DIR>      Links
01/12/2012  08:54 PM    <DIR>      Music
01/12/2012  08:54 PM    <DIR>      Pictures
01/12/2012  08:54 PM    <DIR>      Saved Games
01/12/2012  08:54 PM    <DIR>      Searches
01/12/2012  08:54 PM    <DIR>      Users
01/12/2012  08:54 PM    <DIR>      Virtual Machines
0 Files(s)
14 Dir(s)  45,345,854,728 bytes free

C:\Users\Guest>
```



OS Layers (continue)

- * File Management System: is the layer of system software responsible for organizing and managing the storage of data on permanent media (not on memory).
- * Windows File System Types
 - * The **File Allocation Table (FAT)/Fat32** file system was designed for **small disks** and **simple directory structures**.
E.g. Windows 95/98
 - * The **Windows NT file system (NTFS)** offers major improvements over FAT in the areas of performance, reliability and compatibility.
 - * File level security
 - * Encryption
 - * Disk quotas

OS Layers (continue)

- * Input/output: controls all physical communication with external devices, such as disk drives, keyboard, printers and displays.
- * **Character I/O**, where the data is in the form of single numbers or characters (e.g. keys pressed on a keyboard): keyboard, mouse, joysticks, communications ports and printers
- * **Block I/O**, where larger blocks of data are to be transferred at the same time (e.g. reading or writing a block from disk)
- * **Device Management**: (e.g. printers, scanners)

OS Layers (continue)

- * Memory Management:

- * *MM is responsible for sharing the physical memory of the computer between processes and handling programs which require more memory than physically available.*
- * *This layer is also responsible for ensuring that the memory allocated to any program is protected against access by other programs.*
 - * *Virtual Memory/Page files: same size*
 - * *Segmentation: variable sized blocks*

OS Layers (continue)

- * The Kernal: acts as a regulator for the whole system, controlling the allocation of time slices to users or processes and ensuring that resources are allocated fairly.
- * multi-tasking
- * process control
- * exception handling (or error handling)
- * interrupt processing

OS Types

- * **Centralized Environment**
 - * Mainframe (e.g. IBM zSeries, System9, System10)
 - * Mid-Size Server: (e.g. IBM iSeries, AS/400e, etc.)
- * **Distributed Environemnt**
 - * Unix/Linux (Solaris, HP-UX, AIX, Red Hat, etc.)
 - * Windows (Desktop & Server versions)
 - * Apple OS
 - * Mobile OS (iOS, Android, Microsoft Windows Mobile)
 - * Blackberry

Distributed Environment Pros. Vs. Cons.

Advantages

- * Leverage desktop computing
- * Enable some systems to be delivered sooner than traditional mainframe systems
- * Uses graphic user interface
- * Free up expensive mainframe computing cycle – might delay or lengthen mainframe upgrade cycle
- * User empowerment

Distributed Environment Pros. Vs. Cons.

Advantages

- * May create bottlenecks in network
- * Applications take longer to deliver because they are more complex
- * Uses command line and text base interface
- * Additional cost of desk top and tier-two servers are not accounted for in the long-term budget
- * Decentralized control
- * Security in the client/server environment might not be as strong as mainframe security

Risks Associated with OS

- * Security Risks
- * Change Management Risks
- * Monitoring Risks
- * Availability Risks

Risks Associated with OS

Security Risks

Weak Design and Implementation can lead to a compromise of the system by potentially allowing unauthorized access.

- * No Policy or procedures establishing roles and responsibilities.
- * No Windows hardening standards for services, registry parameters, changing passwords for default accounts, and security settings as a baseline.
- * Poor Password policies
 - * Administrator accounts passwords do not expire.
 - * User accounts (default domain policy) bypass default domain policy.
 - * Service Accounts (bypass default domain policy).
- * Poor Group Policy Management to push policies to servers and workstations.

Lack of Administration of accounts can lead to a compromise of system integrity by potentially allowing unauthorized access gain access to sensitive areas.

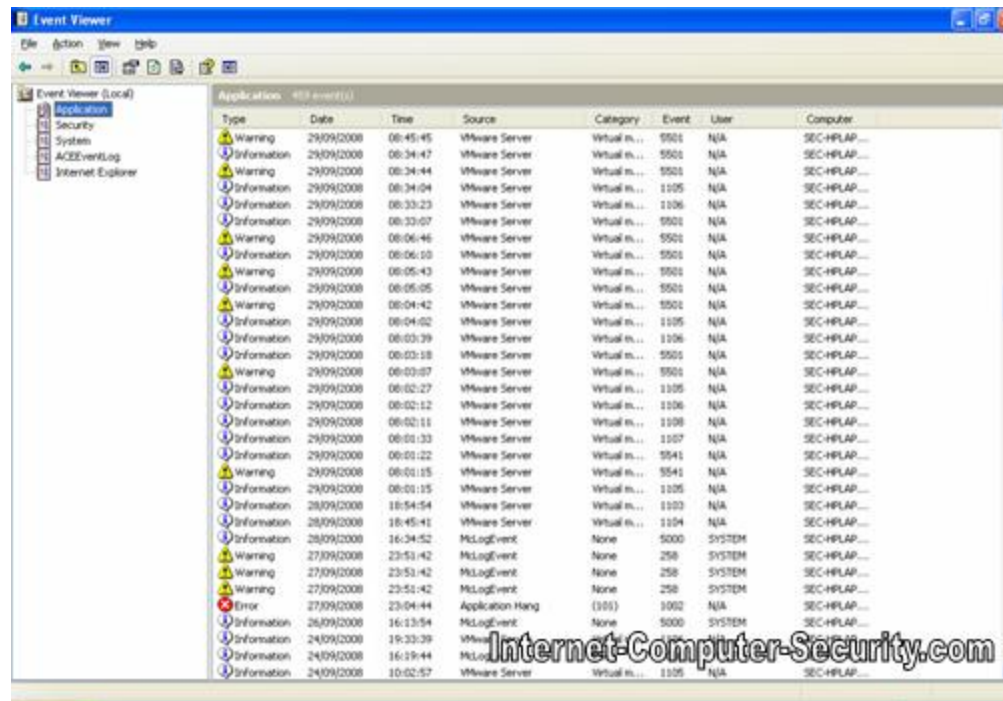
- * No formal policy for authorizing accounts.
- * Administrator powers are NOT limited to a privileged few accounts.
 - * Unauthorized access or access granted is too excessive.
- * No formal recertification of accounts by owners.

Risks Associated with OS

System Monitoring

- Monitoring of Administrator accounts and activities
- Event Logs
 - What's been turn-on?
 - Threshold and filtering tools
 - Who actually reads these?
- Monitoring access to sensitive directories

Risks Associated with OS



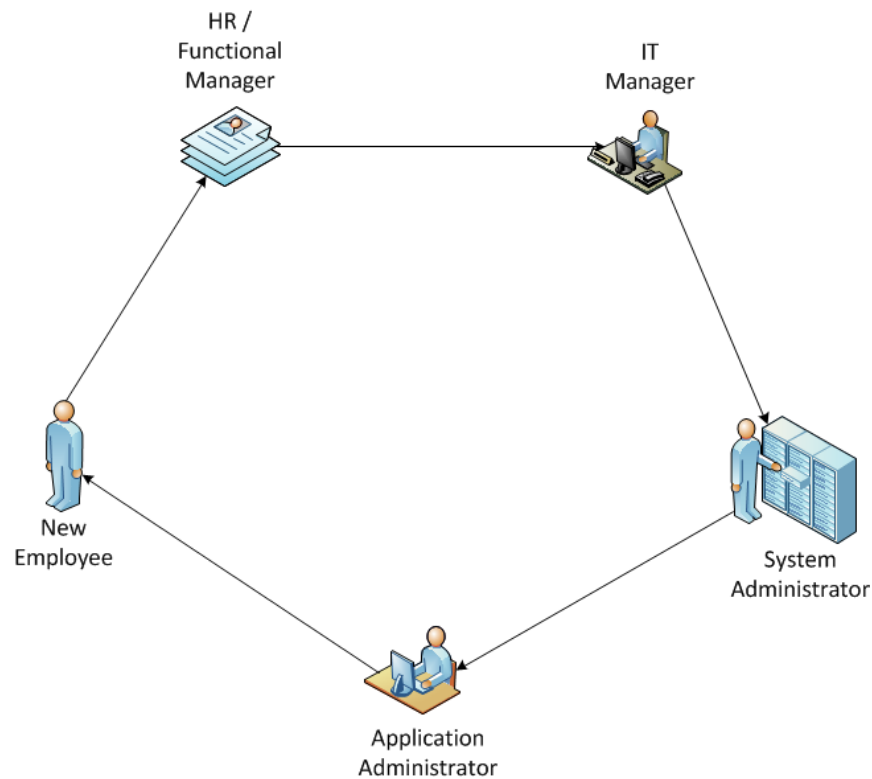
Risks Associated with OS

Change Management

Lack of formal change management procedures could lead to a compromise of system integrity by allowing unauthorized access gain access to resources

- * Patch Management
- * Configuration Management
- * Release Management
- * Emergency Changes

Controls – User Provisioning



Controls – Role Based Access

- * Principles
 - * Creating “roles” based on job functions
 - * Granting “permissions” to “roles”
 - * Assigning “individuals” to “roles” or “groups”
- * Practices
 - * Not assigning rights to individuals
 - * Creating security groups
 - * Adding/removing users from the security groups
 - * Granting permissions to security groups
- * Don't forget “SOD” while practicing Role based access

Controls – Group Policy (AD)

*“**Group Policy** is a hierarchical infrastructure that allows a network administrator in charge of Microsoft's Active Directory to implement specific configurations for users and computers.” -*

Controls – Group Policy (AD)

- * Creating multiple policies
- * Policies can be turned on or off
- * Policies are “inherent” and “cumulative”
- * Local Policy vs. Domain Policy (local ->Site->Domain -> OU->Child OU's.
- * Policy Replication (AD and SYSVOL)

Sample Check-list for OS Review

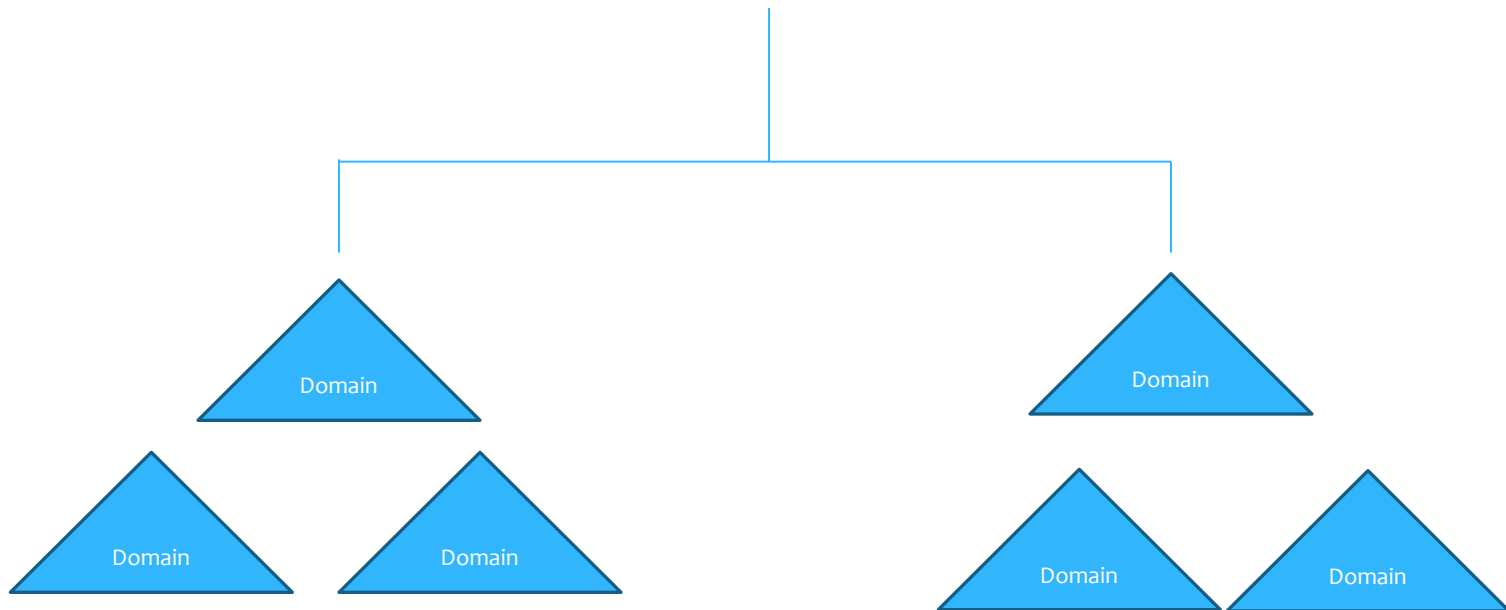
- * System Hardening standards, build document and build process
- * Configuration – unused services/client firewall
- * OS version and Patch level
- * Anti-virus/malware with latest .DAT
- * Password setting and/or other authentication methods
- * Remote access (internal users and vendors)
- * Audit trail and monitoring
- * Disk encryption for laptops
- * Physical security

Windows Active Directory

- * **Definition** - Active Directory is a centralized and standardized system that automates network management of user data, security, and distributed resources, and enables interoperation with other directories. Active Directory is designed especially for distributed networking environments.

Windows Active Directory

Forest



Windows Active Directory

AD Key Characters

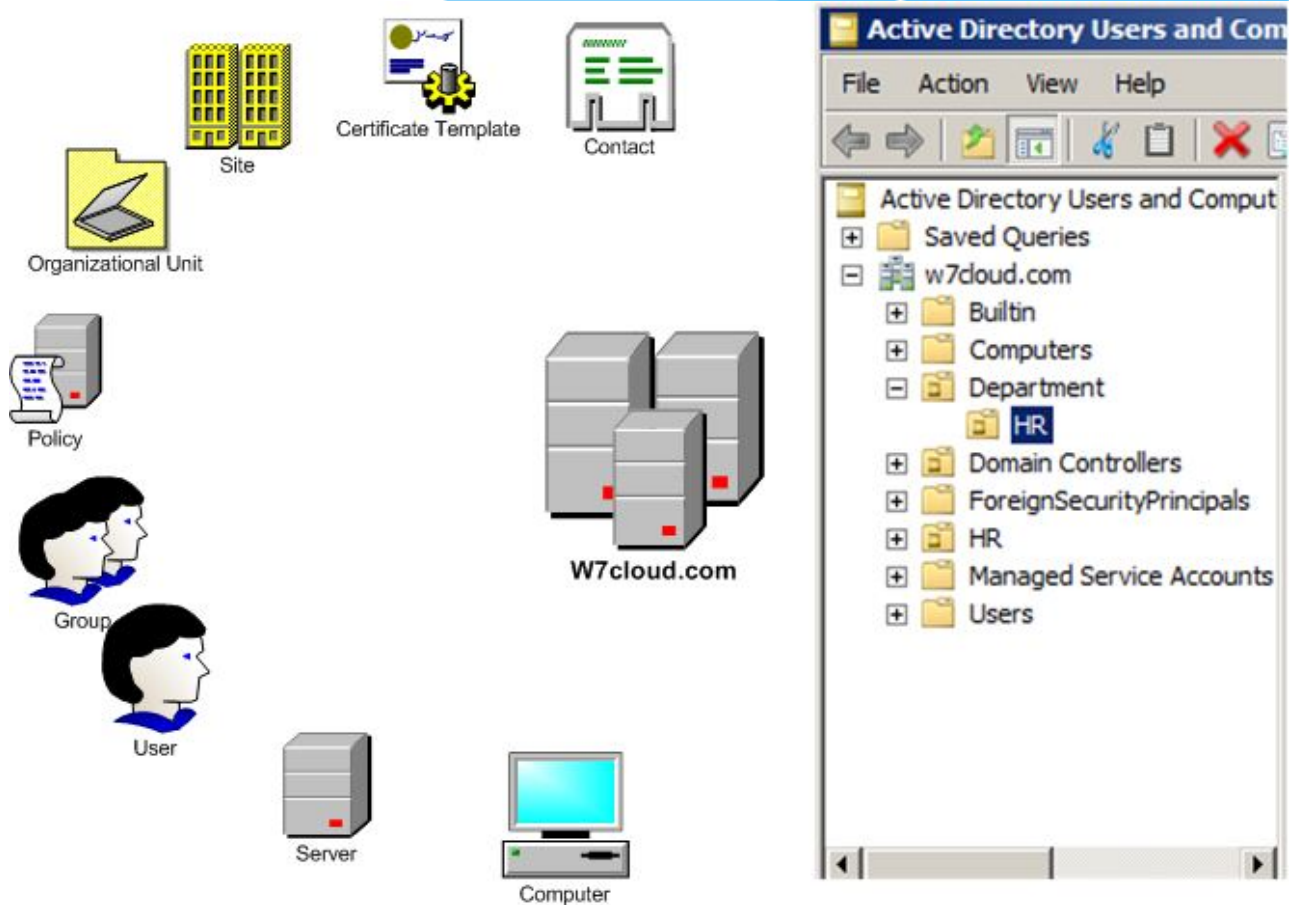
- * A hierarchical structure for containers and objects
- * Each domain has a unique domain name
- * Has a security mechanism to authenticate and authorize access to domain resources
- * Has policies to show how functionality is allowed or restricted for all domain objects such as users, computers

Windows Active Directory

AD Objectives

- * Physical entities within the AD
 - * Samples: forest, domain, organizational units, users, contacts, computers, shared folders, printers, sites, subnets, etc.
- * Obj. can be described by a set of attributes
 - * e.g. User: name, location, department, etc.
- * Container Objs. can contain other objectives
- * Leave Obj. can not contain other objectives
- * Obj. can be authenticated and assigned permission
- * Each obj. has a:
 - * GUID: 128 bit global unique identifier
 - * SID: security identifier

Windows Active Directory



Windows Active Directory

AD Objectives

- * Information and data exchange can happen only between the objectives inside a forest
- * To communicate with objects in other forests, explicitly created Forest Level trusts are required
- * Can contain one or more domain or a combination of domains or domain trees
- * The schema or design of an AD is consistent through out the forest

Windows Active Directory

Domains

- * Logical group(s) of objects
- * Administrative boundary for objects
- * A domain can contain unlimited number of objects
- * Objects need not be in a same physical location
- * Domain controller is the domain's Supreme Authority
- * Domain controller is responsible for all the authentications, authorizations, additions, definitions, edits, modifications inside a domain
- * User can log on to a domain from any locations and any computers that belong to that domain
- * All objects can be linked to policies and be assigned rights at domain level or at the individual level

Windows Active Directory

AD Organizational Units (OUs)

- * Can only appear inside a domain
- * Can be used to denote a department, a location, a team/group or a function
- * Each OU is unique inside a domain
- * Contains other objects
- * Can contain “child” OUs
- * OU level group policies
- * Delegated OU Administrators

Windows Active Directory

AD Users Accounts

- * Part of the Institution
- * Unique IDs in the domain
- * Access the domain's resources
- * Authorizations based access (via ACL)
- * Unique SID (different from Username)
- * Account is unique and is secure by a password

Windows Active Directory

AD Computers

- * Individual computers and servers which a part of the network (join the domain)
- * Unique computer account
- * Sever: domain controller or stand alone member server

Windows Active Directory

AD Groups

- * Contains users and computers
- * Permissions and restrictions should be placed on the group level and apply to all its members
- * Types of groups
 - * Security group – grant permission
 - * Distributed group – email
- * Group scope
 - * Domain local group: to give access resources in the same domain as the group, but users can belong to other domains
 - * Global group: to give access to resources that are in different domains to users from a specific domain
 - * Universal group: to give access to resources located in different domains to a group of users from different domains

Windows Active Directory

Why Using AD?

- * Layers of security
 - * Computer based security policy
 - * Administrative controls
 - * Physical Security
- * Easy to administrate a large number of objects
- * Easy, efficient search function
- * Centralized service management and storage
- * Single Sign On (SSO)
- * Individual and Mandatory user profiles – consistency and easy to restrict
- * Centralized auditing...

Unix System Audit

- * System Access Review:
 - * Privileged Access (root)
 - * Default System Accounts (reason for not disabling those accounts?)
 - * Vendor Accounts (access tracking and monitoring)
 - * .netrc files – containing unencrypted passwords; login and initialization information used by auto-login process (why are .netrc files allowed?)

Unix System Audit

- * User Account Review:
 - * List of active user and group accounts
 - * Account creation and decommissioning process
 - * Password security and settings
 - * /etc/passwd file
 - * UMASK

Unix System Audit

- * System Build Standards
- * Patch Process
- * Vulnerability Scan
 - * Unused services
 - * ftp/spool/telnet/rlogin, etc.
 - * Login as “root”
 - * IP filter/ firewall rules
 - * Remote access

Password File Sample

- * The `/etc/passwd` file is used to keep track of every registered user that has access to a system.
- * The `/etc/passwd` file is a colon-separated file that contains the following information: User name
 - * Encrypted password
 - * User ID number (UID)
 - * User's group ID number (GID)
 - * Full name of the user (GECOS)
 - * User home directory
 - * Login shell

Password File Sample

The following is an example of an /etc/passwd file (AIX version):

```
root!:0:0:::/usr/bin/ksh
daemon!:1:1::/etc:
bin!:2:2::/bin:
sys!:3:3::/usr/sys:
adm!:4:4::/var/adm:
uucp!:5:5::/usr/lib/uucp:
guest!:100:100::/home/guest:
nobody!:4294967294:4294967294::/
lpd!:9:4294967294::/
lp:*:11:11::/var/spool/lp/bin/false
invscout*:200:1::/var/adm/invscout:/usr/bin/ksh
nuucp*:6:5:uucp login user:/var/spool/uucppublic:/usr/sbin/uucp/uucico
paul!:201:1::/home/paul:/usr/bin/ksh
jdoe*:202:1:John Doe:/home/jdoe:/usr/bin/ksh
```

UMASK

- * “The **umask** command is used to control the file mode creation mask, which determines the initial file permissions for newly created files and folders. It is **defined** in the POSIX.1 specification and available on Unix-like operating systems.”
- * RWX (individual)RWX (group)RWX (World/everyone)
- * Read = 4; Write = 2; Execute = 1
- * Umask 000 >>> rwx|rwx|rwx Everyone has Full Access
- * Umask 002 >>> -rwx|rwx|r-x
- * Umask 003 >>> -rwx|rwx|r—
- * Umask 022 >>> -rwx|r-x|r-x
- * Umask 023 >>> -rwx|r-x|r—
- * Umask 027 >>> -rwx|r-x|---
- * Umask 037 >>> -rwx|r-|---
- * Umask 077 >>> -rwx|---|---

good
better
best