FANSHAWE

INFO-6003

O/S & Application Security

Week 04

Agenda

- Test-01 Reminder
- Windows Security
- WSUS
- Windows Security Architecture

Windows Security

Windows Security

- It used to be assumed that the Microsoft operating system is insecure
  - More true in the early days Win95/98 & WinNT 4.0
- It is the most popular operating system and has millions of users
- Used mostly by non technical users who are unaware of the dangers
- Even the most secure OS will still be exploited if hackers can trick users into doing something they shouldn’t

Windows Security

- Trade off ease of use and security
- Many applications and services have been installed by default to make it easier for the user
  - Fewer user frustrations & support calls
- Leads to situations where the vulnerability could be in a service installed by default but not used by the user as they aren't even aware it exists

Windows Security

- Targeted by writers of malware because they would get the most number of computers exploited
- It is estimated that Windows Operating Systems make up over 70% of the total O/S market share

Windows Security

- Windows applications such as Internet Explorer (IE) were historically the most widely used and therefore biggest target for attack
- Historically, users needed to log on as administrators to ensure applications would run correctly
  - Most users still do

Windows Security

- Internet Explorer (IE) was also accessed due to some of the functions it did without user knowledge
- IE stored information such as what files were accessed on the O/S file system
- Could be a gold mine of information for attackers as well as Computer Forensics Investigators

Windows Security

- Some Windows security problems are caused by backwards compatibility demanded by users
- Users expect the software that ran on their old computer to run on their new computer
  - Leads to those situations where applications need administrator privileges to run

Windows Security

- In Windows versions prior to Vista & Win2008 all services started in session 0, kernel mode
- All applications started by the 1st logged on user also ran in session 0
- Lead to the problem of shatter attacks where applications could get elevated privileges by accessing other applications

Windows Security

- 3rd party device drivers were written to need kernel access to run
- "According to Microsoft and Mark Russinovich 99% of Blue screens are caused by incorrectly written 3rd party device drivers"
  - Windows Vista Security
    - Roger Grimes & Jesper Johansson

Windows Security

- Windows specific privilege escalations
  - Most applications run in the security context of the user that launched the application
  - If a hacker takes over an application they gain the permissions and privileges of the user
- Hackers however have found security flaws that allowed them to launch applications, as a non-privileged user, that Windows would then run with elevated privileges

Windows Security

- An example of privilege escalation was a user using the Task Scheduler (at.exe) command to start a command prompt
  - The command prompt ran with System context
  - The command prompt had full system access
- Another example was the Windows help files that all ran with system context even if user starting the app had limited privileges

Windows Security

- You will execute Privilege escalation attacks in future labs done in the second semester of the ISM program
- Typically once a system such as Windows 7 is exploited, the attacker will seek to escalate their privileges on that system and eventually Network Administrator level access

Windows Server Update Services

WSUS

- The “Windows Update” service and the “Windows Server Update Services” assist with the regular maintenance of Microsoft software, and should be configured and used
- Many other third-party applications also provide automatic update support, and these should be enabled for selected applications

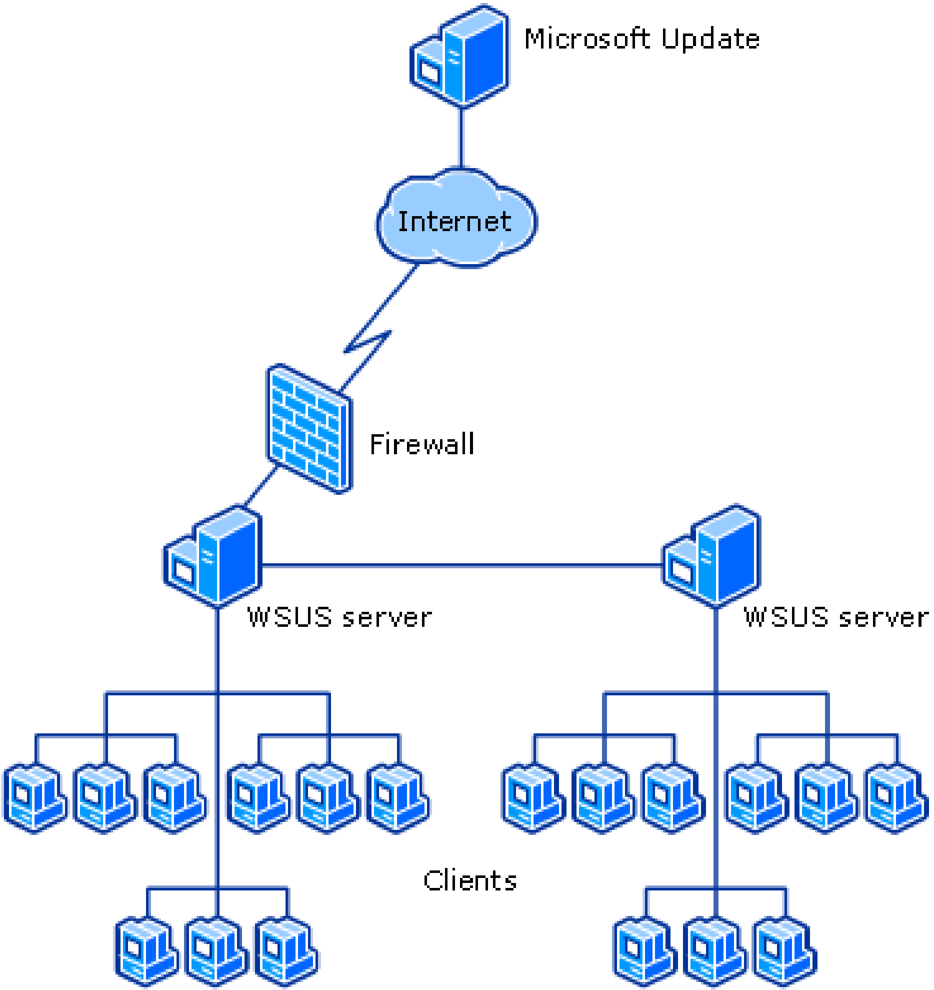
WSUS

- Allows organizations to control how updates are deployed in their environment
- Benefits of WSUS
  - Central Management of OS Updates
  - Central Management of Software Updates
  - Control over when updates are applied
  - Client internet access isn't required
  - Reduce bandwidth usage

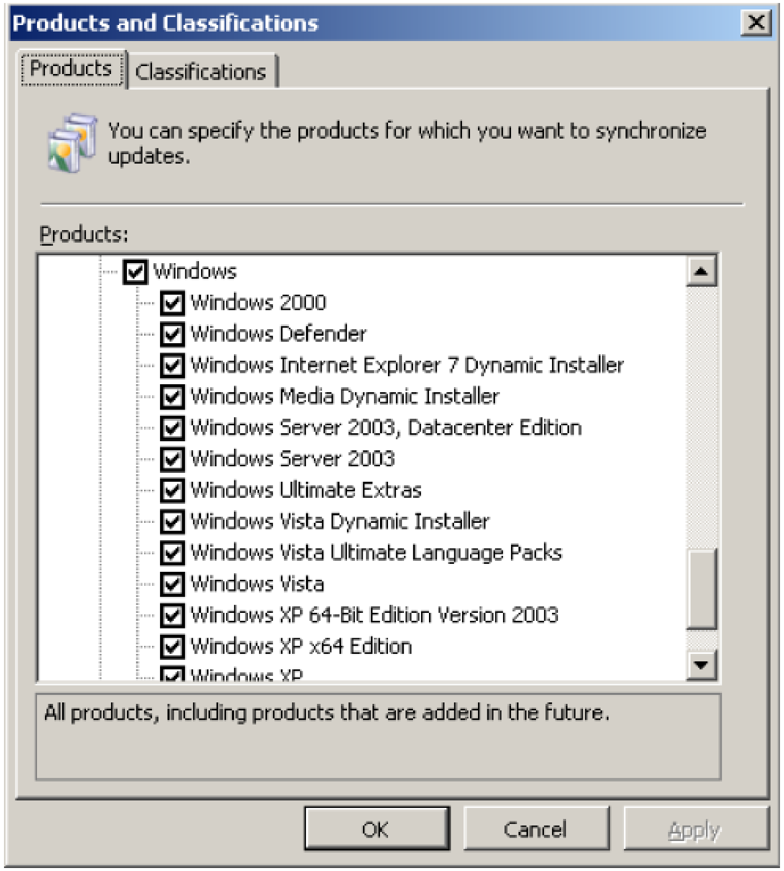
WSUS Components

- Microsoft Updates
  - Microsoft Web site that distributes updates
- Windows Server Update Services server
  - Distributes updates to clients in any domain in the forest
  - Distributes updates to other WSUS servers
  - One server MUST get updates from Microsoft
- Automatic Updates
  - Client computer component built into Windows OSs

WSUS Components



Products & Classifications



Products and Classifications

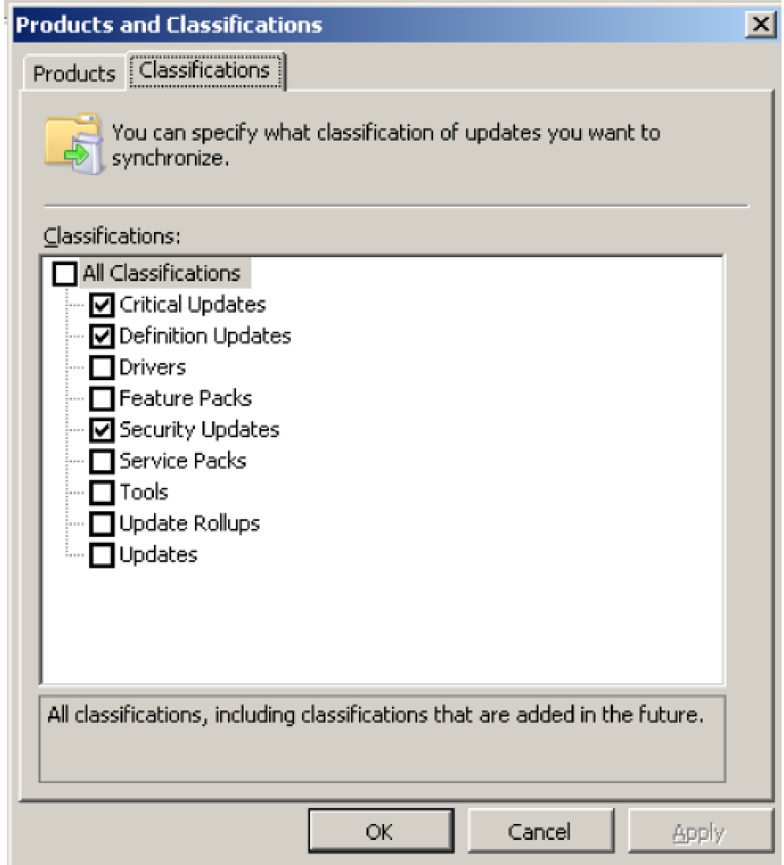
Products | Classifications

You can specify the products for which you want to synchronize updates.

Products:

- ☑ Windows
  - ☑ Windows 2000
  - ☑ Windows Defender
  - ☑ Windows Internet Explorer 7 Dynamic Installer
  - ☑ Windows Media Dynamic Installer
  - ☑ Windows Server 2003, Datacenter Edition
  - ☑ Windows Server 2003
  - ☑ Windows Ultimate Extras
  - ☑ Windows Vista Dynamic Installer
  - ☑ Windows Vista Ultimate Language Packs
  - ☑ Windows Vista
  - ☑ Windows XP 64-Bit Edition Version 2003
  - ☑ Windows XP x64 Edition
  - ☑ Windows XP

All products, including products that are added in the future.



Products and Classifications

Products | Classifications

You can specify what classification of updates you want to synchronize.

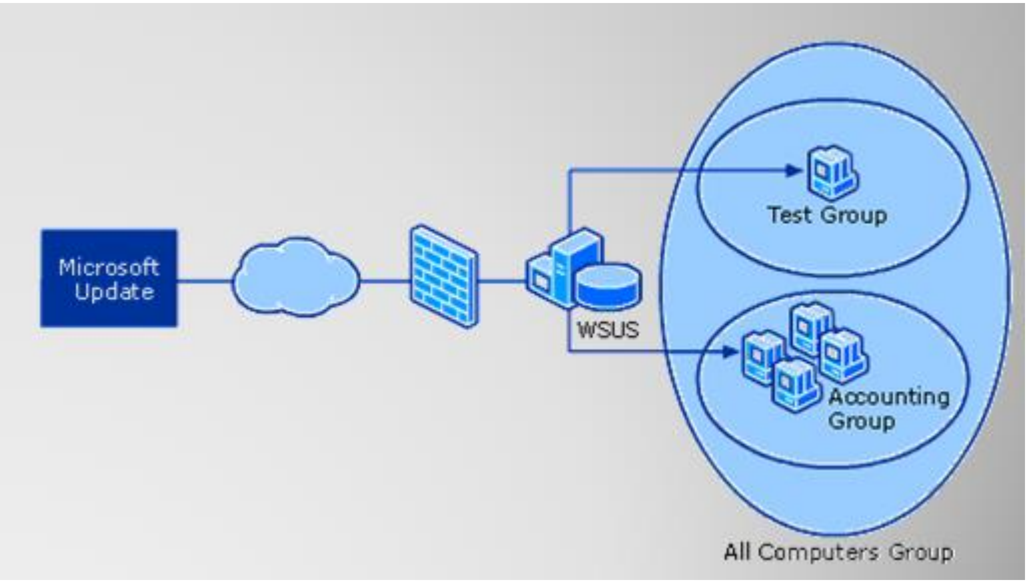
Classifications:

- □ All Classifications
  - ☑ Critical Updates
  - ☑ Definition Updates
  - □ Drivers
  - □ Feature Packs
  - ☑ Security Updates
  - □ Service Packs
  - □ Tools
  - □ Update Rollups
  - □ Updates

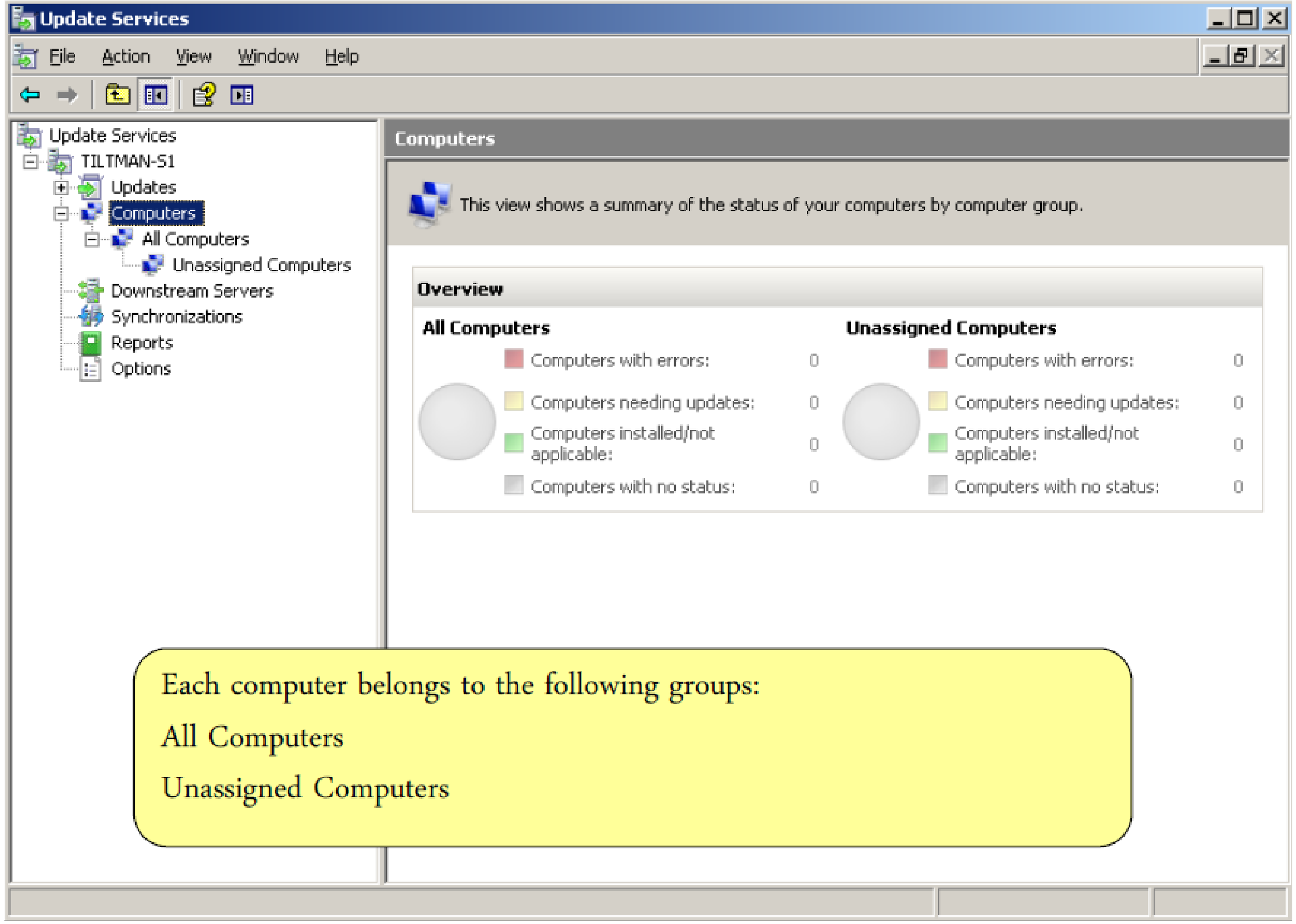
All classifications, including classifications that are added in the future.

Computer Groups

- Top level group is All Computers Group
- Test and Accounting Groups are nested within the All Computers Group
  - Target computers based on group membership



Default Computer Groups



This view shows a summary of the status of your computers by computer group.

Overview

All Computers		**Unassigned Computers**	
🟥 Computers with errors:	0	🟥 Computers with errors:	0
🟨 Computers needing updates:	0	🟨 Computers needing updates:	0
🟩 Computers installed/not applicable:	0	🟩 Computers installed/not applicable:	0
⬜ Computers with no status:	0	⬜ Computers with no status:	0

Each computer belongs to the following groups:

All Computers

Unassigned Computers

WSUS

- Automatic Approvals
  - You can specify how to automatically approve the installation of updates for selected groups
- Configuring a Client Group Policy Object
  - Start Group Policy Management Console
  - Load the WSUS Administrative Template
  - Direct client to WSUS server
  - Configure Automatic Updates behavior
  - Set contact frequency
- WSUS Reporting
  - Reports on the status of your environment

Windows Security Architecture

Security Principal

- In Windows a Subject is referred to as a Security Principal
- Security Principals include
  - Users
  - Groups
  - Computers
  - Processes
  - User Mode Applications
- A security principal is anything that can be assigned a security identifier (SID)

Securable Objects

- Windows has many Securable Objects (Objects)
- These include
  - Files & Directories
  - Registry Keys
  - File Shares
  - Active Directory Objects
  - Services
  - Processes & threads
- Securable Objects are things Security Principals will try to access

Windows Concepts

- Windows uses the terms rights, privileges and permissions (Access Controls)
- These terms are often used interchangeably and in the wrong context
  - Often in Window’s own documentation
- Rights, privileges and permissions control how security principals can access securable objects

Rights, Privileges, Permissions

- Both **Rights** and **Privileges** are applied to security principals
  - Logon Right controls how a security principal can log onto a system (local, network, etc.)
  - A Privilege is a user right that specifies actions a security principal can perform once they are on a system (shut down system, change system time, etc.)
- **Permissions** are assigned to securable objects and control what actions security principals can perform on them
  - NTFS permissions are applied to files and folders

Permissions

- Permissions allow or restrict a security principal’s access to a securable object
  - Included in ACL for the object and will vary based on the type of object
  - NTFS file system has permissions to access folders and files
  - Active Directory objects have additional permissions that can be set based on the specific resource

Privileges

- A privilege is the ability a Security Principal has to make changes to the system configuration
  - Change system time
  - Load device drivers
  - Force remote shutdown
- Complete list of Privileges in Administrative Tools – Local Security Policy – Local Policy – User Rights Assignment
  - WinXP has 38 rights & privileges
  - Windows 7 has 44 rights & privileges

User Mode & Kernel Mode

User Mode & Kernel Mode

- Windows operating system architecture separates the user from the kernel
  - Two modes: User Mode & Kernel Mode
- Each mode has a security responsibility as well as general duties
- User Mode processes pass user requests to the kernel, and through the kernel, to the hardware
- Kernel Mode processes interact directly with the system hardware and memory and contain several subsystems

User Mode Security

User Mode Security

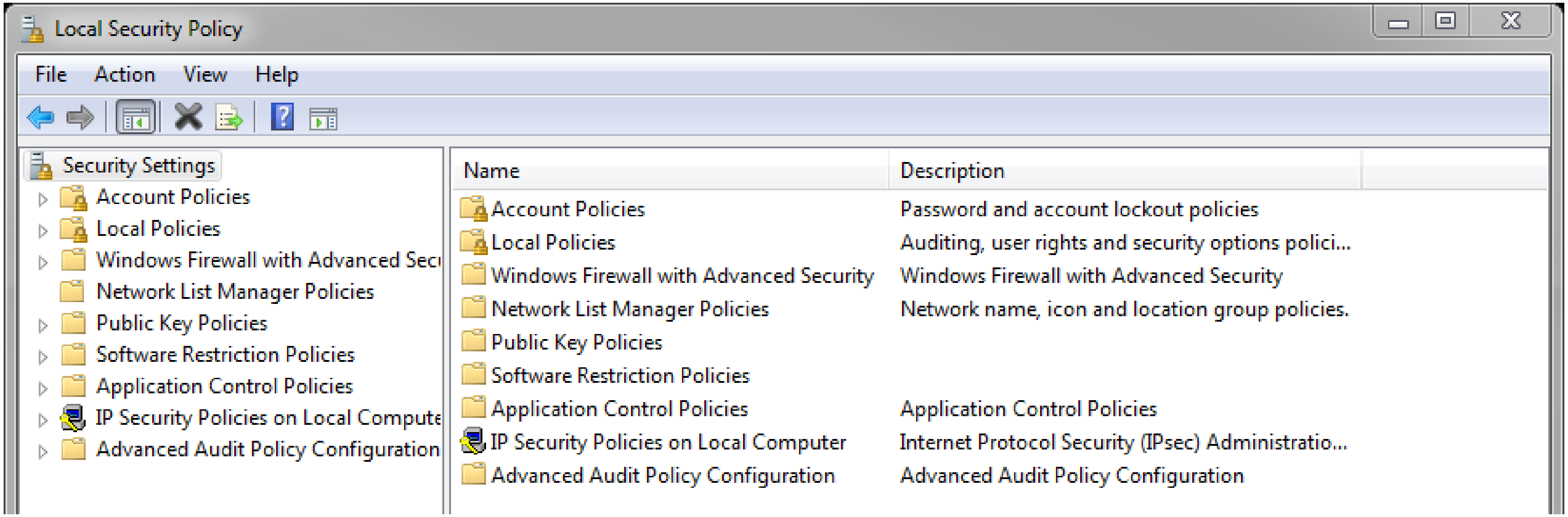
- User Mode layer contains a number of Integral Subsystems that manage OS functions for the user
  - Manage the opening and closing of process threads
  - Manage virtual memory usage
  - Manage input output devices
    - Drives, printers, serial & parallel ports
- User Mode Applications use Application Program Interfaces (APIs) and Dynamic Link Libraries (DLLs) to allow programs run by the user to access the Kernel resources

User Mode Security

- User Mode manages security functions through the Local Security Authority (LSA) subsystem
- The LSA is responsible for
  - Password Policy
  - Account Lockout Policy
  - Audit Policy
  - User Rights (and privileges) Assignment
  - Security Options

Local Security Authority

- The LSA configuration is managed through the Local Security Settings
- Control Panel – Administrative Tools – Local Security Policy

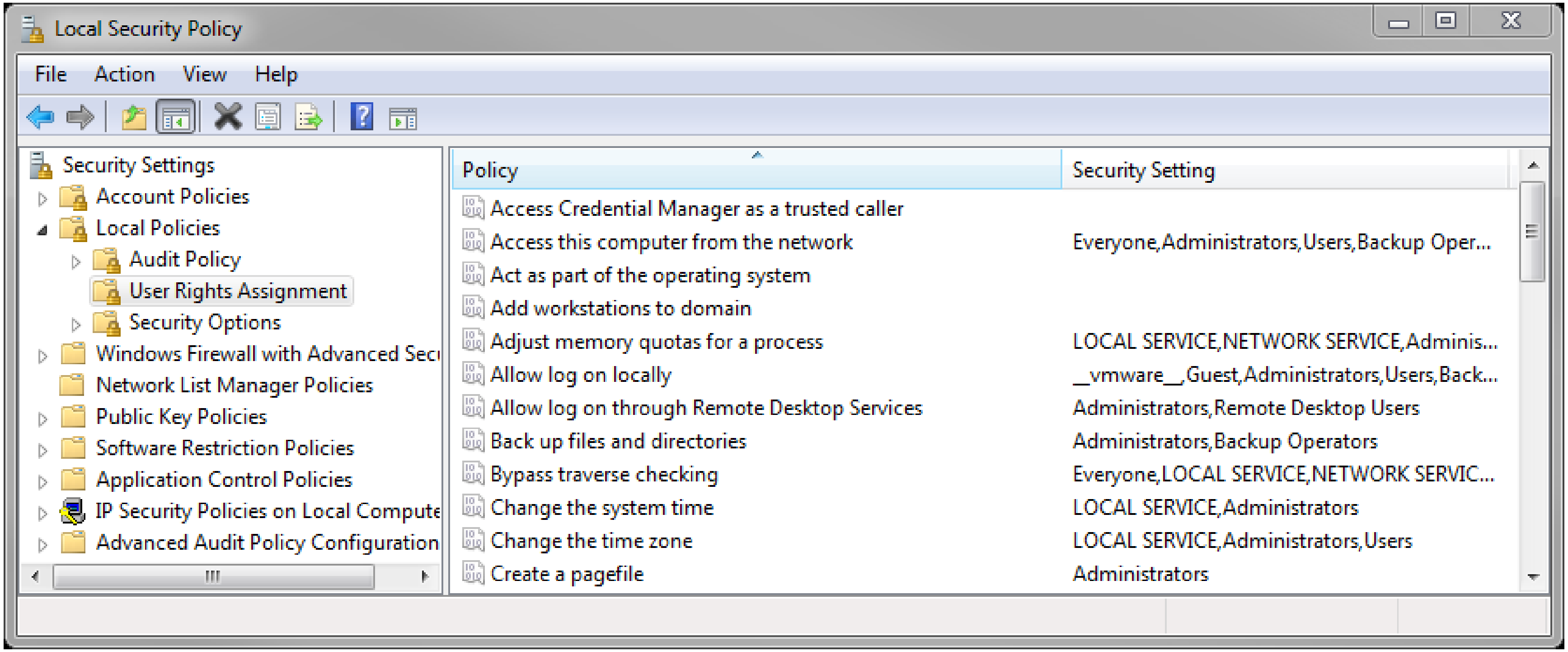


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici...
Windows Firewall with Advanced Security	Windows Firewall with Advanced Security
Network List Manager Policies	Network name, icon and location group policies.
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administratio...
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

Rights & Privileges

- User Rights Assignment (43 items in Win7)
  - Allow log on locally, change system time, etc.

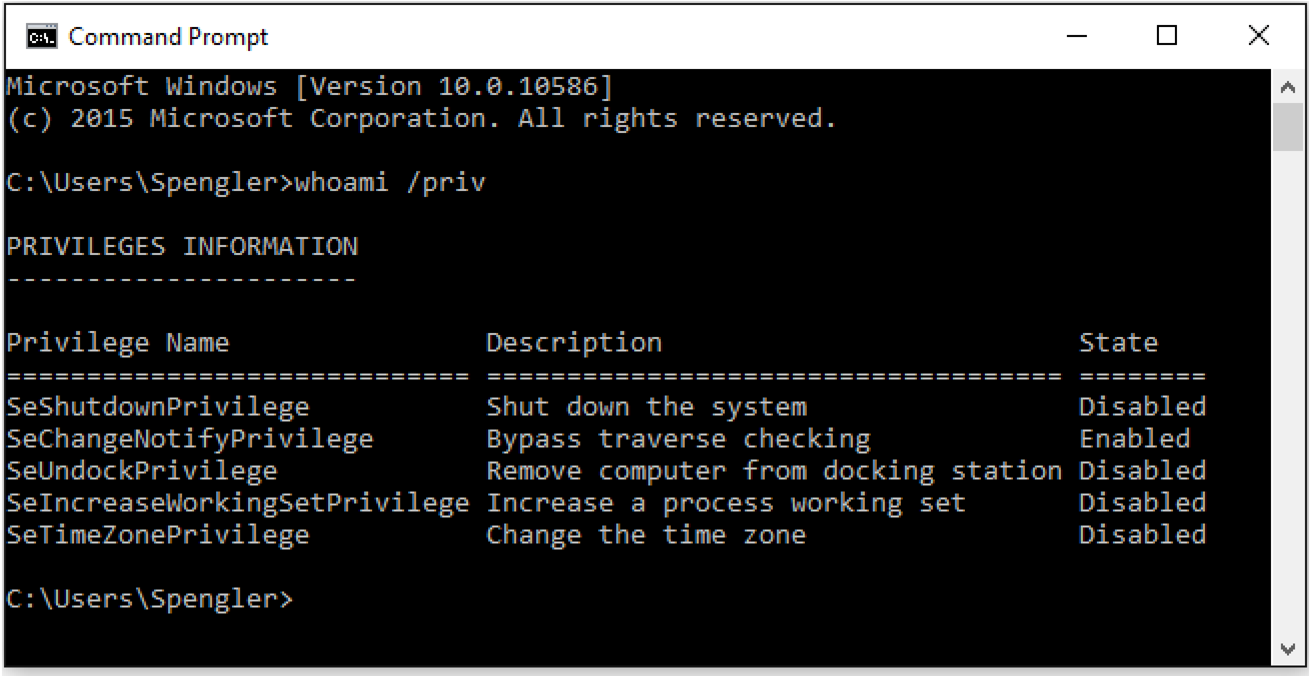


Security Settings
- Account Policies
- Local Policies
  - Audit Policy
  - User Rights Assignment
  - Security Options
- Windows Firewall with Advanced Secu
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Local Compute
- Advanced Audit Policy Configuration

Policy	Security Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	Everyone,Administrators,Users,Backup Oper...
Act as part of the operating system	
Add workstations to domain	
Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SERVICE,Adminis...
Allow log on locally	__vmware__,Guest,Administrators,Users,Back...
Allow log on through Remote Desktop Services	Administrators,Remote Desktop Users
Back up files and directories	Administrators,Backup Operators
Bypass traverse checking	Everyone,LOCAL SERVICE,NETWORK SERVIC...
Change the system time	LOCAL SERVICE,Administrators
Change the time zone	LOCAL SERVICE,Administrators,Users
Create a pagefile	Administrators

Windows Privileges

- The whoami command with the proper option can display the user privileges
  - Example from Windows 10:



```
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Spengler>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled

C:\Users\Spengler>
```

Windows Privileges

- Privileges need to be managed with care
- Change system time
  - Would affect backups and Kerberos tickets
- Act as part of operating system
  - Runs any code as the most trusted system account

Windows Login

- When logging on from the console the LSA takes the entered password for a user account and transforms the password into the cryptographic form stored in the Security Account Manager (SAM) database
- WinLogon Processes Used
  - MSGINA.dll – Graphical Identification and Authentication (XP)
  - Credential Providers – Vista and Above

Security Account Manager (SAM)

- The SAM is the database that stores the user account name and password credentials
  - SAM database is a binary file where the password hash is stored
  - File name SAM
  - C:\windows\system32\config\SAM
- Backup of SAM stored in
  - C:\windows\repair in XP
  - C:\Windows\System32\config\RegBack in Win7
- Tools such as pwdump are required to translate into human readable form

SAM

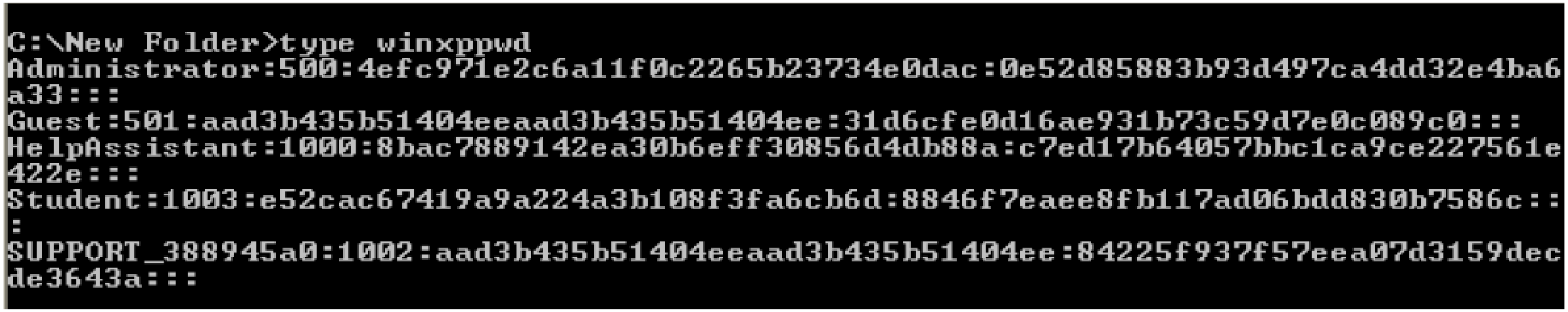
- The password for WinXP & Win2003 server could be stored as an LM hash, an NTLM hash or both
- For backward compatibility LM hashes can still be enabled in Windows Server 2008
- If the hash calculated by the LSA when the user logs in matches the hash stored in the SAM then the user is authenticated

SAM

- Security Account Manager (SAM)
  - Contains the account name, RID and hash
    - artmack:1011:FC525C9863E8FE067095BA2DDC971889
- The long string of numbers above is the NTLM MD4 hash of the password (128 bit) translated to Hexadecimal numbers for display

SAM

- Output of SAM from pwdump2 utility
- Shows account name, RID and hash values
    - The first group of 32 characters is the LM hash the 2nd group is the NTLM hash



```
C:\New Folder>type winxppwd
Administrator:500:4efc971e2c6a11f0c2265b23734e0dac:0e52d85883b93d497ca4dd32e4ba6
a33:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:8bac7889142ea30b6eff30856d4db88a:c7ed17b64057bbc1ca9ce227561e
422e:::
Student:1003:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c::
:
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:84225f937f57eea07d3159dec
de3643a:::
```

Hashing Algorithms

- A hash algorithm will take an input of any length and always produce an output character string of the same length
  - MD5 hash algorithm – 128 bit output
  - SHA1 hash algorithm – 160 bit output
  - SHA2-512 hash algorithm – 512 bit output
- Hash algorithms are considered a one way function
  - The original input can not be recalculated from the output

LM, NTLM & NTLMv2

- There have been three versions of LM
- Both LM and NTLM are basically broken and shouldn’t really be used
- NTLMv2 is used for local authentication on current systems
- When you get into an AD environment you will be using Kerberos

Kernel Mode Security

Kernel Mode Security

- The Kernel Mode layer contains the Kernel Executive subsystems
- These include
  - Object Manager
  - Memory manager
  - Process Manager
  - I/O Manager
  - Power Manager
- Security is handled by
  - Security Reference Monitor

Security Reference Monitor

- Security Reference Monitor
  - Responsible for access control for objects
  - Checks the permissions assigned to objects prior to granting users, groups or programs access
  - Audits and logs events associated with changes to objects

Windows ACLs

- Windows supports 2 forms of ACLs in addition to Role Based Access Control
  - Discretionary ACL, System ACL and Role Based AC
- Discretionary ACLs are under the control of the user or administrator
  - DACLs determine access to the object
- System ACLs are controlled by the operating system and cannot be changed by the user
  - Amongst other things, SACLs determine which access attempts get audited

Windows Security Descriptor

- Most Securable Objects are assigned a Security Descriptor
- The Security Descriptor (SD) for an object contains the owner name (SID), group name (SID) SACL and DACL
- The SACL and DACL will contain lists of individual Access Control Entries (ACE)

Access Control Entries

- Access Control Entries contain
  - SID of the user to be denied or allowed access
  - Access Mask which contains the permissions
    - Read, write, create, delete, modify, etc.
- Access Mask are object type specific
  - File and directories have masks for NTFS permissions
  - Masks for registry objects and services have different permissions

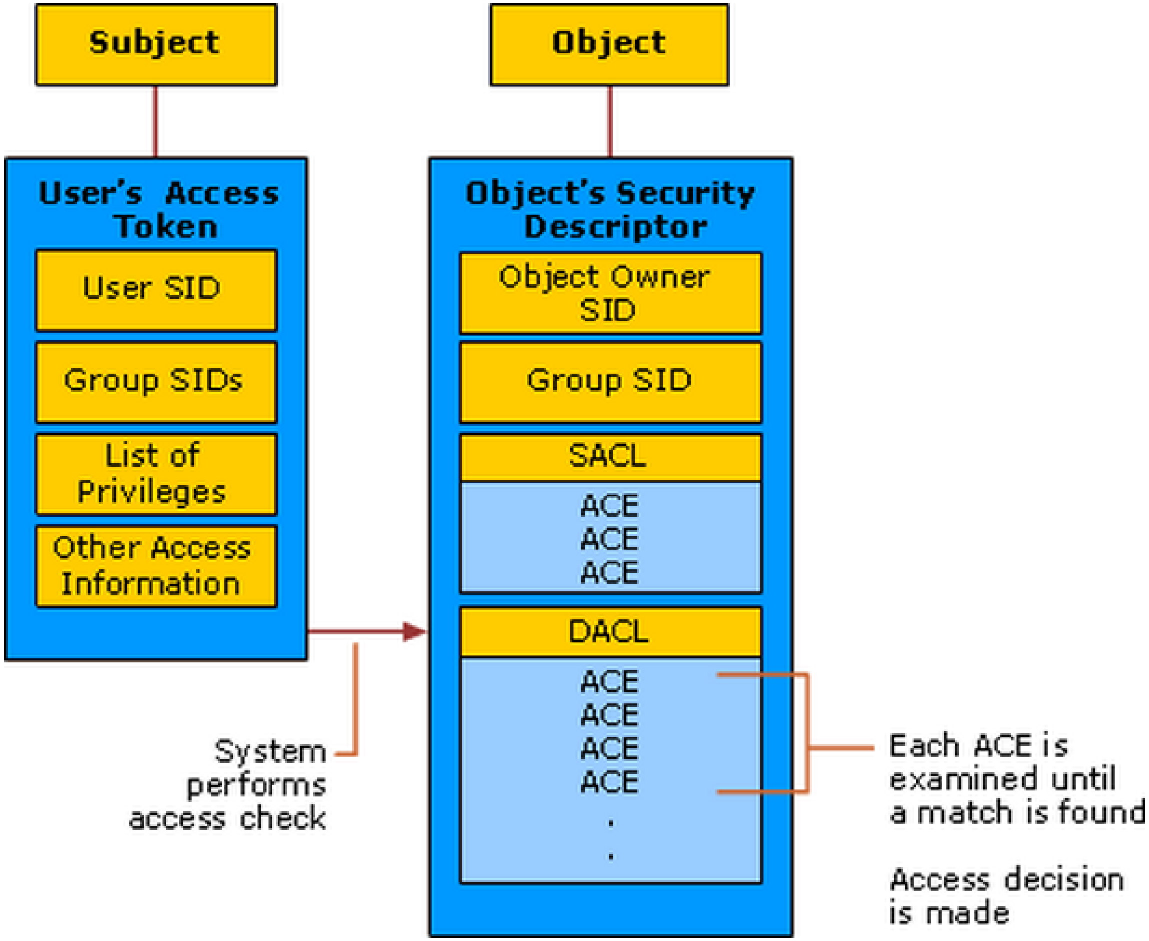
Access Control Entries

- Access Control Entry order is important
- An ACE created by the GUI will always place a Deny ACE at top of list before the Allow ACEs
  - Deny ACE will be processed first if it is at top of list
- System will stop processing when the first match is made

Security Tokens

- When a user logs on to a system a Security Token is created for that user
- The Security Token contains
  - User SID
  - All Group memberships
    - SID of all groups User is a member of
  - List of assigned privileges
- The Security Token is always checked against the ACLs on an object when access by the user is requested
  - Checked against the Security Descriptor

Subjects & Objects



Windows DACLs

- Windows systems implement discretionary access controls to system resources such as files, shared memory, and named pipes
- The access control list has a number of entries that may grant or deny access rights to a specific SID, which may be for an individual user or for some group of users

Windows DACLs

- Windows Vista and later systems also include mandatory integrity controls
- These label all objects, such as processes and files, and all users, as being of low, medium, high, or system integrity level
- Then whenever data is written to an object, the system first ensures that the subject’s integrity is equal or higher than the object’s level

Windows DACLs

- Access Control is checked by comparing SIDs in the Security Token to SIDs in the individual ACEs in the following order
- If the SID privilege is DENY, access is not granted
- Next, look for match to an Allow ACE
- If no match is found the access is denied

Creator / Owner

- In past versions of Windows the Object creator/owner always had full control of the object created
  - Had ability to change the DACL for an object
- Since Vista & Win2008 server there is a new access control OWNER/RIGHTS
  - Allows administrators to remove the owners ability to change permissions on an object

SID Management

- Users and groups in Windows systems are defined with a Security ID (SID)
- This information may be stored and used locally, on a single system, in the Security Account Manager (SAM)
- It may also be centrally managed for a group of systems belonging to a domain, with the information supplied by a central Active Directory (AD) system using the LDAP protocol

SIDs & RIDs

- Each user is assigned a Security Identifier (SID)
  - Long complex number that includes information on the version of the operating system, computer and the user
  - S-1-5-21-57989841-1336601894-682003330-500
- RID
  - Relative Identifier is assigned to a user

Security Identifier

S-1-5-21-57989841-1336601894-682003330-500

- S simply means SID
- 1 is SID version number
  - Currently version 1
- 5 denotes the identifier authority value
  - Currently NT AUTHORITY
- 21 means not unique
  - But always unique within a domain

Security Identifier

S-1-5-21-57989841-1336601894-682003330-500

- 57989841-1336601894-682003330
  - Unique number to identify this computer and domain
- 500 RID which, in this case, identifies the user as the system administrator

- wmic useraccount get name,sid

Security Identifier

- Well Known RIDs
  - 500 - Administrator
  - 501 - Guest
  - 1000 & up for users created
- When a user is created it is assigned a SID
- If the user is deleted and created again with the same name it will have a different SID
  - This is because RID values are never repeated and the 2nd creation with the same name will get a different RID
  - Windows uses the SID to identify the user account the name is just a label
- The same user name on 2 different computers will produce 2 different SIDs

Security Identifier

- Well known SIDs for built-in users and groups are standardized and are shorter
- S-1-1-0
  - SID for Everyone group
- S-1-5-2
  - SID for Network Logon
- S-1-5-4
  - SID for Local or Remote Desktop logon
- S-1-5-13
  - SID for Terminal Services logon

Security Identifier

- More well known SIDs for built-in users and groups
- S-1-5-7
  - SID for Anonymous logon
- S-1-5-11
  - SID for Authenticated User group
- S-1-5-32
  - SID for built-in user & groups
- S-1-5-32-544
  - The built-in Administrators group

Security Identifier

- Reminder: If a user is deleted and then created again with the same name, password and permissions it will receive a new RID
  - A user RID is never reused
- For more details on SID follow the links below to Microsoft and Wikipedia web sites
  - http://support.microsoft.com/kb/243330
  - http://en.wikipedia.org/wiki/Security_Identifier

Windows Security

Patch management

- “Windows Update” and “Windows Server Update Service” assist with regular maintenance and should be used
- Third party applications also provide automatic update support

Users administration and access controls

- Systems implement discretionary access controls resources
- Vista and later systems include mandatory integrity controls
- Objects are labeled as being of low, medium, high, or system integrity level
- System ensures the subject’s integrity is equal or higher than the object’s level

Windows Default Accounts

- 2 default user accounts are created on installation
  - Administrator & Guest
- Since Windows Vista, the Guest and Administrator accounts are disabled by default
- The 2 accounts are stored in local SAM

Default Groups

- A user will be assigned to a number of groups automatically
- These group SIDs will be listed in the Security Token
  - Administrators group
  - Users group
  - Everyone group
  - Authenticated User

Groups

- On the local computer there are 2 types of groups
  - Built-in & Local
  - The Administrators & Users Groups are examples of built-in groups
  - Local groups are created on the local computer by the administrator
- Active Directory defines many types of groups
  - Win 2008 server has 26 abstract concept groups

Groups

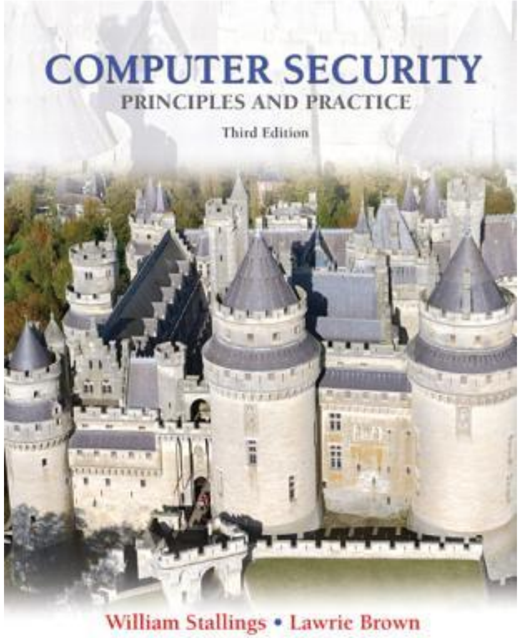
- Everyone Group
  - Automatically includes almost all users accessing the computer including the Guest user
    - Does not include the anonymous user
- Authenticated Users
  - Automatically includes all users accessing the computer with a password
    - Does not include the guest user
    - Does not include the anonymous user

Groups

- There are also groups that indicate how a user logged on to the computer
- Interactive group
  - Contains users that logon to the local system
- Network group
  - All users that logged on across the network

Homework

- Read Chapter 12
- Sections
  - 12.4 – Application Security
  - 12.5 – Security Maintenance
  - 12.7 – Windows Security
- Chapter 4
- Chapter 3
  - 3.1, 3.2



Lab 03 – Domain Prep WSUS GPO

Lab 03 Details

- Server 2008 R2 setup
- Promote to Domain Controller
- Join W7 client to domain
- Create WSUS Group Policy Object
- Create GPO Report