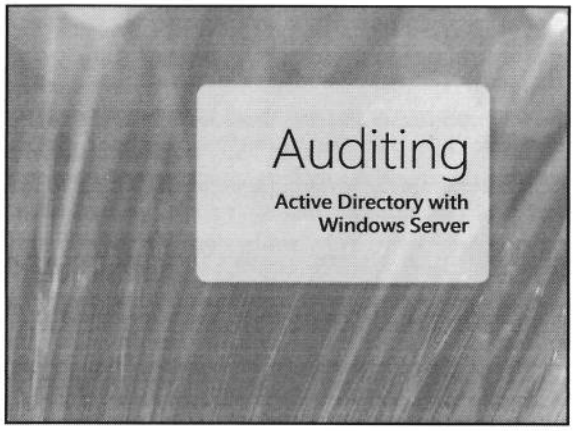
96531BB92F



Instructor Introduction

Jay Ferron

CEHi, CISSP, CHFIi, C)PTEi, CRISC, CVEi, MCITP, MCSE, MCT, MVP, NSA-IAM...

jferron@interactivesecuritytraining.com

blog.mir.net

203-675-8900 Phone

Module Overview

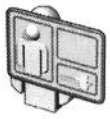
- Overview of Active Directory, Identity, and Access
- Active Directory Components and Concepts
- Install Active Directory Domain Services

powergui
lepide
netwrix
2600 magazine
pg. II.6
whitepaper premium
telport pro
Nessus
OpenVAS
Core Impact ($30K)
PSR
Windows
Robocopy
ZenMap
scan
ipssPX
not tcp/ip
Windows to Direct Access
cheap VPN

Lesson 1: Overview of Active Directory, Identity, and Access

- Information Protection
- Identity and Access
- Authentication and Authorization
- Authentication
- Access Tokens
- Security Descriptors, ACLs, and ACEs
- Authorization
- Stand-Alone (Workgroup) Authentication
- Active Directory Domains: Trusted Identity Store
- Active Directory, Identity, and Access
- Active Directory IDA services

Information Protection



- It's all about connecting users to the information they require securely
- IDA: Identity and Access
- AAA: Authentication, Authorization, Accounting
- CIA: Confidentiality, Integrity, Availability, and Authenticity

Identity and Access

- Identity: User account
- Saved in an identity store (directory database)
- Security principal
- Represented uniquely by the SID

- Resource: Shared Folder
- Secured with a security descriptor
- DACL or "ACL"
- ACEs or "permissions"

Security Identity Module
SAM file = Security Account Manager
SID
Audit group not user

DACL Discretionary ACL = ACL + ACE
ACL Access Control List
ACE Access Control Entries
(SACL System Access Control List)

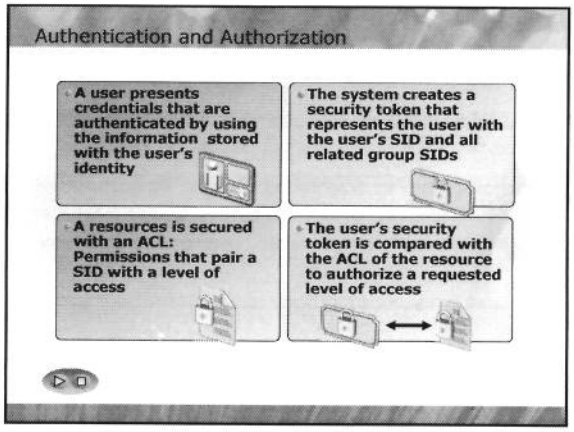
noPAP → CHAP

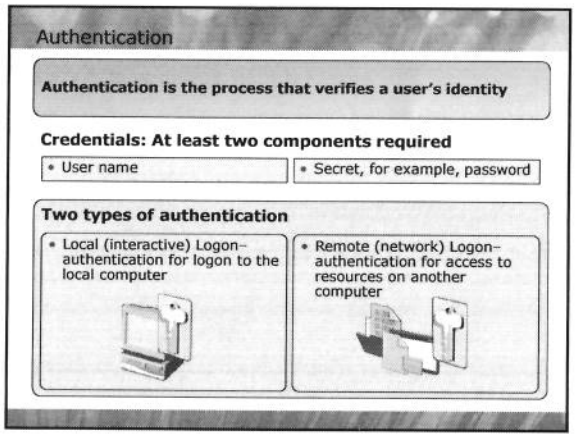
(LM hash)

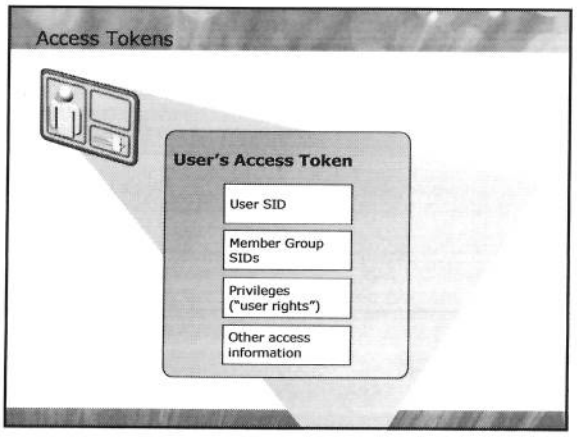
IBM lan Manager hash (must be 2)

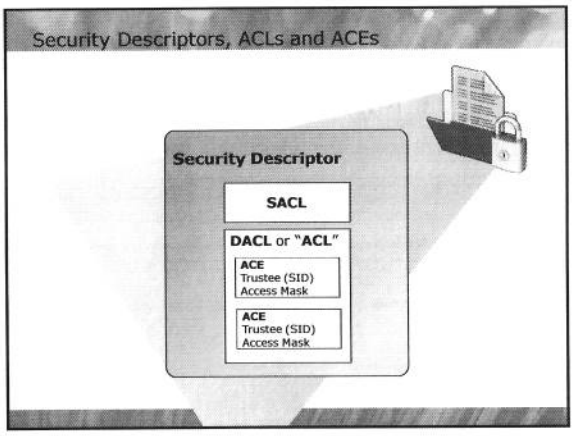
kerberos = ticket level 2

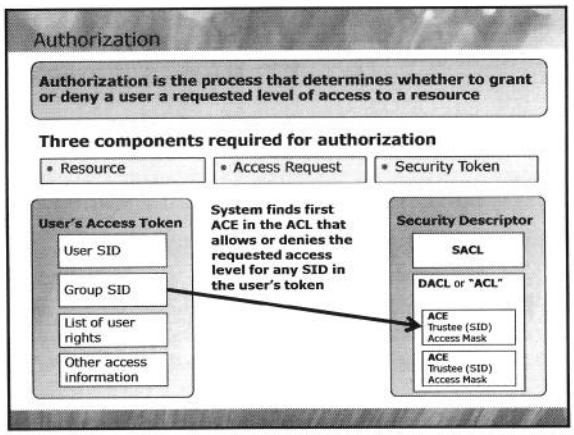
EAP (RSA) level 3

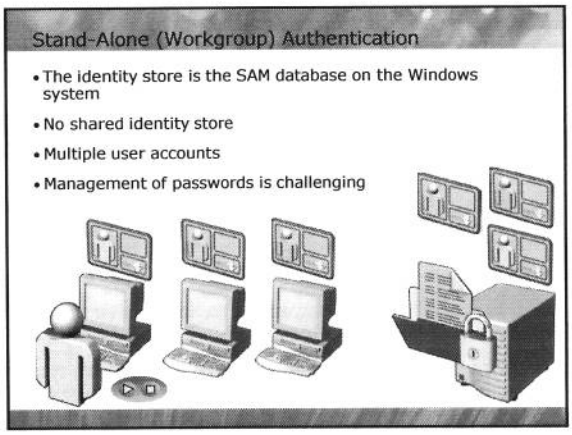







Security Descriptors, ACLs and ACEs
Security Descriptor
SACL
DACL or "ACL"
ACE
Trustee (SID)
Access Mask
ACE
Trustee (SID)
Access Mask


Authorization
Authorization is the process that determines whether to grant or deny a user a requested level of access to a resource
Three components required for authorization
• Resource
• Access Request
• Security Token
User's Access Token
User SID
Group SID
List of user rights
Other access information
System finds first ACE in the ACL that allows or denies the requested access level for any SID in the user's token
Security Descriptor
SACL
DACL or "ACL"
ACE
Trustee (SID)
Access Mask
ACE
Trustee (SID)
Access Mask


Stand-Alone (Workgroup) Authentication
• The identity store is the SAM database on the Windows system
• No shared identity store
• Multiple user accounts
• Management of passwords is challenging

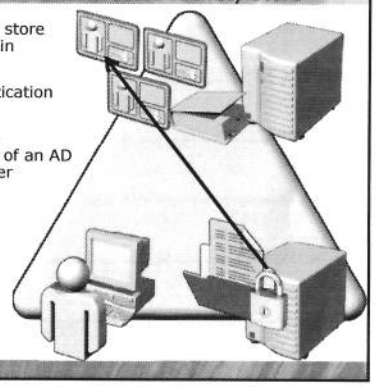
Azure Active Directory

AD database = Scheme

service not in a file

Active Directory Domains: Trusted Identity Store

- Centralized identity store trusted by all domain members
- Centralized authentication service
- Hosted by a server performing the role of an AD DS domain controller



Min. 2 domain controllers

5 Roles inside DC

a) Scheme master role (Box 1)

b) I/E master role (names)

c) RID Master role (gen. unique ID)

d) PDC emulator ← for repl. rules

e) Domain Naming master

FSRM = File System Resource Manager
→ find all files with SID=0 and move to folder X

~~powershell always on~~
↑ Empire

powershell controls? (for security)

Active Directory, Identity, and Access

An IDA infrastructure should:

- Store information about users, groups, computers and other identities
- Authenticate an identity
  - Kerberos authentication used in Active Directory provides single sign-on. Users are authenticated only once.
- Control access
- Provide an audit trail

IDA = Identity & Access

Active Directory IDA Services

Active Directory IDA services :

- Active Directory Lightweight Directory Services (AD LDS)
- Active Directory Certificate Services (AD CS)
- Active Directory Rights Management Services (AD RMS)
- Active Directory Federation Services (AD FS)

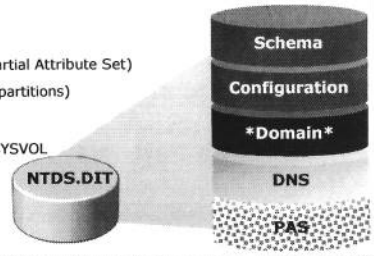
Active Directory as a Database

- Active Directory is a database
  - Each "record" is an object
    - Users, groups, computers, and so on
  - Each "field" is an attribute
    - Logon name, SID, password, description, membership, and so on
  - Identities (security principals or "accounts")
- Services: Kerberos, DNS, and replication
- Accessing the database
  - Windows tools, user interfaces, and components
  - APIs (.NET, VBScript, Windows PowerShell)
  - LDAP

All DC must be within 15 mins of each other
Must have central time! <GP force>

Active Directory Data Store

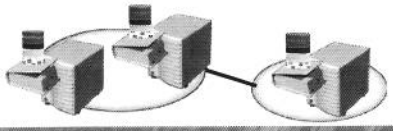
- %systemroot%\NTDS\ntds.dit
- Logical partitions
  - Domain naming context
  - Schema
  - Configuration
  - Global catalog (Partial Attribute Set)
  - DNS (application partitions)
- SYSVOL
  - %systemroot%\SYSVOL
  - Logon scripts
  - Policies



Remote Server Admin tool (RSAT)
RODC = Read Only Domain Controller

Domain Controllers

- Servers that perform the AD DS role
  - Host the Active Directory database (NTDS.DIT) and SYSVOL
    - Replicated between domain controllers
  - Kerberos KDC service: Performs authentication
  - Other Active Directory services
- Best practices
  - Availability: At least two in a domain
  - Security: Server Core and RODCs



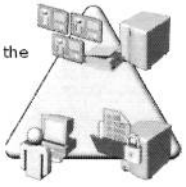
Organizational Units

- Objects
  - Users
  - Computers
- Organizational Units
  - Containers that can be used to group objects within a domain
  - Create OUs to:
    - Delegate administrative permissions
    - Apply Group Policy

{Security Boundary
{Replication Boundary

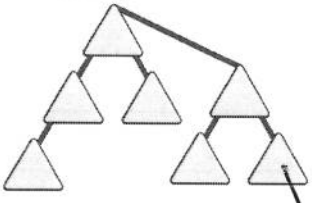
Domain

- Requires one or more domain controllers
- All domain controllers replicate the Domain naming context (Domain NC)
  - The domain is the context within which Users, Groups, Computers, and so on are created
  - "Replication boundary"
- Trusted identity source: Any domain controller can authenticate any logon in the domain
- The domain is the *maximum* scope (boundary) for certain administrative policies
  - Password
  - Lockout



Forest

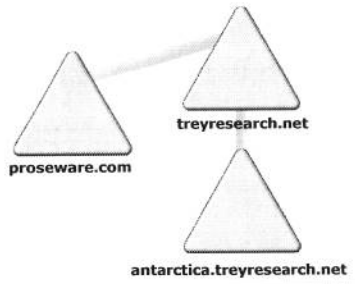
- A collection of one or more Active Directory domain trees
- First domain is the *forest root domain*
- Single configuration and schema replicated to all domain controllers in the forest
- A security and replication boundary



is trusted but dont have permission

Tree

- One or more domains in a single instance of AD DS that share *contiguous DNS namespace*

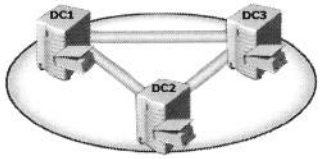


service in DC

Knowledge Consistency Checker (KCC)
~~Bridge head server~~

Replication

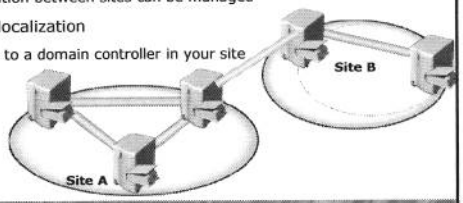
- Multimaster replication
  - Objects and attributes in the database
  - Contents of SYSVOL are replicated
- Several components work to create an efficient and robust replication topology and to replicate granular changes to AD
- The Configuration partition of the database stores information about sites, network topology, and replication



Audit replication log?
Audit KCC

Sites

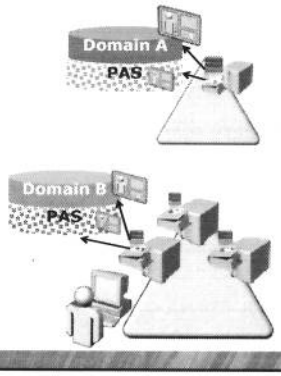
- An Active Directory object that represents a well-connected portion of your network
  - Associated with subnet objects representing IP subnets
- Intrasite vs. intersite replication
  - Replication within a site occurs very quickly (15–45 seconds)
  - Replication between sites can be managed
- Service localization
  - Log on to a domain controller in your site



subset of scheme (excl. fields not used)

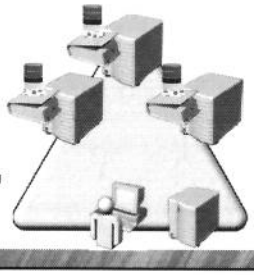
Global Catalog

- Partial Attribute Set or Global Catalog
- Contains every object in every domain in the forest
- Contains only selected attributes
- A type of index
- Can be searched from any domain
- Very important for many applications



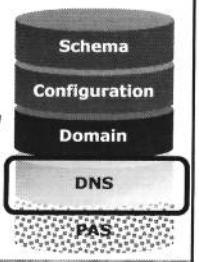
Functional Levels

- Domain functional levels
- Forest functional levels
- New functionality requires that domain controllers are running a particular version of Windows
  - Windows 2000
  - Windows Server 2003
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 r2
  - Windows Server 2016
- Cannot raise functional level while domain controllers are running previous Windows versions
- Cannot add domain controllers running previous Windows versions after raising functional level



DNS and Application Partitions

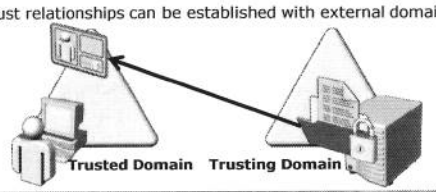
- Active Directory and DNS are closely integrated
- One-to-one relationship between the DNS domain name and the logical domain unit of Active Directory
- Complete reliance on DNS to locate computers and services in the domain
- A domain controller acting as a DNS server can store the zone data in Active Directory itself—in an *application partition*



* Trust is between companies

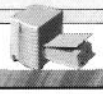
Trust Relationships

- Extends concept of trusted identity store to another domain
- Trusting domain (with the resource) trusts the identity store and authentication services of the trusted domain
- A trusted user can authenticate to, and be given access to resources in, the trusting domain
- Within a forest, each domain trusts all other domains
- Trust relationships can be established with external domains



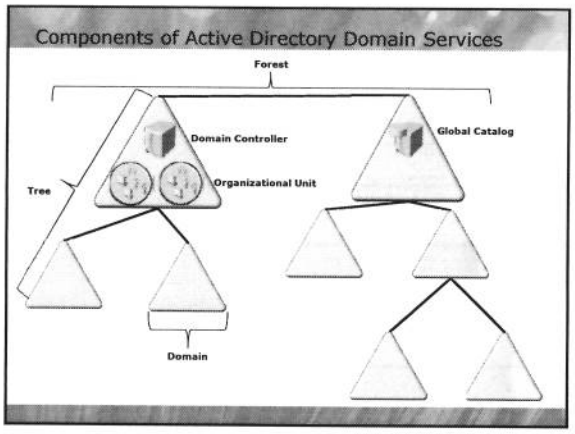
Install and Configure a Domain Controller

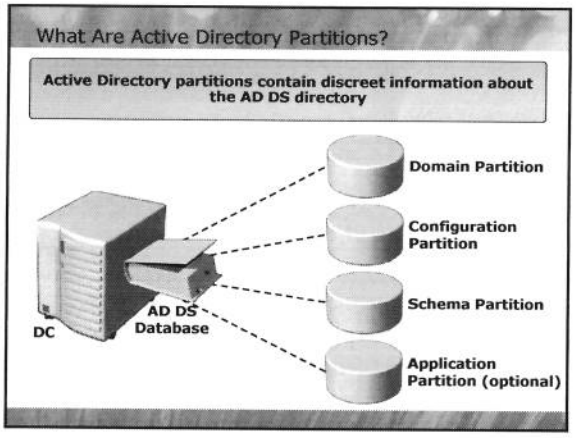
1. **Install the Active Directory Domain Services role by using the Server Manager**
2. **Run the Active Directory Domain Services Installation Wizard**
3. **Choose the deployment configuration**
4. **Select the additional domain controller features**
5. **Select the location for the database, log files, and SYSVOL folder**
6. **Configure the Directory Services Restore Mode Administrator Password**

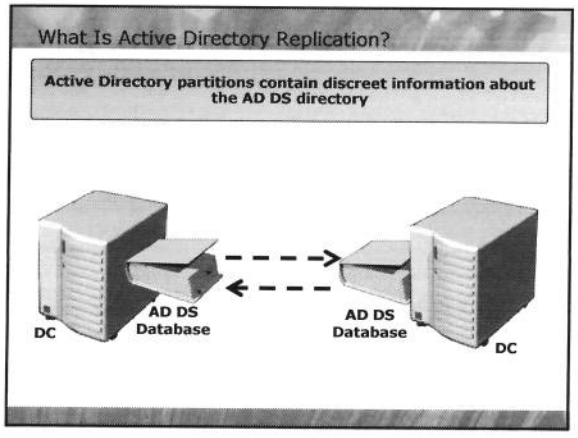


Prepare to Create a New Forest with Windows Server 2012 R2

- Domain's DNS name (contoso.com)
- Domain's NetBIOS name (contoso)
- Whether the new forest will need to support domain controllers running previous versions of Windows (affects choice of functional level)
- Details about how DNS will be implemented to support AD DS
  - Default: Creating domain controller adds DNS Server role as well
- IP configuration for the domain controller
  - IPv4 and, optionally, IPv6
- User name and password of an account in the server's Administrators group. Account must have a password.
- Location for data store (ntds.dit) and SYSVOL
  - Default: %systemroot% (c:\windows)

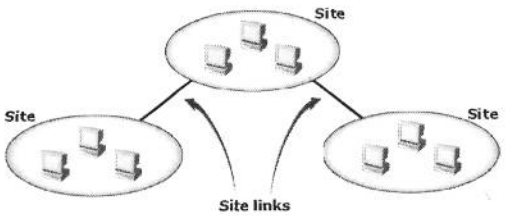

Components of Active Directory Domain Services
Forest
Domain Controller
Global Catalog
Organizational Unit
Tree
Domain


What Are Active Directory Partitions?
Active Directory partitions contain discreet information about the AD DS directory
Domain Partition
Configuration Partition
Schema Partition
Application Partition (optional)
DC
AD DS Database


What Is Active Directory Replication?
Active Directory partitions contain discreet information about the AD DS directory
DC
AD DS Database
AD DS Database
DC

What Are Active Directory Sites?

Active Directory sites are objects stored in the directory representing network topology



Domain and Forest Functional Levels

Domain and forest functional levels define the level of Active Directory functionality supplied by all domain controllers within a domain or forest

Domain Functional Levels:

- Windows 2000 native
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

Forest Functional Levels:

- Windows 2000
- Windows 2003
- Windows 2008
- Windows 2008 R2

In order to use Windows Server 2008 as a domain controller, the domain must be set to a functional level of Windows 2000 native or higher

Operations Master Roles

Operations Master Roles are assigned to a server that is responsible for performing that role's task

Forest-Wide Operation Master Roles:

- Domain Naming Master Role
- Schema Master Role

Domain-Wide Operations Master Roles

- RID Master Role
- Infrastructure Master Role
- PDC Emulator Role

only 1 in forest

Need special permission

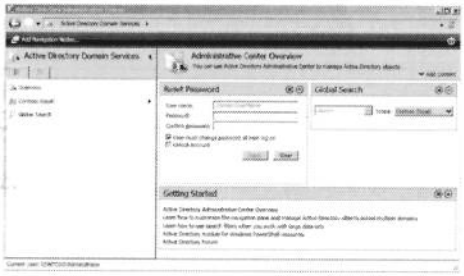
Overview of the Active Directory Administration Snap-ins

Active Directory Administration snap-ins consist of four different Microsoft Management Console snap-ins

- **Active Directory Users and Computers**
- **Active Directory Sites and Services**
- **Active Directory Domains and Trusts**
- **Active Directory Schema**

Active Directory Administrative Center

Active Directory Administrative Center is a task-oriented tool based upon Windows PowerShell



local admin (500)
guest account (501)

What Is a User Account?

A user account is an object that enables authentication and access to local and network resources

A user account can be stored:

- **In AD DS (AD DS account)**
  - **AD DS accounts enable log on to domains and provide access to shared network resources**
- **On the local computer (local account)**
  - **Local accounts enable log on to a single computer and local resources**

Creating a user account also creates a SID

Passware kit Forensic

Password Recovery

Do not enable

User Account Password Options

User account password options help to mitigate the threat of unauthorized account access

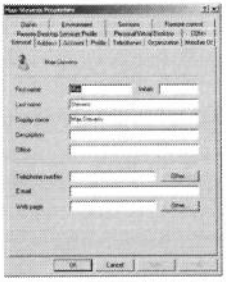
Policies	Default Settings
Password	Controls complexity and lifetime of passwords • Complex Password: enabled • Enforce password history: 24 • Maximum password age: 42 days • Minimum password age: 1 day • Minimum password length: 7 characters • Store password using reversible encryption: disabled
Account Lockout	Controls how many incorrect attempts can be made • Lockout threshold: 0 invalid logon attempts • Lockout duration: not defined • Reset account lockout after: not defined

User Account Attributes

User account attributes control how the user account interacts with the environment

Commonly used User Account sections:

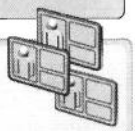
- **General**
- **Account**
- **Profile**
- **Organization**
- **Member Of**
- **Dial-in**



Active Directory Template

What Is a User Account Template?

A user account template is an account with common properties already configured



User accounts templates take advantage of similarity between user accounts

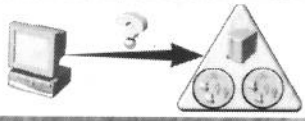
To use user templates:

- **Create several typical users reflecting various groups within your organization**
- **Copy the user account most like the new account you want to create**
- **Modify the attributes: names, e-mail address, logon name, etc.**

Considerations for Joining a Computer to a Domain

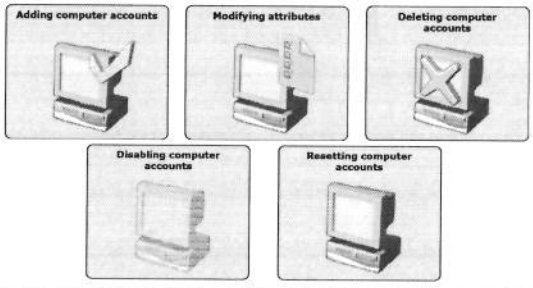
The following points need to be considered when joining a computer to a domain:

- A computer object must be created in the directory service and placed in a container or organizational unit
- You must have appropriate permissions in the domain to create computer objects in AD DS
- Only members of the local Administrators group can change a computer's domain or workgroup membership

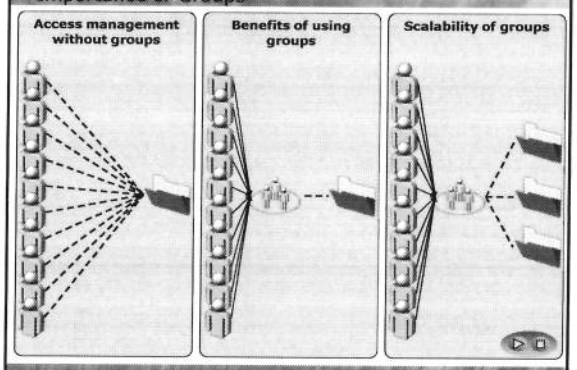


Managing Computer Accounts

Managing computer accounts requires several management tasks



Importance of Groups

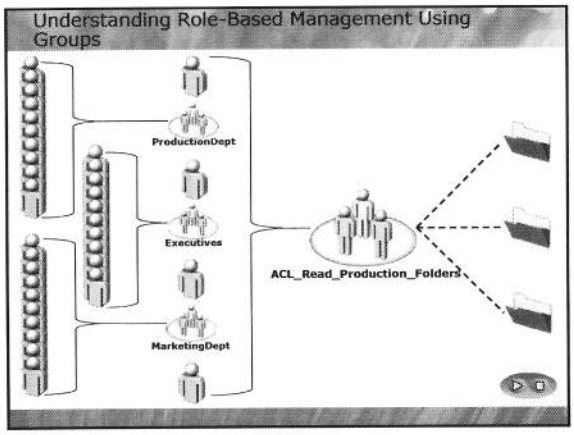


Nested group - domain / permission

U - G - G - DL - P

U - G - G - U - DL - P

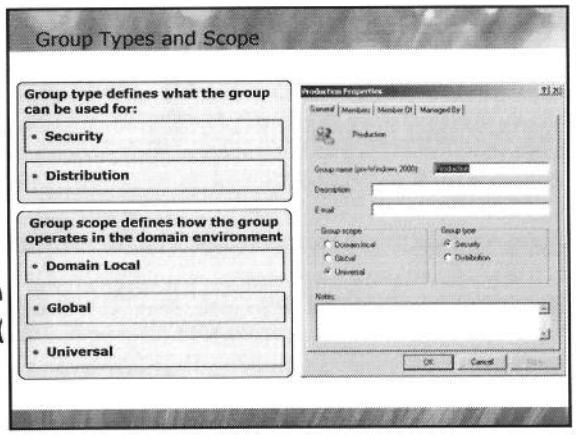
Universal group

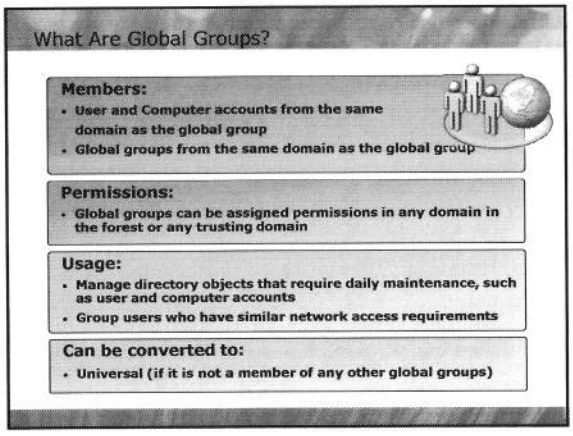


group membership on Global Catalog
SID in the group does not
change even if group name
change
Active Directory resulting set
shows conflicts.

Group types

Group scope





What Are Universal Groups?

Members:
- Global groups from any domain in the forest
- User and Computer accounts from any domain in the forest
- Universal groups from any domain in the forest

Permissions:
- Can be assigned permissions in any domain in the forest or any trusting domain

Usage:
- Use to combine groups that span domains

Can be converted to:
- Domain local
- Global (if no other universal groups exist as members)

What Are Domain Local Groups?

Members:
- Accounts from any domain in the forest or any trusted domain
- Global groups from any domain in the forest or any trusted domain
- Universal groups from any domain in the forest or any trusted domain
- Domain local groups, but only from the same domain as the domain local group

Usage:
- Use to define and manage access to resources in a single domain

Permissions:
- Member permissions can be assigned only within the same domain as the domain local group

Can be converted to:
- Universal (if no other domain local groups exist as members)

What Is Group Nesting?

Nesting allows for groups to be members of other groups

Benefits of using a nesting strategy in managing AD DS groups:
- Groups that are members of other groups reduce replication
- Nested groups provide for simplified management

When nesting, apply the AGDLP or AGUDLP principle

Universal

Options for Locating Objects in AD DS

- **Sorting:** use column headings in Active Directory Users and Computers to find the objects based on the columns
- **Searching:** provide the criteria for which you want to search
- **Command-line:** dsquery *parameter*

Windows Server 2008 R2 - 2016 options:

- **Active Directory module for Windows PowerShell**
- **Active Directory Administrative Center**

What Is Configuration Management?

Configuration management is a centralized approach to applying one or more changes to one or more users, computers or both

The key elements of configuration management are:

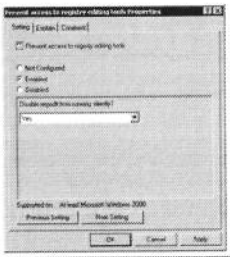
- **Setting: Definition of a change or configuration**
- **Scope: Definition of the users or computers to which the change applies**
- **Application: A mechanism that applies the setting to users and computers within the scope**

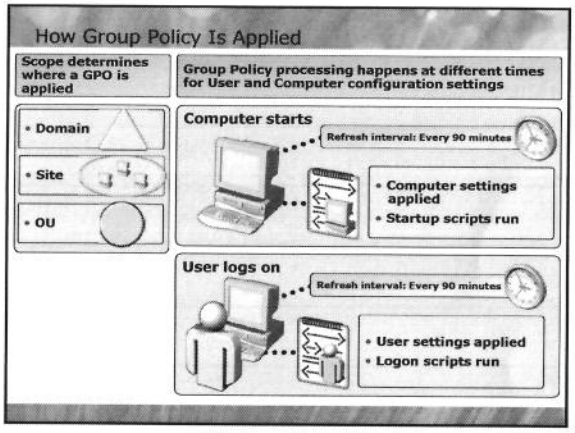
Group Policy provides the framework for configuration management in the Windows environment

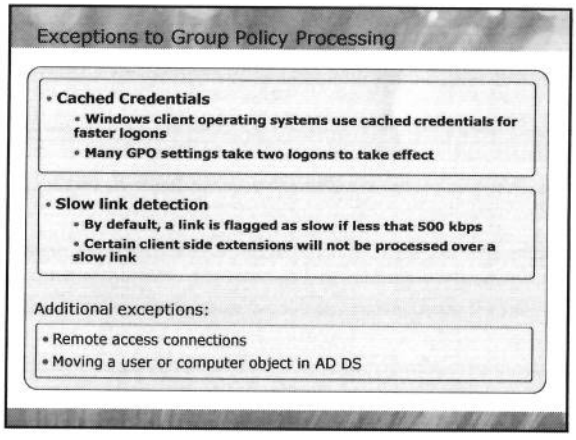
What Are Group Policy Objects and Settings?

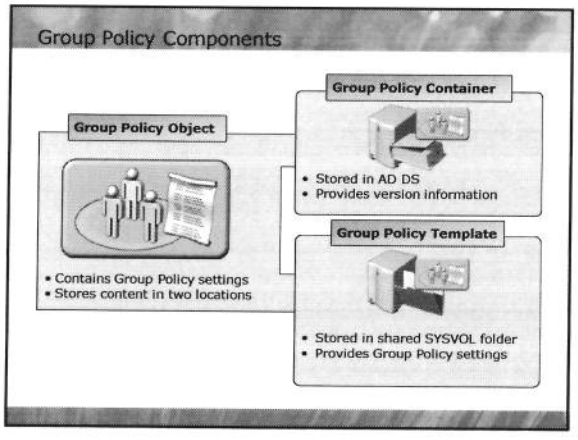
A Group Policy setting defines a specific configuration change to apply to a user, computer or both

A Group Policy Object is a collection of Group Policy settings that can be applied to a user, computer or both to enact changes

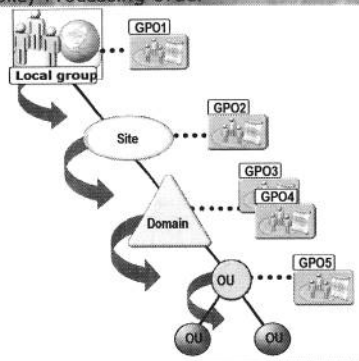



How Group Policy Is Applied
Scope determines where a GPO is applied
Group Policy processing happens at different times for User and Computer configuration settings
• Domain
• Site
• OU
Computer starts
Refresh interval: Every 90 minutes
• Computer settings applied
• Startup scripts run
User logs on
Refresh interval: Every 90 minutes
• User settings applied
• Logon scripts run


Exceptions to Group Policy Processing
• Cached Credentials
• Windows client operating systems use cached credentials for faster logons
• Many GPO settings take two logons to take effect
• Slow link detection
• By default, a link is flagged as slow if less that 500 kbps
• Certain client side extensions will not be processed over a slow link
Additional exceptions:
• Remote access connections
• Moving a user or computer object in AD DS


Group Policy Components
Group Policy Object
• Contains Group Policy settings
• Stores content in two locations
Group Policy Container
• Stored in AD DS
• Provides version information
Group Policy Template
• Stored in shared SYSVOL folder
• Provides Group Policy settings

Group Policy Processing Order



Options for Modifying Group Policy Processing

Six methods to modify GPO default processing:

1. Block inheritance
2. Enforcement
3. Filtering using security groups
4. Filtering using WMI filters
5. Disabling GPOs
6. Loopback processing

Options for Delegating Control of GPOs

Delegation of GPO-related tasks allows the administrative workload to be distributed across the enterprise

The following Group Policy tasks can be independently delegated:

- Creating GPOs
- Editing GPOs
- Managing Group Policy links for a site, domain or OU
- Performing Group Policy Modeling analysis in a domain or OU
- Reading Group Policy Results data in a domain or OU
- Creating WMI filters on a domain

Modeling

What Is Group Policy Reporting?

Group Policy reporting is a method of planning and troubleshooting Group Policy

Group Policy reporting consists of two tools:

- **GPResult is a command-line utility**
- **The Group Policy Results Wizard is available in the GPMC**

What Is Group Policy Modeling?

The Group Policy Modeling Wizard calculates the simulated net effect of GPOs

The Group Policy Modeling Wizard simulates:

- **Site membership**
- **Security group membership**
- **WMI filters**
- **Slow links**
- **Loopback processing**
- **The effects of moving user or computer objects to a different Active Directory container**

Demonstration: How to Evaluate Group Policy Processing

In this demonstration, you will see how to:

- Use GPResult.exe and the Group Policy Reporting Wizard
- Use the Group Policy Modeling Wizard

Scenarios for Group Policy Troubleshooting

Common scenarios that require troubleshooting:

- ☑ **Polices not applied**
- ☑ **Policies are applied but settings are inconsistent**

Potential reasons why policies are not applied correctly:

- **Replication issues**
- **Slow network conditions**
- **Policy filtering**
- **Inheritance or enforcement**
- **Loopback processing**
- **Local computer policies**

Troubleshooting Group Policy

Group Policy issues can be caused by Group Policy-specific issues, or they can be caused by unrelated issues like network connectivity or authentication problems

Key Group Policy troubleshooting areas:

- **Inheritance**
- **Security group or WMI filtering**
- **Replication**
- **Policy refresh**

WDS = Windows Deployment Service

Tools Used for Troubleshooting Group Policy

Group Policy has a number of built-in tools that can help to expedite the troubleshooting process

Group Policy troubleshooting tools:

- **Group Policy reporting - RSoP**
- **GPResult.exe**
- **GPUpdate.exe**
- **Dcgpofix.exe**
- **GPOLogView.exe**
- **Group Policy log files**
- **Group Policy Management Scripts**

What Are Group Policy Scripts?

You can use scripts to perform many tasks, such as clearing page files or mapping drives, and clearing temp folders for users

Group Policy script settings can be used to assign:

- **For computers:**
  - **Startup scripts**
  - **Shutdown scripts**
- **For users:**
  - **Logon scripts**
  - **Logoff scripts**

Overview of Group Policy Administrative Template Settings

Administrative Templates allow you to control both the environment of the operating system and user experience

Administrative Templates sections for computers are:

- Control Panel
- Network
- Printers
- System
- Windows components

Administrative Templates sections for users are:

- Control panel
- Desktop
- Network
- Start menu and taskbar
- System
- Windows components

Each of these main sections contain many subfolders to further organize settings

What Are ADM and ADMX Files?

ADM files are:

- Copied into every GPO in SYSVOL
- Difficult to customize

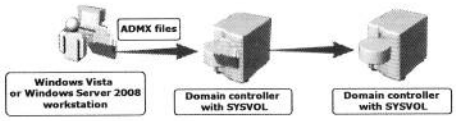
ADMX files are:

- Language neutral–ADML files provide the localized language
- Not stored in the GPO
- Extensible through XML

What Is the Central Store?

The Central Store:

- Is a central repository for ADMX and ADML files
- Is stored in SYSVOL
- Must be created manually
- Is detected automatically by Windows Vista or Windows Server 2008



Auditing Active Directory

UAC
User Admin
A/C

Beyond Trust

Split Token
Split user

Conditional Access

Monitor User Privileged Accounts

Accounts that have not been made members of any of the groups that have the highest levels of privilege in Active Directory, but have instead been granted high levels of privilege on many servers and workstations in the environment are called Privilege-attached. Even though these accounts have no privileges in Active Directory, if they are granted high privilege on large numbers of systems, they can be used to compromise or even destroy large segments of the infrastructure. This type of event achieves the same effect as compromise of a privileged Active Directory account. Privileged accounts can include administrator accounts, embedded accounts used by one system to connect to another and accounts used to run service programs

Only Use Admin Accounts When Needed

Controlling the access to network administration is very important. You have to ensure that each administrator is thoroughly trained and understands the importance of the position. Administrators should not be logged in with their administrator account if not performing administrative functions. These users should have a non-administrative account that is used for doing non-administrative tasks. It is recommended that you delegate control to the lowest level that is needed for someone to perform their job.

Granting Temporary Membership in Privileged Groups

You can create an account that can be used to manage the membership of privileged groups without requiring the account to be granted excessive rights and permissions.
Your Active Directory should contain Organizational Units (OUs) that allow for separating protected accounts from the normal user accounts.
When you create the management accounts, they should be created as a regular user account. There is no need to grant additional user rights.
After you have created the management account, make sure it is only usable for the specialized purpose for which it was created. Management accounts should have their passwords reset at each use and should be disabled when not being used.
Configure the permissions on the AdminSDHolder object to allow management accounts to change the membership of the privileged groups in the domain.

Implementing a Least-Privilege Administrative Model

One way to keep permissions simple is to grant full control permissions to everyone. Most administrators realize that this would also be a recipe for disaster. It is, however, easy to get in the habit of extending more privilege than necessary to servers, workstations, applications and Active Directory. You should always to take the time to do what is right and not what is easy.

Retire Legacy Systems and Applications

Everyone wants to get the most out of their investment, but there is a time to just say goodbye to old technology. If you are still running Windows XP or Windows Server 2003, you should be developing a plan to move on. Legacy systems, especially those that are no longer supported, are a security risk on your network. They can create backdoor opportunities for would-be hackers. When Microsoft no longer supports an operating system, security updates will no longer be issued for that platform making it a security risk.

Make Security Simple for the End User

If security measures are too difficult to follow, users will try to find a way around them. Instead of super long and complicated passwords, maybe you should move your organization to card readers or even biometrics. I have known users to minimize PowerPoint presentations or to use a fake keystroke program to prevent their systems from locking automatically. If you find your security policies are overly restrictive, you may be able to find other ways to achieve the desired results.

Physical Security

Many breaches of security do come in the form of a hacker exploiting a software vulnerability. Still, don't overlook physical security. You may want to take steps to prohibit flash drive user or the ability to burn DVDs. This may keep your data from walking away without permission. You can also never underestimate the importance of a locked door. If someone has physical access to your datacenter, then they also have the ability to destroy or remove drives, processors, etc.
It seems like every day, there is a new report about a company being hacked. Whether it is Home Depot, Target, OPM or Anthem, every company who has a presence on the internet is a potential victim. Make sure that you take all necessary steps to secure your Active Directory environment.

Auditing changes to objects in AD DS

In Windows 2000 Server and Windows Server 2003, there was one audit policy, Audit directory service access, that controlled whether auditing for directory service events was enabled or disabled. In Windows Server 2008, this policy is divided into four subcategories:

Directory Service Access

Directory Service Changes

Directory Service Replication

Detailed Directory Service Replication

New audit policy subcategory Directory Service Changes

- When a successful modify operation is performed on an attribute, AD DS logs the previous and current values of the attribute. If the attribute has more than one value, only the values that change as a result of the modify operation are logged.

- If an object is moved, the previous and new location (distinguished name) is logged for moves within the domain. When an object is moved to a different domain, a create event is generated on the domain controller in the target domain.

- If a new object is created, values of the attributes that are populated at the time of creation are logged. If the user adds attributes during the create operation, those new attribute values are logged. In most cases, AD DS assigns default values to attributes (such as **samAccountName**). The values of such system attributes are not logged.

- If an object is undeleted, the location where the object is moved to is logged. In addition, if the user adds, modifies, or deletes attributes while performing an undelete operation, the values of those attributes are logged.

SACL (Security Access Control List)

The SACL on the object is still the ultimate authority in determining whether an access check must be audited or not. The SACL is the part of an object's security descriptor that specifies which operations are to be audited for a security principal.
The content of the SACL is controlled by security administrators for the local system. Security administrators are users who have been assigned the Manage Auditing and Security Log (SeSecurityPrivilege) privilege. By default, this privilege is assigned to the built-in Administrators group.
If there is no access control entry (ACE) in the SACL requiring attribute modifications to be logged, even if the Directory Service Changes subcategory is enabled, no change auditing events are logged. For example, if there is no ACE in a SACL requiring Write Property access on the telephone number attribute of a user object to be audited, no auditing events are generated when the telephone number attribute is modified, even if the subcategory Directory Service Changes is enabled.

Schema

To avoid the possibility of an excessive number of events being generated, there is an additional control in the schema that you can use to create exceptions to what is audited.
For example, if you want to see what values have changed as a result of all but a few attribute modifications on a user object, you can set a flag in the schema for the attributes that you do not want audited. The searchFlags property of each attribute defines behavior such as whether the attribute is indexed or replicated to the global catalog. The searchFlags property has seven currently-defined bits.
If bit 8 (zero-based indexing, value 256) is set for an attribute, AD DS will not log change events when modifications are made to the attribute. This applies to all objects that contain that attribute.

Example modify operation and log entry

SACL	User action	Audit policy settings	Audit events logged
Object: CN=GroupX, CN=Users, <domain DN> ACE in SACL: [WP; AU]	Object modified: CN=GroupX, CN=Users, <domain DN> Attribute modified: **Member** Operation: Add Value: User1 Attribute modified: **Description** Operation: Add Value: Group of users with role X	Subcategory: **Directory Service Access** ON Subcategory: **Directory Service Changes** ON Description attribute in schema: search flag bit 8 set to disable change auditing	Event ID: 4662 Object: CN=GroupX, CN=Users, <domain DN> Permission: Write Property Attributes: **Member** **Description** Event ID: 5136 Object: CN=Group X, CN=Users, <domain DN> Operation: Add Attribute: **Member** Value: **User1**

Benefits of auditing changes in AD DS

If you can identify how object attributes have changed, the event logs are more useful as a tracking mechanism for changes that occur over the lifetime of an object.

How to set up AD DS auditing

Steps to set up auditing
This section includes procedures for each of the primary steps for enabling change auditing:
Step 1: Enable audit policy.

Step 2: Set up auditing in object SACLs by using Active Directory Users and Computers.

Step 1: Enable audit policy.
This step includes procedures to enable change auditing with either the Windows interface or a command line:

·By using Group Policy Management, you can turn on the global audit policy, Audit directory service access, which enables all the subcategories for AD DS auditing. If you need to install Group Policy Management, click Add Features in Server Manager. Select Group Policy Management and then click Install.

·By using the Auditpol command-line tool, you can enable individual subcategories.

To enable the global audit policy using the Windows interface

1.Click Start, point to Administrative Tools, and then Group Policy Management.
2.In the console tree, double-click the name of the forest, double-click Domains, double-click the name of your domain, double-click Domain Controllers, right-click Default Domain Controllers Policy, and then click Edit.
3.Under Computer Configuration, double-click Policies, double-click Windows Settings, double-click Security Settings, double-click Local Policies, and then click Audit Policy.
4.In the details pane, right-click Audit directory service access, and then click Properties.
5.Select the Define these policy settings check box.
6.Under Audit these attempts, select the Success, check box, and then click OK.

To enable the change auditing policy using a command line

1.Click Start, right-click Command Prompt, and then click Run as administrator.
2.Type the following command, and then press ENTER:
3.auditpol /set /subcategory:"directory service changes" /success:enable

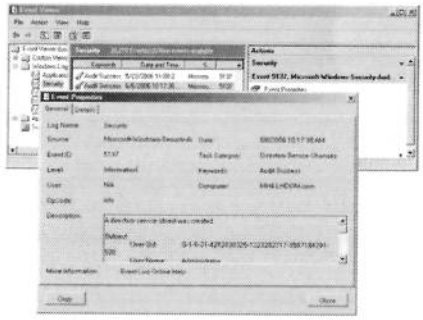
Step 2: Set up auditing in object SACLs.

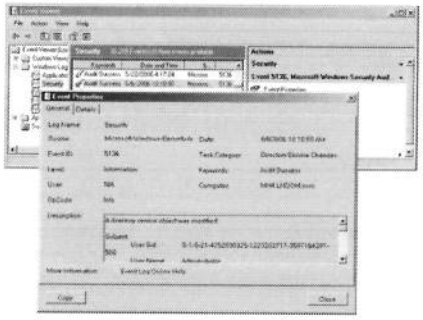
The following procedure presents an example of just one of many different types of SACLs that you can set based on the operations that you want to audit.

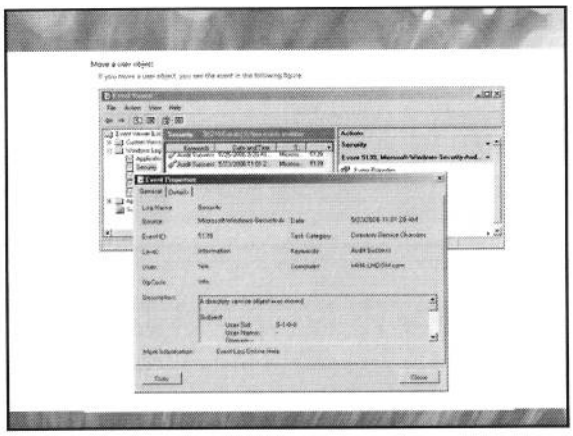
To set up auditing in object SACLs

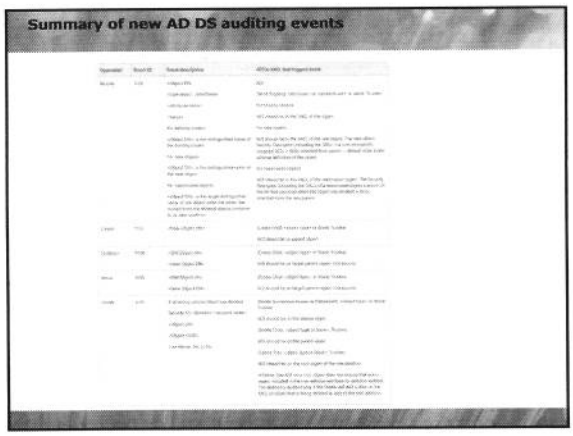
1. Click Start, point to Administrative Tools, and then click Active Directory Users and Computers.
2. Right-click the organizational unit (OU) (or any object) for which you want to enable auditing, and then click Properties.
3. Click the Security tab, click Advanced, and then click the Auditing tab.
4. Click Add, and under Enter the object name to select, type Authenticated Users (or any other security principal), and then click OK.
5. In Apply onto, click Descendant User objects (or any other objects).
6. Under Access, select the Successful check box for Write all properties.
7. Click OK until you exit the property sheet for the OU or other object.

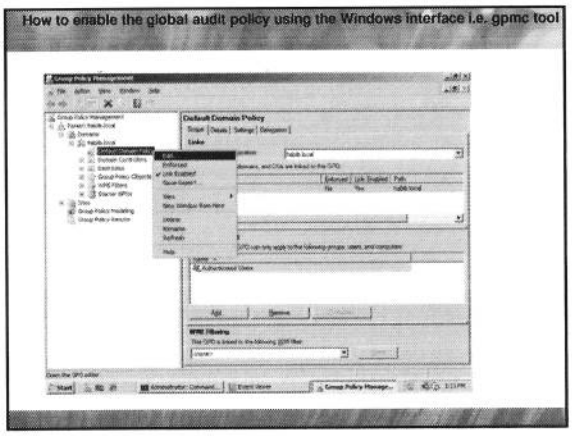
Example audit events

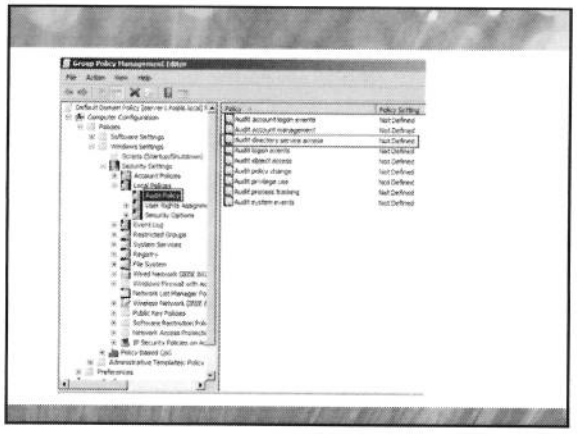


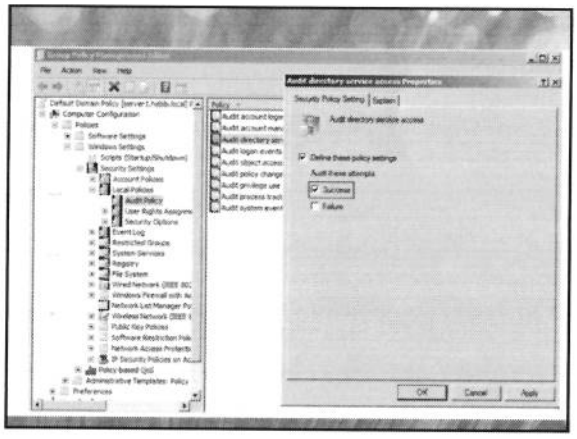





Summary of new AD DS auditing events


How to enable the global audit policy using the Windows interface i.e. gpmc tool





How to enable the change auditing policy using a command line

- **Click Start, right-click** Command Prompt, **and then click** Run as administrator.
- **Type the following command, and then press ENTER:**
- auditpol /set /subcategory:"directory service changes" /success:enable

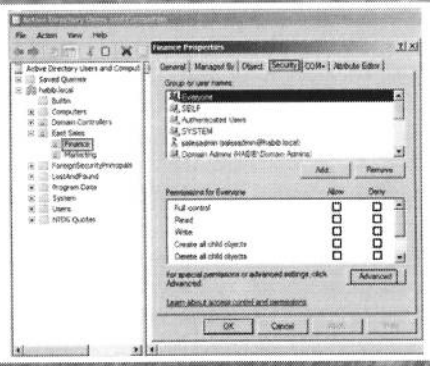
To verify if the auditing is enabled or not for "Directory Service Changes", you can run below command:

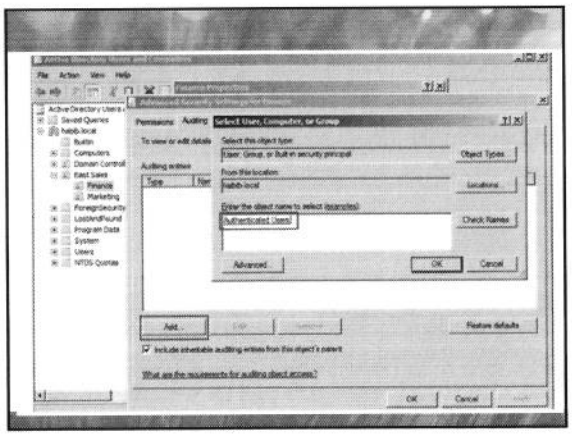
```
Auditpol /get /category:"DS Access"
```

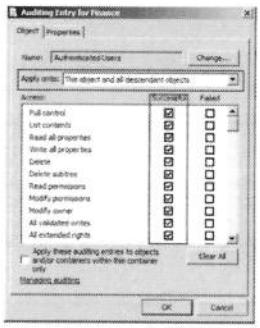
Administrator: Command Prompt

```
C:\>auditpol /set /subcategory:"directory service changes" /success:enable
The command was successfully executed.

C:\>auditpol /get /category:"DS Access"
System audit policy
Category/Subcategory                    Setting
DS Access
  Directory Service Changes             Success
  Directory Service Replication         No Auditing
  Detailed Directory Service Replication No Auditing
  Directory Service Access              No Auditing

C:\>
```

How to set up auditing in object SACLs

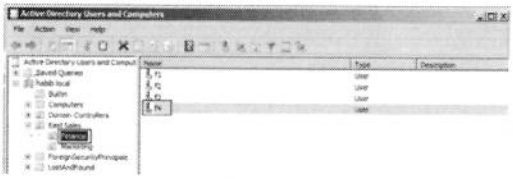




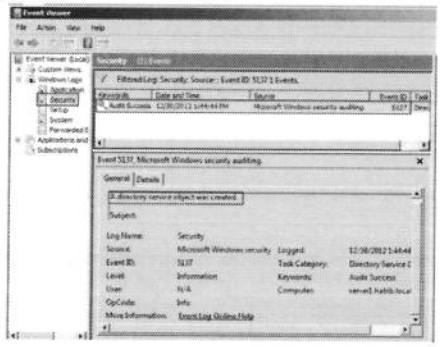


To Test whether auditing is working or not, try creating or modifying objects in Finance OU and check the Security event logs

I just created a new user account in Finance OU named f4.



If you check the security event logs you will find eventid 5137 (Create)



Change Auditor for Active Directoy - Quest Software

Change Auditor for Active Directory helps ensure the security, compliance and control of AD and Azure AD. The solution proactively protects objects and tracks all changes in real time with complete visibility. Easily detect insider attacks and accidental changes with reports, alerts and visibility into events and actions without the complexity of native tools.

https://www.quest.com/products/change-auditor-for-active-directory/

ManageEngine

ADAudit Plus

REAL-TIME WINDOWS ACTIVE DIRECTORY AUDITING
In real-time, ensure critical resources in the network like the Domain Controllers are audited, monitored and reported with the entire information on AD objects - Users, Groups, GPO, Computer, OU, DNS, AD Schema and Configuration changes with 200+ detailed event specific GUI reports and email alerts.

https://www.manageengine.com/products/active-directory-audit/

Lepide

Active Directory Auditing
It is our belief that all organizations, irrespective of size, sector or budget, should be able to easily audit Active Directory changes without breaking the bank. Our award-winning Active Directory change auditing solution provides a scalable means to instantly track who, what, where and when changes are made to your Active Directory. It sends real time alerts and provides detailed Active Directory audit reports to help with all manner of security, systems management and compliance challenges.
Aside from alerting, reporting and meeting compliance mandates, this audit solution also offers users the ability to rollback changes made to Active Directory and an integrated HealthCheck monitoring of Active Directory. It provides a simple way of tracking and managing inactive Active Directory user accounts.

https://www.lepide.com/lepideauditor/active-directory-auditing.html

netwrix

Active Directory Auditing

- Get Alerts in Real Time
- Report on Any-Point-in-Time Configurations
- Rollback Unwanted Changes
- See Who did What, When & Where

https://www.netwrix.com/active_directory_auditing.html

Penetration Testing

About Your Instructor

Jay Ferron

CEHi, CISSP, CHFIi, C)PTEi, CRISC, CVEi, MCITP, MCSE, MCT, MVP, NSA-IAM...

jferron@interactivesecuritytraining.com

blog.mir.net

203-675-8900 Phone

Penetration Testing

Definition of Penetration Testing:

- A penetration test or pentest is a test evaluating the strengths of all security controls on the computer system. Penetration tests evaluate procedural and operational controls as well as technological controls.

What is Pen Testing?

Security testing is the process of providing evidence of how well an application satisfies its security requirements.

Penetration testing is a method of security testing, in which testers simulate the efforts of attackers.

Who needs Penetration Testing

- Banks/Financial Institutions, Government Organizations, Online Vendors, or any organization processing and storing private information

- Most certifications require or recommend that penetration tests be performed on a regular basis to ensure the security of the system.

- PCI Data Security Standard's Section 11.3 requires organizations to perform application and penetration tests at least once a year.

- HIPAA Security Rule's section 8 of the Administrative Safeguards requires security process audits, periodic vulnerability analysis and penetration testing.

Penetration Testing Viewpoints

-External vs. Internal

Penetration Testing can be performed from the viewpoint of an external attacker or a malicious employee.

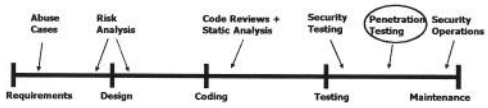
- Overt vs. Covert

Penetration Testing can be performed with or without the knowledge of the IT department of the company being tested.

What is Pen Testing?

Penetration testing evaluates the security of software in its deployed environment.

- Effect of firewalls
- Deployed cryptographic libraries
- Effect of other security services and processes



Purposes of Pen Tests

1. Identify vulnerabilities that may be difficult or impossible to detect in design or code reviews.
2. Determine the feasibility of certain attacks.
3. Assess the impact of potential attacks.
4. Test the ability of system to detect attacks.
5. Provide evidence to support increased investments in security.

Vulnerability Assessment VS Penetration Testing

Vulnerability Assessment :

It detects vulnerabilities of a system and also provides an overview of the flaws exists in a system .

Penetration testing :

It gains unauthorized access to the network or system and identifies possible impacts of system flaws .

Risk = Asset Value * Vulnerability * Threat

Rules of Engagement

Which systems are being tested?
- Deployment or development?
- Web, DB, others?

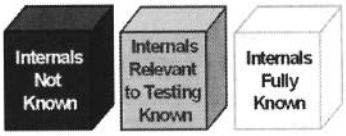
What tests will be performed?
- Read-only
- Read-write
- DoS

When will the tests be performed?

Who to contact if tests cause problems?

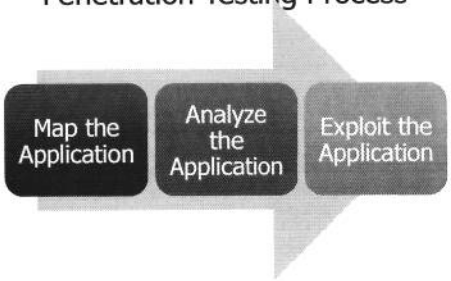
Black, White, Grey Box Testing

Conceptual Difference Among Three Types of Testing



www.softwaretestinggenius.com

Penetration Testing Process



Phases of Penetration Testing

- Reconnaissance and Information Gathering
- Network Enumeration and Scanning
- Vulnerability Testing and Exploitation
- Reporting

Reconnaissance and Information Gathering

Purpose: To discover as much information about a target (individual or organization) as possible without actually making network contact with said target.

Methods:
- Organization info discovery via WHOIS
- Google search
- Website browsing

WHOIS Results for www.isacact.org

Contact Information

Registrant Contact	Admin Contact	Tech Contact
Name: Perfect Privacy, LLC	Name: Perfect Privacy, LLC	Name: Perfect Privacy, LLC
Organization: GREATER HARTFORD CHAPTER ISACA	Organization: ISACA Greater Hartford Chapter	Organization: GREATER HARTFORD CHAPTER ISACA
Mailing Address: 12808 Gran Bay Parkway West, Jacksonville FL 32258 US	Mailing Address: 12808 Gran Bay Parkway West, Jacksonville FL 32258 US	Mailing Address: 12808 Gran Bay Parkway West, Jacksonville FL 32258 US
Phone: +1.5707082700	Phone: +1.5707082700	Phone: +1.5707082700
Ext:	Ext:	Ext:
Fax:	Fax:	Fax:
Fax Ext:	Fax Ext:	Fax Ext:
Email: wkapelgaffin@netwoknwtw-rempin-wkewgfaitions.com	Email: w7fm3xc576@networkwtw-rempin-wafenegfaition.com	Email: wkapelgaffin@netwoknwtw-rempin-wafenegfaition.com

Registrar

WHOIS Server:
URL:
Registrar:
IANA ID:
Abuse Contact Email:
Abuse Contact Phone:

Status

Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited

Network Enumeration and Scanning

Purpose: To discover existing networks owned by a target as well as live hosts and services running on those hosts.

Methods:
- Scanning programs that identify live hosts, open ports; services, and other info (Nmap, autoscan)
- DNS Querying
- Route analysis (traceroute)

Vulnerability Testing and Exploitation

Purpose: To check hosts for known vulnerabilities and to see if they are exploitable, as well as to assess the potential severity of said vulnerabilities.

Methods:
- Remote vulnerability scanning (Nessus, OpenVAS)
- Active exploitation testing
  - Login checking and bruteforcing
  - Vulnerability exploitation (Metasploit, Core Impact)
  - 0day and exploit discovery (Fuzzing, program analysis)
  - Post exploitation techniques to assess severity (permission levels, backdoors, rootkits, etc)

Reporting

Purpose: To organize and document information found during the reconnaissance, network scanning, and vulnerability testing phases of a pentest.

Methods:
- Documentation tools (Dradis)
  - Organizes information by hosts, services, identified hazards and risks, recommendations to fix problems

Penetration Testing Overview

Penetration testing is a security testing methodology that gives an attacker insight into the target's security posture and the strength of the target's network security. A complete security snapshot includes:

Level I, High-level assessment. A top-down look at the organization's policies, procedures, standards and guidelines. A Level I assessment is not usually hands-on, in that the system's security is not actually tested.

Level II, Network evaluation. More hands-on than a Level I assessment, a Level II assessment has some of the Level I activities with more information gathering and scanning.

Level III, Penetration test. A penetration test is not usually concerned with policies. It's more about taking the adversarial view of a hacker, by seeing what can be accomplished and with what difficulty.

The need of Penetration Testing

The reason a security professional may wish to conduct a penetration test of his or her company is the same as the reason a business has a security policy

Several factors have converged in the marketplace to make penetration testing a necessity.

The skill level required to execute a hacker exploit has steadily decreased.

The size and complexity of the network environment has mushroomed.

The number of network and Web-based applications has increased.

The detrimental impact of a security breach on corporate assets and goodwill is greater than ever.

Penetration Testing Phases

Penetration testing is most commonly carried out within a *black-box (that is,* with no prior knowledge of the infrastructure to be tested). At its simplest level, the penetration test involves three phases

Preparation phase. A formal contract is executed containing nondisclosure of the client's data and legal protection for the tester. At a minimum, it also lists the IP addresses to be tested and the time to test.

Execution phase. The penetration test is executed, with the tester looking for potential vulnerabilities

Delivery phase. The results of the evaluation are communicated to the tester's contact in the organization, and corrective action is advised.

Legal and Ethical Implications

Attacking a network from the outside carries ethical and legal risk to the tester,and remedies and protections must be spelled out in detail before the test is begun.

For example, the Cyber Security Enhancement Act 2002 implicates life sentences for hackers who "recklessly" endanger the lives of others, and several U.S. statutes address cyber crime. Statute 1030, *Fraud and Related Activity in Connection with Computers, specifically states that whoever intentionally accesses a* protected computer without authorization

Legal and Ethical Implications.....

It's vital that the tester receive specific written permission to conduct the test from the most senior executive possible. A tester should be specifically indemnified against prosecution for the work of testing.

The Three Pretest Phases

Penetration testing usually starts with three pretest phases: **footprinting**, **scanning**, and **enumerating.**

These pretest phases are very important and can make the difference between a successful penetration test that provides a complete picture of the target's network and an unsuccessful test that does not

Together, the three pretest phases are called *reconnaissance*

- Gather initial information
- Determine the network range
- Identify active machines
- Discover open ports and access points
- Fingerprint the operating system
- Uncover services on ports
- Map the network

Footprinting

"Footprinting" is the blueprinting of the security profile of an organization.

It involves gathering information about your target's network to create a profile of the organization's networks and systems.

It's an important way for an attacker to gain information about an organization passively (that is, without the organization's knowledge).

"Footprinting" employs the first two steps of reconnaissance: gathering the initial target information and determining the network range of the target

Common tools and resources used in the footprinting phase are:

- Whois
- SmartWhois
- Nslookup
- Sam Spade

Footprinting (Manual Research)

Company contact names, phone numbers, and email addresses

Company locations and branches

Other companies with which the target company partners or deals

News, such as mergers or acquisitions

Links to other company-related sites

Company privacy policies, which may help identify the types of security mechanisms in place

Other resources that may have information about the target company are:

- The SEC's EDGAR database if the company is publicly traded
- Job boards, either internal to the company or external sites
- Disgruntled employee blogs and Web sites
- Trade press

Scanning

The next four steps of gathering information (identifying active machines, discovering open ports and access points, fingerprinting the operating system, and uncovering services on ports) are considered part of the scanning phase

Your goal here is to discover open ports and applications by performing external or internal network scanning, pinging machines, determining network ranges, and scanning the ports of individual systems

Some common tools used in the scanning phase are

- Nmap
- Ping
- Traceroute
- SuperScan
- Netcat
- NeoTrace
- Visual Route

SNMPutil

SNMP → MIBS
↑ Port 61 ↳ Command Read
password : Public

Enumerating

The last step mentioned, mapping the network, is the result of the scanning phase and leads us to the enumerating phase. As the final pretest phase, the goal of enumeration is to paint a fairly complete picture of the target

To enumerate a target, a tester tries to identify valid user accounts or poorly protected resource shares using directed queries and active connections to and from the target

The type of information sought by testers during the enumeration phase can be names of users and groups, network resources and shares, and applications. The techniques used for enumerating include

- Obtaining Active Directory information and identifying vulnerable user accounts
- Discovering the NetBIOS name with Nbtscan
- Using SNMPutil for SNMP
- Employing Windows DNS queries
- Establishing null sessions and connections
- Note:- Document every step taken during penetration testing

Penetration Testing Tools and Techniques

Several tools, including public sources such as Whois and Nslookup, can help you gather information about your target network

With "Whois", you can find information like the domain's registrant, its administrative and technical contacts, and a listing of their domain servers

Nslookup allows you to query Internet domain name servers.

It displays information that can be used to diagnose Domain Name System (DNS) infrastructure and find additional IP addresses.

The common traceroute utility is also very handy. Traceroute works by exploiting a feature of the Internet Protocol called Time to Live (TTL).

Penetration Testing Tools and Techniques.....

It reveals the path IP packets travel between two systems by sending out consecutive UDP packets with ever-increasing TTLs

As each router processes an IP packet, it decrements the TTL. When the TTL reaches zero, the router sends back a "TTL exceeded" ICMP message to the origin.

Thus, routers with DNS entries reveal their names, network affiliations, and geographic locations

Penetration Testing Tools and Techniques.....

Here are other useful Windows-based tools for gathering information:

VisualRoute. VisualRoute by VisualWare includes integrated traceroute, ping tests, and reverse DNS and Whois lookups. It also displays the actual route of connections and IP address locations on a global map.

SmartWhois. Like Whois, SmartWhois by TamoSoft obtains comprehensiveinfo about the target: IP address, host name or domain, including country, state or province, city, name of the network provider, administrator and technical support, and contact information.SmartWhois can find the information about a computer located in any part of the world, intelligently querying the right database and delivering all the related records within a few seconds

Sam Spade. Sam Spade, a freeware tool primarily used to track down spammers, can also be used to provide information about a target. It comes with a host of useful network tools, including ping, Nslookup, Whois, IP block Whois, dig, traceroute, finger, SMTP, VRFY, Web browser, keep-alive, DNS zone transfer, SMTP relay check, and more

Port Scanners

Port scanning is one of the most common reconnaissance techniques used by testers to discover the vulnerabilities in the services listening to well-known ports.

Once you've identified the IP address of a target through footprinting, you can begin the process of port scanning:

looking for holes in the system through which you, or a malicious intruder, can gain access. A typical system

has 2^16 -1 port numbers, each with its own TCP and UDP port that can be used to gain access if unprotected.

Port Scanners "nmap"

Nmap, the most popular port scanner for Linux, is also available for Windows

Nmap can scan a system in a variety of stealth modes, depending upon how undetectable you want to be

Nmap can determine a lot of information about a target, such as what hosts are available, what services are offered, and what OS is running

Vulnerability Scanners

Nessus, a popular open-source tool, is an extremely powerful network scanner that can be configured to run a variety of scans. While a Windows graphical front-end is available, the core Nessus product requires Linux to run.

Microsoft's Baseline Security Analyzer is a free Windows vulnerability scanner. MBSA can be used to detect security configuration errors on local computers or on computers across a network, and it is now in its second release.

It does have some issues with Windows Update, however, and can't always tell if a patch has been installed.

Popular commercial vulnerability scanners include Retina Network Security Scanner, which runs on Windows, and SAINT, which runs on various Unix/ Linux versions

Password Crackers

Three basic types of password-cracking tests can be automated with tools:

Dictionary. A file of words is run against user accounts; if the password is a simple word, it can be found pretty quickly.

Hybrid. A hybrid attack works like a dictionary attack but adds simple numbers or symbols to the file of words. This attack exploits a weakness of many passwords: They are common words with numbers or symbols tacked to the ends.

Brute force. The most time-consuming but comprehensive way to crack a password. Every combination of character is tried until the password is broken.

Password Crackers

Brutus is a password-cracking tool that can perform both dictionary attacks and brute force attacks where passwords are randomly generated from a given character. It can crack the multiple authentication types, HTTP (Basic authentication, HTML Form/CGI), POP3, FTP, SMB, and Telnet.

WebCracker. WebCracker is a simple tool that takes text lists of usernames and passwords and uses them as dictionaries to implement basic password guessing.

ObiWan. ObiWan is a password-cracking tool that can work through a proxy. It uses wordlists and alternates numeric or alphanumeric characters with Roman characters to generate possible passwords.

Trojan Horses

An unauthorized program contained within a legitimate program

A legitimate program that has been altered by the placement of unauthorized code within it

Any program that appears to perform a desirable and necessary function but does something unintended

Trojans can be transmitted to the computer in several ways

- Email attachments
- freeware, physical installation
- ICQ/IRC chat
- infected websites

Trojan Horses

The list of Trojan horses in the wild is expanding quickly, but a few of the earliest have remained relevant since the beginning, and many of these serve as platforms for the development of more lethal variations

Trojans can be:

- Remote access Trojans
- Keystroke loggers or password-sending Trojans
- Software detection killers
- Purely destructive or denial-of-service Trojans

Buffer Overflows

A buffer overflow (or overrun) occurs when a program allocates a specific block length of memory for something but then attempts to store more data than the block was intended to hold.

This overflowing data can overwrite memory areasand interfere with information crucial to the normal execution of the program

To generate the overflow, the attacker must create a specific data feed to induce the error, as random data will rarely produce the desired effect

For a buffer overflow attack to work, the target system must fail to test the data or stack boundaries and must also be able to execute code that resides in the data or stack segment

Once the stack is smashed, the attacker can deployhis or her payload and take control of the attacked system

Buffer Overflows

Three common ways to test for a buffer overflow vulnerability are as follows:

- Look for strings declared as local variables in functions or methods, and verify the presence of boundary checks in the source code.
- Check for improper use of input/output or string functions.
- Feed the application large amounts of data and check for abnormal behavior.

SQL Injection Attack

- SQL injection is an example of a class of injection exploits that occur when one scripting language is embedded inside another scripting language.
- The injection targets the data residing in a database through the firewall in order to alter the SQL statements and retrieve data from the database or execute commands.
- It accomplishes this by modifying the parameters of a Web-based application.
- An injection attack will allow an attacker to execute SQL codeon a server, such as SHUTDOWN WITH NOWAIT, which causes the server to shut down and stop services immediately.
- For example, creating a username with 1=1, a', or 't'='t or any text within single quotes could force the execution of SQL commands on a vulnerablesystem

SQL Injection Attack Prevention

Preventing SQL injection vulnerability involves enforcing better coding practices and database administration procedures. Here are some specific steps to take

- Disable verbose error messages that give information to the attacker
- Protect the system account (sa). It's very common for the sa passwordto be < blank >
- Enforce the concept of least privilege at the database connection
- Secure the application by auditing the source code to
  - Restrict length of input
  - Avoid single quotes
  - Whitelist good input
  - Blacklist bad input

Cross Site Scripting (XSS)

- Web application attacks are often successful because the attack is not noticed immediately. One such attack exploits the Cross Site Scripting (XSS) vulnerability
- An XSS vulnerability is created by the failure of a Web-based application to validate user-supplied input before returning it to the client system
- Attackers can exploit XSS by crafting malicious URLs and tricking users into clicking on them
- These links enable the attacker's client-side scripting language, such as JavaScript or VBScript, to execute on the victim's browser
- Many Web application vulnerabilities can be minimized by adhering to proper design specifications and coding practices and implementing security early in the application's development lifecycle

MAC Address Vulnerabilities

- MAC addresses are easily sniffed by an attacker since they must appear in the clear even when WEP is enabled.
- An attacker can masquerade as a valid MAC address by programming the wireless card to enter the wireless network.
- Spoofing MAC addresses is also very easy. Using packet capturing software, an attacker can determine a valid MAC address by setting up a rogue access point near the target wireless network

WLAN Vulnerabilities

- Wireless LANs are susceptible to the same protocol-based attacks that plague wired LAN but also have their own set of unique vulnerabilities.
- Since wireless access points may proliferate in the organization, unsecured wireless access points can be a danger to organizations because they offer the attacker a route around the company's firewall and into the network

SSID Issues

- The service set identifier (SSID) is an identification value programmed in the access point or group of access points to identify the local wireless subnet
- This segmentation of the wireless network into multiple networks is a form of an authentication check
- SSID acts as a simple password, providing a measure of security. When a client computer is connected to the access point
- The wireless access point is configured to broadcast its SSID. When enabled, any client without an SSID is able to receive it and have access to the access point
- Many access points use default SSIDs provided by the manufacturers, and a list of those default SSIDs is available for download on the Internet
- This means that it's very easy for a hacker to determine an access point's SSID and gain access to it via software tools

Wireless Network Penetration Testing

- The rapid popularity of wireless networking technologies has introduced a host of new security issues
- *War driving is a term used to describe the process of a hacker who, armed* with a laptop and a wireless adapter card and traveling by car, bus, subway train, or other form of mechanized transport, goes around sniffing for WLANs
- *War walking refers to the same process, commonly in public areas like malls,* hotels, or city streets, but using shoe leather instead of the transportation methods listed earlier
- The hacker moves from place to place, letting these devices do their jobs. Over time, the hacker builds up a database containing the network name, signal strength, location, and IP/namespace in use for all of the discovered wireless hotspots

Wireless Network Penetration Testing.....

- With SNMP, the hacker may even log packet samples and probe the access points for available data
- This is called *war chalking and alerts other intruders that an exposed WLAN is nearby*
- Common war-driving exploits find many wireless networks with WEP disabled and using only the SSID for access control.
- The SSID for wireless networks can be found quickly. This vulnerability makes these networks susceptible to what's called the *parking lot attack, where, at a safe distance from* the building's perimeter, an attacker gains access to the target network

WEP Weaknesses

Wired Equivalent Privacy (WEP) is a component of the IEEE 802.11 wireless local area network WLAN standard. Its primary purpose is to provide confidentiality of data on wireless networks at a level equivalent to that of wired LANs

This is accomplished by encrypting data with the RC4 encryption algorithm

Nevertheless, WEP is vulnerable because of relatively short keys that remain static.

Most WEP products implement a 64-bit shared key, using 40 bits of this for the secret key and 24 bits for the initialization vector.

The key is installed at the wired network AP and must be entered into each client as well

WEP was not designed to withstand a directed cryptographic attack

Wireless Scanning Tools

AirSnort

AirSnort is a WLAN tool that cracks WEP encryption keys. AirSnort passively monitors wireless transmissions and automatically computes the encryption key when enough packets have been gathered.

MiniStumbler

This is a smaller version of NetStumbler designed to work on PocketPC 3.0 and PocketPC 2002 platforms. It rovides support for ARM, MIPS, and SH3 CPU types

NetStumbler

NetStumbler displays wireless access points, SSIDs, channels, whether WEP encryption is enabled, and signal strength. NetStumbler can connect with GPS technology to log the precise location of access points

Wireless Scanning Tools.....

WifiScanner

WifiScanner analyzes traffic and detects 802.11b stations and access points. It can listen alternatively on all 14 channels, write packet information in real time, and search access points and associated client stations. All network traffic may be saved in the libpcap format for analysis

SSID Sniff

A tool to use when looking to discover access points andsave captured traffic. Comes with a configured script and supportsCisco Aironet and random prism2 based cards

Kismet

Kismet is an 802.11 wireless network detector, sniffer, and intrusion detection system. Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of nonbeaconing networks via data traffic.

Social Engineering

Common techniques used by an intruder to gain either physical access or system access are

- Asserting authority or pulling rank
- Professing to have the authority, perhaps supported with altered identification to enter a facility or system
- Browbeating the access control subjects with harsh language or threatening behavior to permit access or release information
- Praising, flattering, or sympathizing
- Using positive reinforcement to coerce a subject into providing access or information for system access

Social Engineering.....

Some examples of successful social engineering attacks are:

- Emails to employees from a tester requesting their passwords to validate
- the organizational database after a network intrusion has occurred
- Emails to employees from a tester requesting their passwords because work has to be done over the weekend on the system
- An email or phone call from a tester impersonating an official who is conducting an investigation for the organization and requires passwords for the investigation

Social Engineering.....

Some examples of successful social engineering attacks are:

- An improper release of medical information to individuals posing as medical personnel and requesting data from patients' records
- A computer repair technician who convinces a user that the hard disk on his or her PC is damaged and irreparable, and installs a new hard disk for the user, then takes the hard disk, extracts the information, and sells the information to a competitor or foreign government

IDS and Penetration

- The IDS monitors packets on the network wire and endeavors to discover if a tester is attempting to break into a system
- Anomaly detection systems employ a baseline of statistics such as CPU utilization, disk activity, user logins, file activity, and so on. Then network activity is matched against this baseline
- After capturing packets, a good IDS uses several techniques to identify information in the packets indicative of an attack, such as protocol stack verification and application protocol verification
- *Protocol stack verification looks for intrusions, such as Ping-O-Death and TCP* Stealth Scanning, that use violations of the IP protocols to attack.
- The verification system can flag invalid packets, which can include valid but suspicious behavior such as frequent, fragmented IP packets

IDS and Penetration.....

- *Application protocol verification looks for intrusions that use invalid protocol* behavior, such as WinNuke. WinNuke uses the NetBIOS protocol
- Since many IDS simply rely on matching the patterns of well-known attack scripts, they can easily be evaded by simply changing the script and altering the appearance of the attack.
- For example, some POP3 servers are vulnerable to a buffer overflow when a long password is entered. This may be easy to evade by simply changing the password script