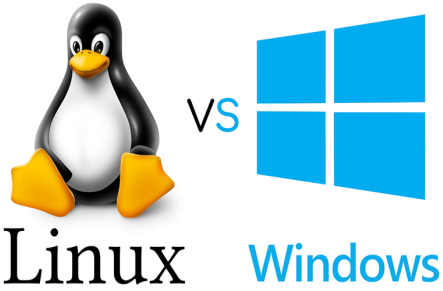
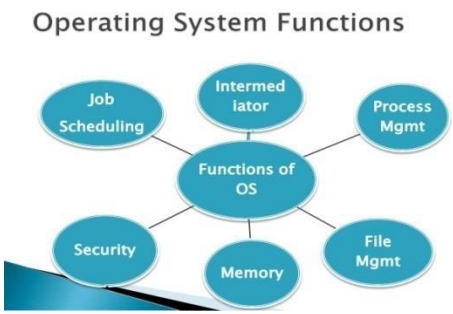
CIT210 OP. SYS. MANAG.

CSUN
COLLEGE OF ENGINEERING AND COMPUTER SCIENCE

Week14Day2 : OS Security Management, Group Policy Management, Incident Response Plan, Group Police Inheritance, Security Incident, Logon/Logoff Event ID, Best Practices of Incidence Handling





Group Policy and Group Policy Objects

- Centralized set of rules that govern the way Windows operates.
- Group Policy uses a “pull” technology, which means that Windows periodically searches for any updated GPOs. If it finds a new GPO, it downloads and applies the changes to the existing environment
- Windows checks for new or updated GPOs at a random interval between every 90 to 120 minutes.

What Are Group Policies?

Group Policies enable IT administrators to automate one-to-many management of users and computers

Use Group Policies to:

- Apply standard configurations
- Deploy software
- Enforce security settings
- Enforce a consistent desktop environment

Local group policies are always in effect for local and domain users and local computer settings

Introduction to Group Policy

- Group policy centralizes management of user and computer configuration settings throughout a network
- A group policy object is an Active Directory object used to configure policy settings for user and computer objects
- There are two default Group Policy Objects:
  - Default Domain Policy (linked to domain container)
  - Default Domain Controllers Policy (linked to domain controller OU)

TABLE 6-1 Categories of settings in GPOs.

CATEGORY	DESCRIPTION
Password Policy	Requirements for password strength, age, history, and how Windows stores passwords
Account Lockout Policy	How Windows handles accounts locked after failed login attempts
Kerberos Policy	Lifetime limits for Kerberos tickets and clock synchronization
Audit Policy	Defines events Windows should record in audit files
User Rights Assignment	Individual user rights that define what general actions users can perform, such as "Access this computer from the network" or "Change the system time"
Security Options	Rights that define what security related actions users can perform, such as "Allowed to format and eject removable media" or "Require smart card"
Event Log	Defines maximum size, retention settings, and guest access settings for event logs
Restricted Groups	Lists users in security-sensitive groups and to what other groups the restricted group can belong
System Services	Defines startup mode and access permissions for system services
Registry	Define access permissions and audit settings for registry keys
File System	Defines access permissions on Discretionary Access Control Lists DACLs and audit settings for System Access Control Lists (SACLs)

Making Group Policy

- Making Group Policy conform to your security policy is a three-step process.
  - First, examine a list of GPO settings that already exist in the default Windows templates.
  - Identify any GPO settings that satisfy parts of your security policy. Activate all settings that are appropriate for your policy.
  - The second step is to identify any elements in your security policy that do not already exist in default Windows templates.
  - The third step in making Group Policy conform to your security policy is to create new GPOs for each of the remaining goals in your security policy that you identified in the second step.

Introduction to Group Policy (continued)

- You can modify default GPOs
- You can create new GPOs and link them to particular sites, domains, and OUs
  - Policy settings will be propagated to all users and computers in container including child OUs
- Group policy can only be applied to computers running Windows Server.
- Two ways to create a GPO:
  - Group Policy standalone Microsoft Management Console (MMC) snap-in
  - Group Policy extension in Active Directory Users and Computers

Group Policy Targets

- Local GPOs — GPOs defined and stored on the local computer
- Site GPOs defined in AD — GPOs defined in AD for a specific site
- Domain GPOs — Domain-wide GPOs defined in AD
- Organizational Unit GPO — OU GPOs defined in AD

FIGURE 6-2

Group Policy Object order.

- **Any setting in a higher-level GPO will override a lower-level GPO setting. For example, a setting in a domain GPO will override a conflicting setting in a local GPO.**

Editing a GPO

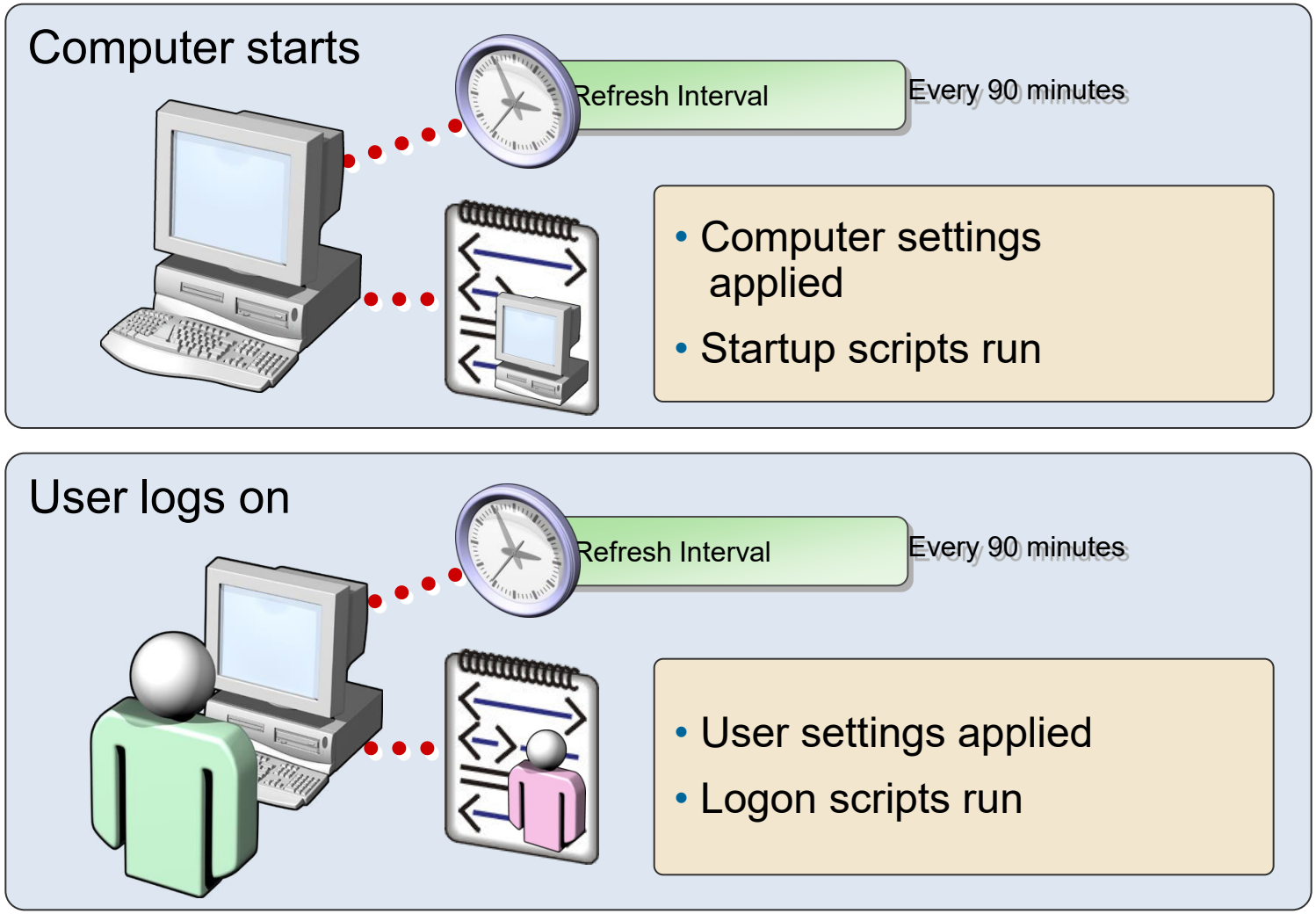
Table 9-1 Configuration categories available for GPOs

Configuration Category	Explanation
Software Settings	Centralizes the management of software installation and maintenance; the installation, upgrading, and removal of applications can be controlled from one central location
Windows Settings	Manages the deployment and oversight of scripts, security settings, Internet Explorer settings, and features such as Remote Installation Services and folder redirection
Administrative Templates	Sets registry-based settings to configure application and user desktop settings; this includes access to the operating system components, access to Control Panel settings, and configuration of offline files

Application of Group Policy

- Two main categories to a Group Policy
  - Computer configuration (settings apply to computers in the container)
  - User configuration (settings apply to users in the container)
- Upon computer startup (or user logon)
  - Computer queries domain controller for GPOs.
  - Domain controller finds applicable GPOs.
  - Domain controller presents list of GPOs.
  - The client gets Group Policy templates, applies the settings and runs the scripts.
  - Same basic process happens for user logons

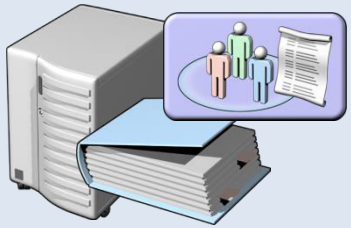
How Group Policies are Applied



Group Policy Components

Group Policy Container

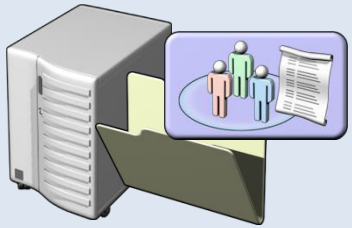
- Stored in Active Directory
- Provides version information



Group Policy Object

- Contains Group Policy settings
- Stores content in two locations

Group Policy Template



- Stored in shared SYSVOL folder
- Provides Group Policy settings
- Supports both ADM and ADMX templates

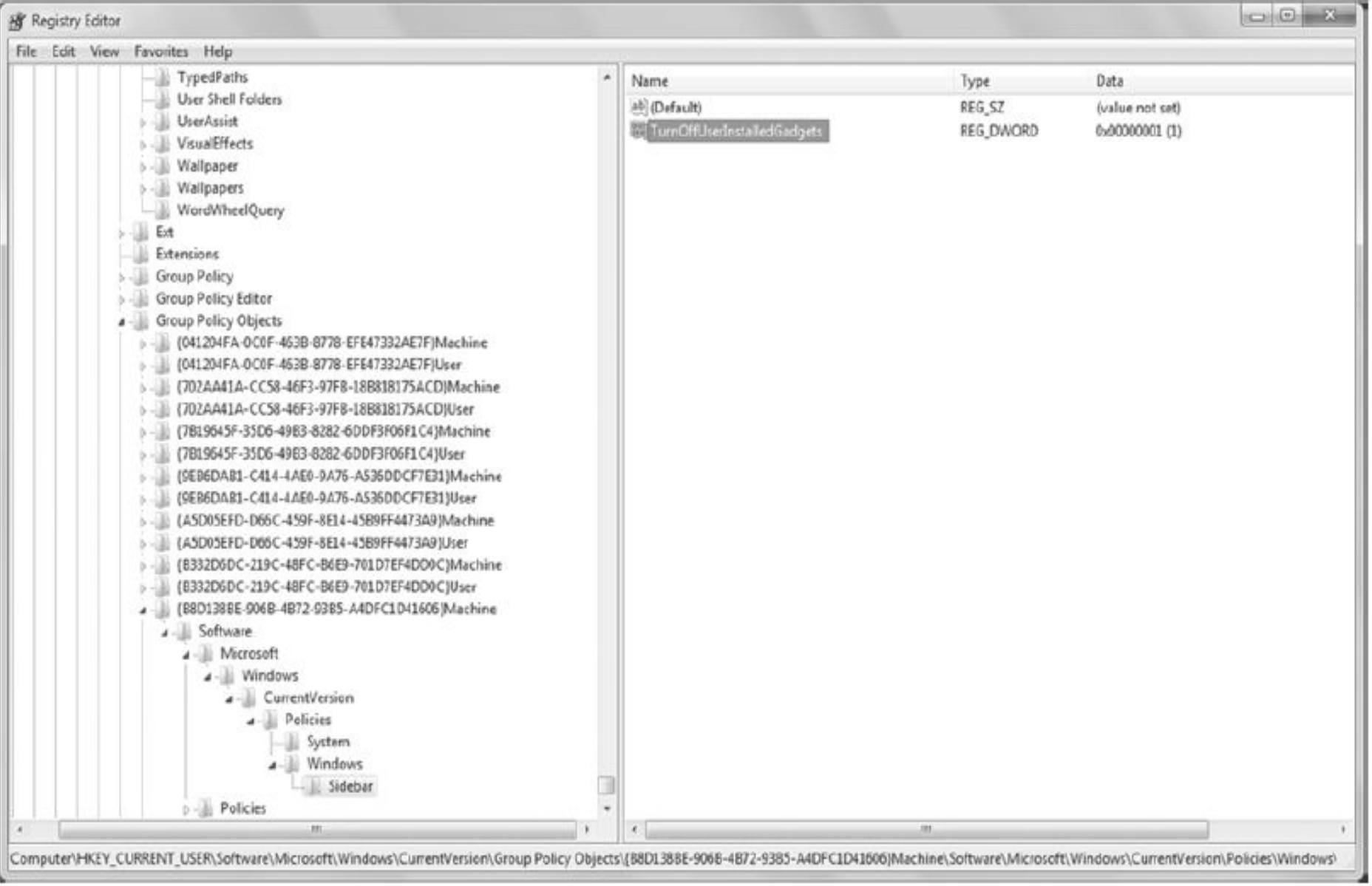


FIGURE 6-5

Group Policy setting in the registry editor.

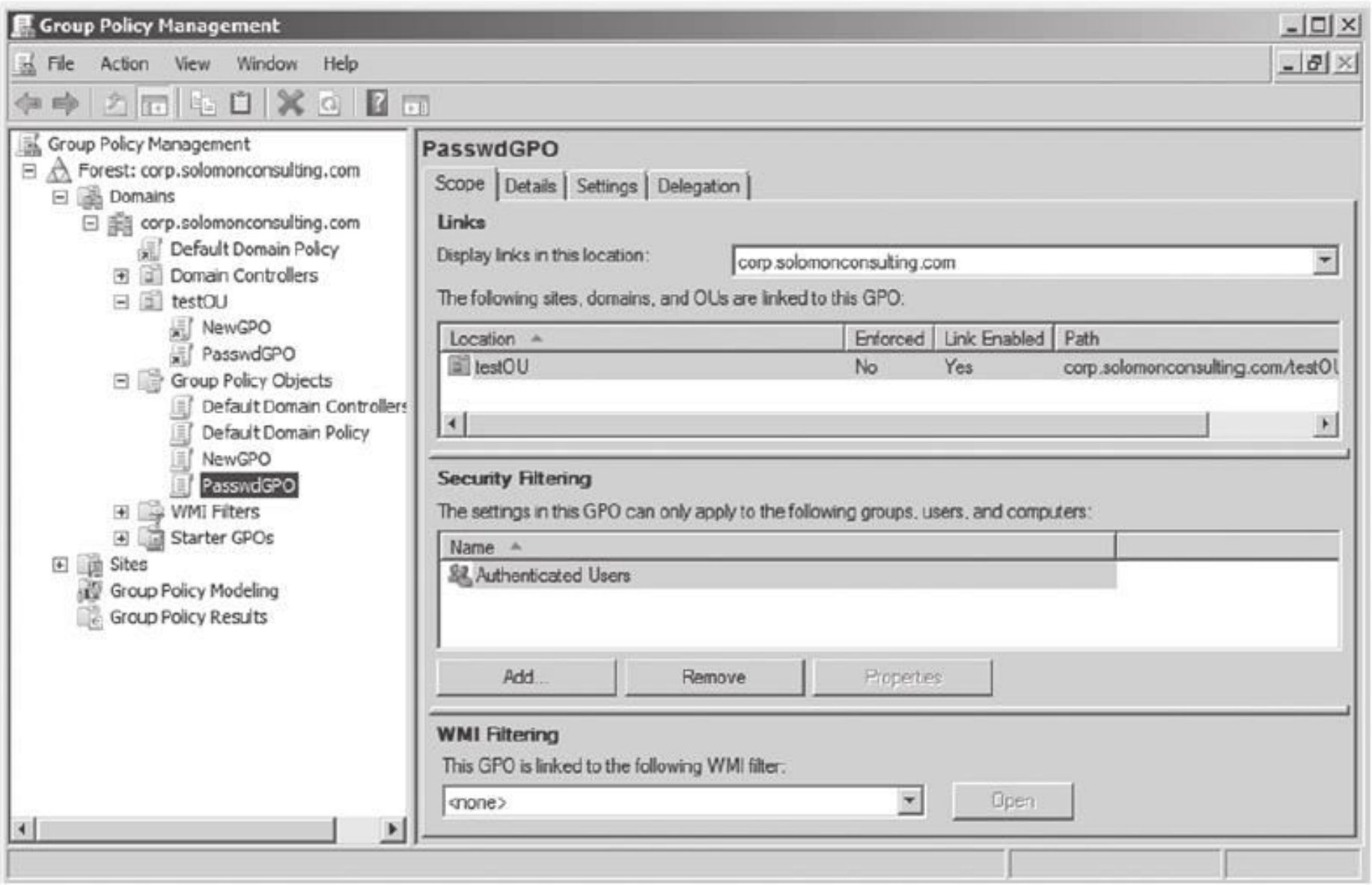


FIGURE 6-6

Group Policy Management Console.

Common Group Policy Object (GPO) Settings

Category	Description
Password Policy	Requirements for password strength, age, history, and how Windows stores passwords
Account Lockout Policy	How Windows handles accounts locked after failed login attempts
Kerberos Policy	Lifetime limits for Kerberos tickets and clock synchronization
Audit Policy	Defines events Windows records in audit files
User Rights Assignment	Individual user rights that define what general actions users can perform, such as “access this computer from the network” or “change the system time”

Common GPO Settings (Continued)

Category	Description
Security Options	Defines what security-related actions users can perform, such as “Allowed to format and eject removable media” or “Require smart card”
Event Log	Defines maximum size, retention settings, and guest access settings for event logs
Restricted Groups	Lists users in security-sensitive groups and to what other groups the restricted group can belong
System Services	Defines startup mode and access permissions for system services
File System	Defines access permissions on discretionary access control lists (DACLs) and audit settings for system access control lists (SACLs)

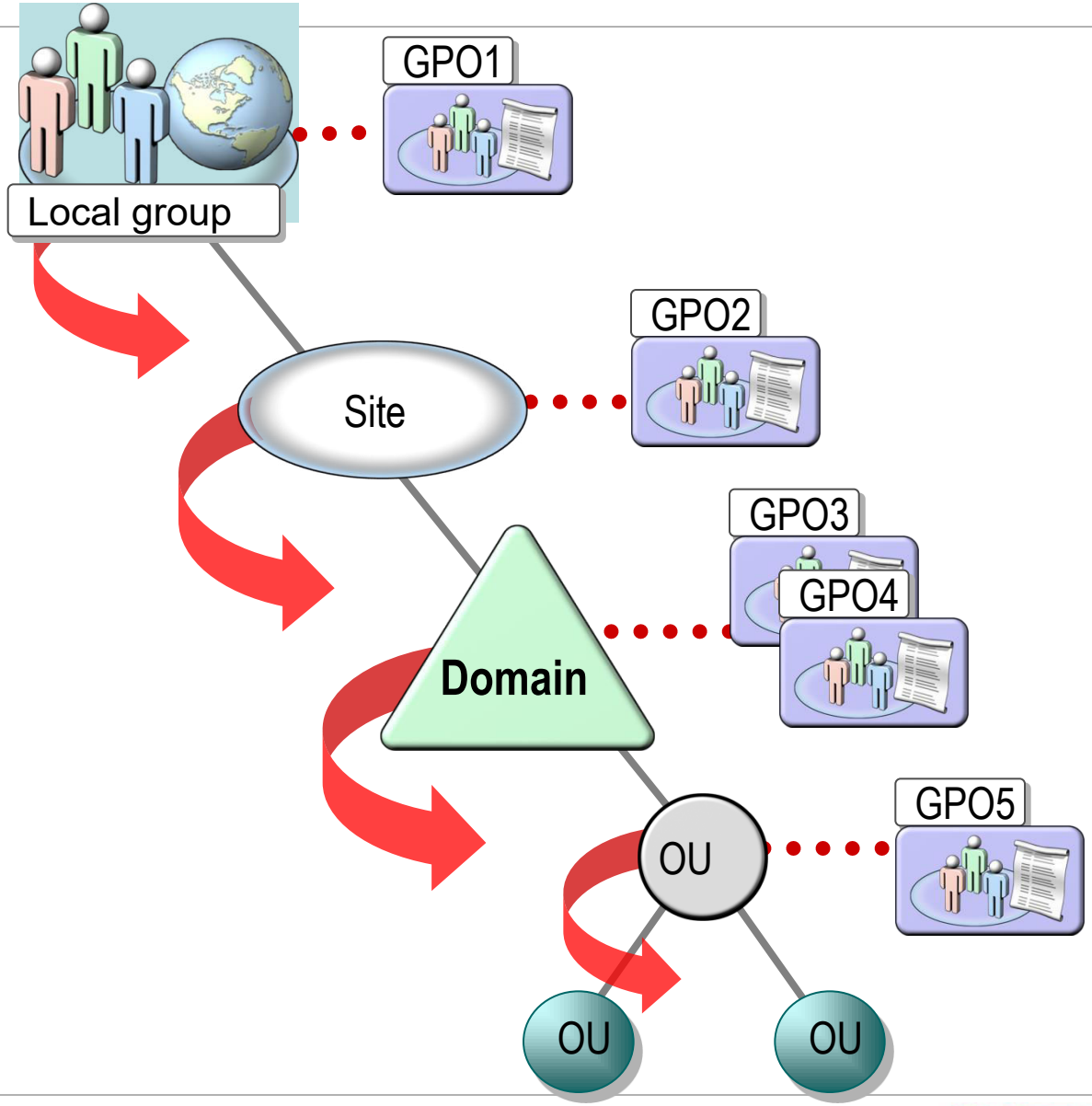
Group Policy Strategies

- Create GPOs for closely-related settings.
- Avoid making GPOs too specific.
- Create organizational units (OUs) for logical groups of computers.
  - Group Policy best practices analyzer
  - Security compliance management toolkit
  - GPO accelerator

Group Policy Strategies

- **Group Policy Best Practices Analyzer –**
  - The Microsoft Group Policy Best Practice Analyzer helps you identify Group Policy configuration errors or dependency issues that may prevent settings from functioning as you expected.
- **Security Compliance Management Toolkit –**
  - Resources "to help you plan, deploy, and monitor the security baselines of servers running Windows Server.
- **GPO Accelerator –**
  - The GPO Accelerator tool helps you automatically deploy the recommendations in the *Security Compliance Management Toolkit*.
  - The security guides in the toolkit recommend Group Policy configurations and Security Template configurations that are enforced via Active Directory Domain Services.

Group Policy Processing Order



Auditing Group Policy

- Two main tools to audit Group Policy
- Resultant Set of Policy (RSOP)
  - Included in Windows
  - Shows what settings apply to a specific user on a specific computer

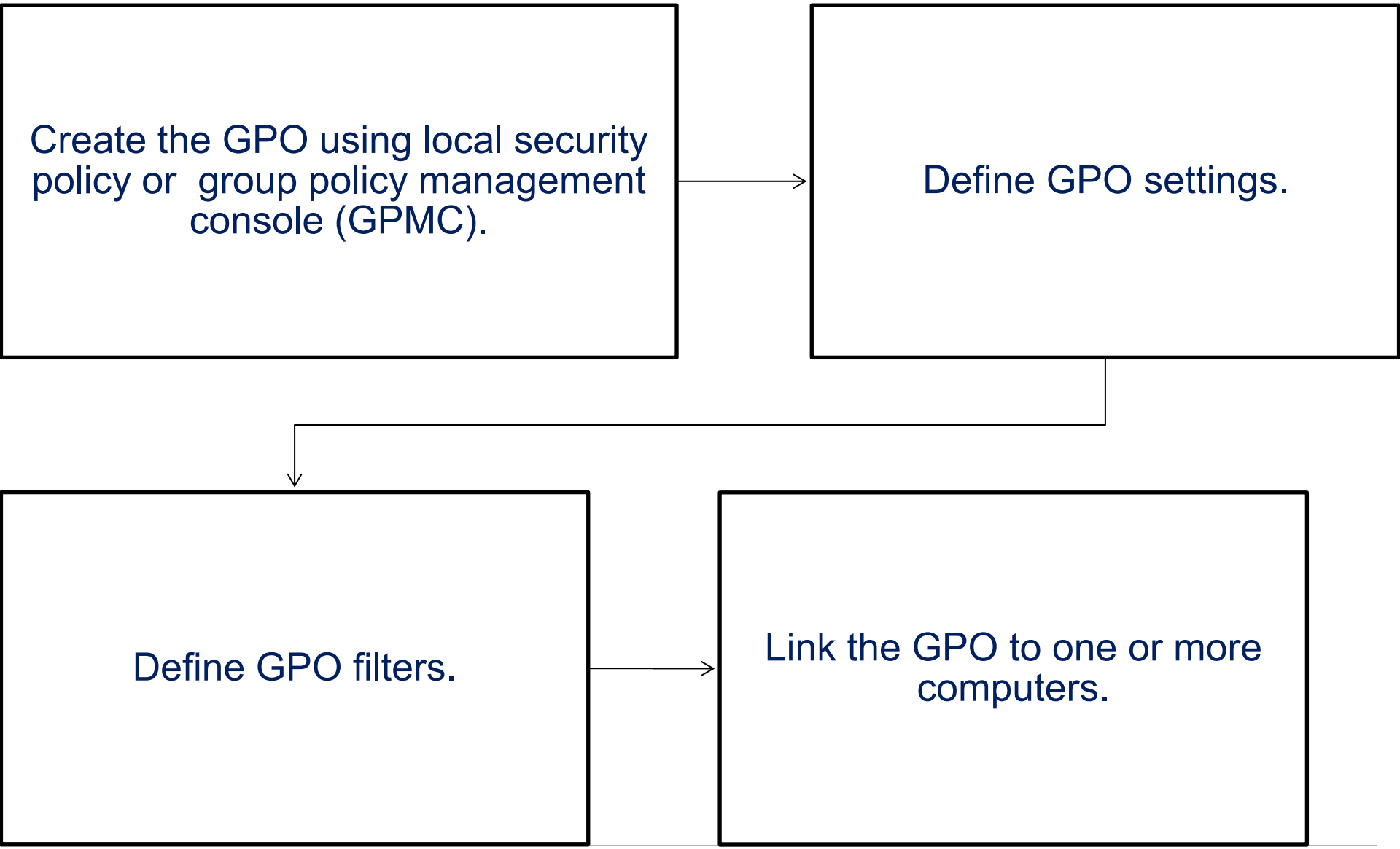
Blocking Group Policy Inheritance

- To change default inheritance, use the Block Policy inheritance check box on the Group Policy tab for a child container
  - Child will not inherit parent's policies
  - Useful if one OU needs to be managed separately

Configuring No Override

- If a policy is configured with No Override
  - It will be enforced despite conflicts in lower-level policies
  - It will be enforced on lower-level containers with Block Policy inheritance set

Steps to Deploying a GPO



Definition of Security Audit

- Helps identify potential vulnerabilities in the system based on audit report
- Auditors compare the effectiveness of security with respect to industry standards

Audit Log

- Types of activities/events to log
  - Logins (successful, failure, all, none)
  - Physical entry (scan card)
  - Changes to system (e.g., permissions)
  - Changes to sensitive data (e.g., salary)
- Automation of logging
- Length of retention for logged data
  - One month for login data
  - One week for physical entry data
  - One month for system change data
  - One year for sensitive data

Windows Logging

- Windows uses the Event Viewer as its primary logging mechanism
  - Found in Administrative Tools
- Event Viewer log files
  - **Security log**
    - Records security-related events
    - Controlled by a system administrator
    - Typical information includes failed logon attempts and attempts to exceed privileges

Windows Logging

- **Application log**
  - Records events triggered by application software
  - System administrators have control over what events to store
- **System log**
  - Contains events recorded by the operating system
  - System administrator generally has no control over this log
  - Typical events include hardware/software problems
- **Other specialized log files:** directory service log, file replication service log, and DNS server log

Windows Logging

- Four types of events are stored in Event Viewer logs
  - **Error events** are created when a serious problem occurs (corruption of a file system)
  - **Warning events** are created to alert administrators to potential problems (a disk nearing capacity)
  - **Information events** are details of some activity that aren't indications of a problem (starting or stopping a service)
  - **Success/failure auditing events** are administrator-defined events that can be logged when they succeed, when they fail, or both (unsuccessful logon attempts)

Detecting Anomalies

- Define anomalies based on thresholds
- The following questions must be answered
  - How much of a deviation from the norm represents an anomaly?
  - How long must the deviation occur before registering an anomaly?
  - What anomalies should trigger immediate alerts?
- Anomalies can occur at any level
  - For example, if a user's behavior deviates from normal, it may indicate a serious security event

Sample Security Audit Questionnaire

1. Are you preventing people from misusing your information processing facilities?
2. Are you protecting your information processing facilities by reducing the risk of human error?
3. Are you protecting information processing facilities by reducing the risk of theft?
4. Are you protecting information processing facilities by reducing the risk of fraud?
5. Are you addressing information security issues during the personnel recruitment process?

Sample Security Audit Questionnaire

1. Are all new users of information processing facilities subjected to a security screening?
2. Are all new users of information processing facilities asked to sign confidentiality agreements?
3. Are users aware of information security threats and concerns?
4. Are users capable of applying your information security policy?
5. Do you teach users how to apply your security procedures?

Auditing Group Policy (Continued)

- **Group Policy Inventory**
  - **You must download from Microsoft**
  - **Provides an inventory list of GPO and other settings**

Security and Vulnerability Analyzer

- Evaluates the current state of a Windows computer
- Compares the state to a known baseline
- Reports any differences as issues
  - Ranks issues based on severity
  - Recommends methods to fix each issue

MBSA Procedure

Download and install MBSA

Run MBSA and select the desired option

- Scan a computer
- Scan multiple computers
- View scan reports

Select desired scan options

Review scan results when done

When to run MBSA

- MBSA is a convenient tool for any organization.
- MBSA is most helpful in following scenarios:
  - After adding new computers
  - To verify compliance
  - To ensure you haven't missed important vulnerabilities

MBSA Benefits

- Visibility of multiple computers' security
- Comparing of multiple computers' security
  - Comparing settings is difficult with stand-alone computers
- Identifying differences from standards
  - Scanning large and small groups of computers becomes easy

First things first, what is an “incident”?

- **An *incident* is an adverse event (or threat of an adverse event) in a computer system**
- **Adverse events include the following general categories:**
  - Compromise of Confidentiality
  - Compromise of Integrity
  - Denial of Resources
  - Intrusions
  - Misuse
  - Damage
  - Hoaxes

Security Incidents

- An incident is any event that:
  - Violates security policy
  - Poses an imminent threat to security policy
- Examples of Incidents
  - Excessive bandwidth use caused by the compromise of a system
  - Commercial use of IT resources
  - Compromised computers
  - Copyright infringement
  - Digital harassment
  - IP spoofing
  - Intruder activity
  - Network attack or denial-of-service condition
  - Virus or Internet worm activity

Incident Handling Methodology

- **“Failing to Plan, is Planning to Fail!”**
- **So how do we do that?**
  - **You have in place, an IR (Incidence Recovery)/IH (Incidence Handling) methodology**
- **Why should we bother using an incident handling methodology?**
  - **Provides structure and organization**
  - **Improves efficiency**
  - **Facilitates understanding the process of responding**
  - **Helps dealing with the unexpected**

Incident Response Lifecycle

- **The incident response lifecycle consists of six stages:**

1. **Prepare**
2. **Detect**
3. **Contain**
4. **Eradicate**
5. **Recover**
6. **Follow-Up**

PANIC is not one of the stages.

Step 1 - Prepare

- Your direction:
  - Develop an incident response policy
  - Create procedures for dealing with incidents as efficiently as possible
  - Ensure that a suitable management infrastructure is in place
  - Implement a reasonable set of defenses for systems that are to be used in responding to incidents

Solving “Now What?!?”:

Your written Incident Response policy

- The anchor of an entire incident response effort
- A suitable incident response policy should address/include
  - Provides scope, purpose and objectives
  - Help define what is a “security-related” incident
  - Acceptable risk limits, eval criteria, reporting reqs, etc.
  - Roles, responsibilities and authority

Remember…

- Good planning will help you mitigate the situation.
- You are not the first person this has ever happened too.
- Panic is worthless and contagious.
- Where are you in your process?

Step 2 - Detect

- **Determine if Incident Occurred:**
  - **Determine what the problem is and to assess its magnitude**
  - **Major sources of information**
    - Log files and syslog output
    - Wrapper tools (e.g., TCP wrapper)
    - Personal firewalls (e.g., BlackIce Defender)
    - Firewall logs
    - Intrusion detection systems (IDS) and prevention systems (IPS)
  - **Analyze all anomalies**

What should I be looking for?

- Are any IP Header fields suspect?
  - Is the Source IP address suspect?
  - Is odd fragmentation occurring?
  - Does the size of the packet raise concerns?
- Are any TCP header fields suspect?
  - Is the destination port a valid service?
- Does the traffic follow RFC standards?
- What are the timestamps of the traffic?

Developing an Audit Policy

- **As with all security policy, proper design of audit policy requires a threat analysis**
  - **Audit mitigates some threats with non-repudiation**
  - **Audit has real costs**
    - Storage (disk)
    - Collection (network)
    - Analysis (machine and human)
- **Sometimes additional audit categories are desirable for correlation**
  - **Process Tracking (except on batch/CGI servers)**
  - **Account Logon**
- **Audit Policy is iterative: Test & Refine**

Some Logon/Logoff Event IDs

- 528 - Successful Logon
- 529 - Logon Failure: Unknown user name or bad password
- 530 - Logon Failure: Account logon time restriction violation
- 531 - Logon Failure: Account currently disabled
- 532 - Logon Failure: The specified user account has expired
- 533 - Logon Failure: User not allowed to logon at this computer
- 534 - Logon Failure: User not granted requested logon type at this machine
- 535 - Logon Failure: The specified account's password has expired
- 539 - Logon Failure: Account locked out
- 540 - Successful Network Logon

Important Event IDs on your Domain Controller

- 675 – Failed logon from workstation, usually a bad password
- 676/672 – Other AutN failure
- 681/680 – Failed logon with a domain account
- 642 – Reset PW or Disabled account was re-enabled
- 632/636/660 – User was added to a group
- 624 – New user account created
- 644 – Account lockout after repeated logon failures
- 517 – User cleared the logs

Success/Failure Policy

- Audit can be a denial-of-service (DoS)!!
  - Success audit requires more attacker access & resources and can be constrained by quota
  - Failure audit can, in the worst case, allow anonymous remote users to consume resources

- Success audit
  - Provides a forensic or accounting record

- Failure audit
  - Provides evidence that security controls are working
  - Can be used for intrusion detection (if scenarios are clearly defined and analyst resources are allocated)
  - Can be difficult to analyze
  - Some failures are normal

Setting Audit Policy

- **When thinking about your policy, consider…**
  - **Audit <u>is</u> good at:**
    - Tampering- changes to system executables & config
    - Change tracking to data files
  - **Audit is ***<u>not</u>* **good at:**
    - Recording reads to files (audit directory instead or audit a single critical file)
    - Explaining events from the user's point of view (one click often causes multiple audits
    - Copy protection (where the file went)
  - **Beware of:**
    - Oddly-behaved applications (winword.exe, explorer.exe)

Step 3 - Contain

- To keep incident from spreading
- Important decisions need to be made during this stage:
  - Do we shut down?
  - Should we disconnect from the network?
  - Continue monitoring?
  - Set a trap?
  - Disable features?
  - Call in the Feds?

Step 4 - Eradicate

- To eliminate cause of incident
- Be sure to save any copies of malicious programs before deleting them
- May require the use of eradication software
- Clean/reformat disks (if appropriate)
- Ensure that backups are clean
- Continue to document all activities
- Continue to keep your public relations and legal offices advised (if warranted)

Step 5 - Recover

- **Business Resumption:**
  - **Return to mission status**
  - **Follow procedures for system recovery**
  - **Send the “All Clear" message**
  - **Restore data**
  - **Change passwords**
  - **Continue to log all activities**
  - **For classified/sensitive/proprietary systems, require verification of data integrity**

Step 6 – Follow Up

- Make things better:
  - Review and integrate info
  - Most neglected stage of the process, and the most valuable.
  - Conduct Postmortem
  - Reevaluate procedures
  - Assess time and resources used, and financial damage
  - Prepare report(s)
  - Support prosecution activity (if applicable)

Technical Considerations

- **React Accordingly!!!**
  - **Some incidents occur on large servers with special complications**
    - They cannot be taken off-line, OR
    - They have so much storage that it cannot be successfully imaged (or have RAID, so an image will be technically infeasible)
  - **The best option is still to perform some sort of backup, at least of the suspicious files and logs, then analyze them off-line**
  - **A backup will not include all the information such as slack space data, but it may be the only alternative**

Legal Considerations

- Incident Response has legal implication
- Documentation is a legal foundation. Do it thoroughly!
- Keep good records
- Know when to contact law enforcement

Some Best Practices for Incident Handling

- Verify the incident, ruling out alternative explanations of what has happened
- Follow written procedures during incidents
- Ensure that you have backups very early during the course of an incident
- Coordinate and consult with other technical experts
- Keep management advised of status of incident and your efforts
- Log all activities

Why form an incident response team?

- Incidents are complex- experts are needed
- Efficiency
- Proactive element
- Agency or corporate requirements
- Liaison function
- Authority to engage in activities that a normal organization doesn't get

Considerations for your Incident Response Team

- **Executive Sponsorship**
  - **Without it, your team will die.**
  - **Keep the sponsor aware of the situation**

- **Identify the Key Stakeholders**
  - **Not just the “IT guys”**
  - **Key reps from all the LOB owners**

- **Choosing a Team Leader**
  - **Owns the CSIRT, not necessarily each incident response**
  - **Conducts team “post-mortems” to make policy update changes**

Train your “A-Team”,

- **Mock Incident Response Exercises:**
  - **Allows validation of your procedures**
  - **“Practice makes perfect”**
  - **You can gauge the size and complexity of the process**
  - **Benefits increased if external objective observer helps identify issues**
- **Mock Incident Handling Exercises:**
  - **Develop a variety of scenarios**
  - **Record critical data and evaluate**
  - **Conduct at regular intervals**
  - **Warning--Carefully plan any mock incident handling exercises to avoid disruption of operational environments**

Resources to Help

- Security Response Center
- Security Advisories & Bulletins