Module 6 - Honors SIM

Web Application, Windows, and Linux security

Basic security audit policies

The event categories that you can choose to audit are:

Audit account logon events

Audit account management

Audit directory service access

Audit logon events

Audit object access

Audit policy change

Audit privilege use

Audit process tracking

Audit system events

Windows Audit Policy

The Windows Audit Policy defines the specific events you want to log, and what particular behaviors are logged for each of these events.

For example, your audit policy may determine that you want to log any remote access to a Windows machine, but that you do not need to audit login attempts from someone on your business premises.


Planning
Risk Assessment
Audit Cycle
Reporting
Fieldwork

Types of Windows Events that Can be Audited

Logon and logoff events: Attempts to access and login to a particular device, whether those attempts are successful or not.

Account management: Changes to user profiles and accounts on Windows machines.

Active Directory: Changes to Active Directory configurations or user profiles.

Server access and logins: Client-server access from a remote machine to a Windows server.

Object access: When Windows machines access specific devices or objects on the network including files, folders, or printers.

Registry access: Changes to a Windows machine's registry. Registry keys are normally updated when applications are installed, changed, or removed.

Policy changes: Amendments to access rights or other IT policies.

Systems events: Starting up and shutting down machines and other system status updates.

Windows Audit Policy Best Practices

1. Use the Advanced Audit Policy Configuration where possible

It’s important to note that the advanced policies do not override the basic policies, but rather complement them. That said, it is not a good idea to use both the basic audit policy settings and the advanced audit policy settings simultaneously, as this can cause conflicts. Configuring audit policies with the Advanced Audit Policy Configuration provides more control and prevents overwhelming log volumes.

2. Determine what types of events you want to audit

3. Specify the max size of the audit log

You should specify the maximum size and other attributes of the Security log using the Event Logging policy settings. This is important because the amount of storage space allocated to storing the audit data can quickly fill up.

Windows Audit Policy Best Practices

4. Conduct performance tests

It is important to keep in mind that changing audit settings can impact computer performance. Therefore, it is advisable to carry out performance tests before implementing new audit settings in a production environment. If you wish to audit directory service access or object access, you can configure the Audit directory service access and Audit object access policy settings.

5.Opt Important Windows Auditing Settings

Account Logon: Audit Credential Validation for success and failure

Account Management: Audit Computer Account Management, Audit Other Account Management Events, Audit Security Group Management, and Audit User Account Management for success and failure

DS Access (Directory Service Access): Audit Directory Service Access and Audit Directory Service Changes for success and failure on domain controllers (DCs)

Logon/Logoff: Audit Account Lockout, Audit Logoff, Audit Logon, and Audit Special Logon for success and failure

Object Access: Enable these settings selectively to avoid generating a large volume of entries in Security logs

Policy Change: Audit Audit Policy Change and Audit Authentication Policy Change for success and failure

Privilege Use: Enable these settings selectively to avoid generating a large volume of entries in Security logs

Process Tracking: Audit Process Creation, but enable selectively due to potential high volume of entries in Security logs

System: Audit Security State Change, Audit Other System Events, and Audit System Integrity for success and failure.

What is server security?

Server security focuses on the protection of data and resources held on the servers. It comprises tools and techniques that help prevent intrusions, hacking and other malicious actions. Server security measures vary and are typically implemented in layers.

What are the functions of server security?

Server security includes a combination of technical and administrative measures, such as using cybersecurity software, complex passwords, disabling unnecessary services and ports, and optimizing user privileges on a need-to-access basis.

What is Active Directory Group Policy?

- AD Group Policies are critical pieces of instructions in an AD environment that an IT administrator can configure. AD group policies will determine the behavior and privileges for users and computers.
- Group Policies are primarily a security solution for the AD network. Administrators can configure these settings and then implement sets of these settings on sites, domains, or OUs containing users and computers.
- Group Policy is used to regulate user and computer configurations within Windows Active Directory (AD) domains. It is a policy-based approach that can be applied to the whole organization or selectively applied to certain departments or groups in organizations.

What are the benefits of Active Directory Group Policies?

Uniform user experience

Users are no longer confined to a single computer in their workplace. They use different computers for different tasks. So, all their files and folders along with their personalized settings such as taskbar location, wallpaper settings, desktop icons, and more have to be made available in all the machines the user logs on to.

Security

Even with all the authentication protocols and authorization techniques involved in AD, a malicious user can still gain access to network resources if he/she gets to know a user's password. So, it is extremely important to have a strong password set for all the users in an organization. It is also important to record certain events like user log in, access to a particular folder, and more for auditing purposes.

Organization-wide Policies

Most organizations use wallpapers, screen savers, interactive logon messages, and more in an effort to establish a standard among all their employees. Organizations also have Internet policies that all users in the organization should adhere to.

Cost and Time

Tasks like software installation consume a lot of time. Installing and updating software on all computers, for all users, will not only take time but also affect productivity, as employees will not have access to their computers when the installation is taking place.

Group Policies play a crucial role in ensuring that the employees of an organization can have a hassle-free experience when it comes to using the IT resources to accomplish their tasks.

Types of Group Policies in AD

There are two types of Group Policies in AD, which are:

- Local Group Policy
- Non-local Group Policy

Local Group Policy

Each computer running the windows line of the operating system has exactly one local group policy. It is available only to the particular computer in which it resides and the users who log on to that computer. The local group policy objects reside in the **%systemroot%\System32\Group Policy folder.** The local Group Policy settings only contain a subset of the entire settings available in the centralized Group Policy settings.

Centralized Group Policy

Each domain controller has one or more centralized group policies. They are available to all the machines and users in the AD environment. A centralized Group Policy can be applied to all users and computers in a domain, or to a particular OU depending on where the Group Policy is linked.

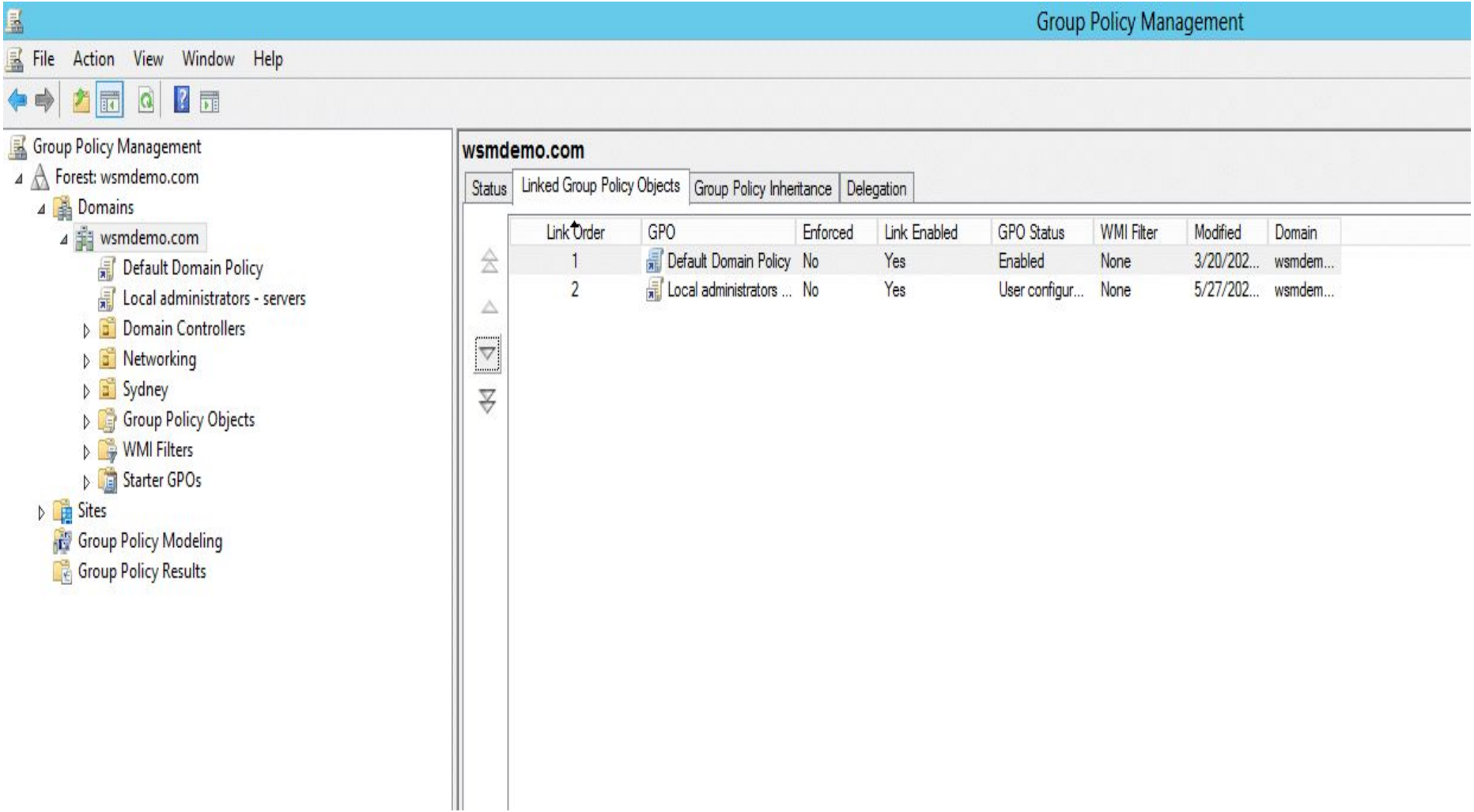
How to manage Group Policies in AD

AD Group Policies are managed using the Group Policy Management Console (GPMC). This is a snap-in that comes built-in since Windows Server 2008. The GPMC allows you to create GPOs, and link them to domains, sites, or OUs as necessary. For example, if you want to link a GPO to an OU or a domain, here's how you can do it:

Go to Start, and navigate to Administrative tools. Then, navigate to Group Policy Management and click on it.

Click on a domain or an OU that you want to view.

In the tabs available on the right side of the console, click on Linked Group Policy Objects tab.


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: wsmdemo.com
Domains
wsmdemo.com
Default Domain Policy
Local administrators - servers
Domain Controllers
Networking
Sydney
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
wsmdemo.com
Status
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Link Order
GPO
Enforced
Link Enabled
GPO Status
WMI Filter
Modified
Domain
1
Default Domain Policy
No
Yes
Enabled
None
3/20/202...
wsmdem...
2
Local administrators ...
No
Yes
User configur...
None
5/27/202...
wsmdem...

Anti-Virus,Mails, Malware

What is malware?

Malware, short for malicious software, refers to any intrusive software developed by cybercriminals (often called hackers) to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware.

What is computer virus?

A computer virus is a type of malicious software, or malware, that spreads between computers and causes damage to data and software.

What is antivirus in computer?

Antivirus is a kind of software used to prevent, scan, detect and delete viruses from a computer. Once installed, most antivirus software runs automatically in the background to provide real-time protection against virus attacks

Endpoint protection, Shadow Passwords, SUDO users

Endpoint protection involves monitoring and protecting endpoints against cyber threats. Protected endpoints include desktops, laptops, smartphones, tablet computers, and other devices.

What is endpoint protection vs antivirus?

Antivirus – will monitor the device in which it is installed to find viruses or malware. It will do so at a certain time, as scheduled.

Endpoint security – will scan all the devices from a network for threats, anomalies, and suspicious behavior

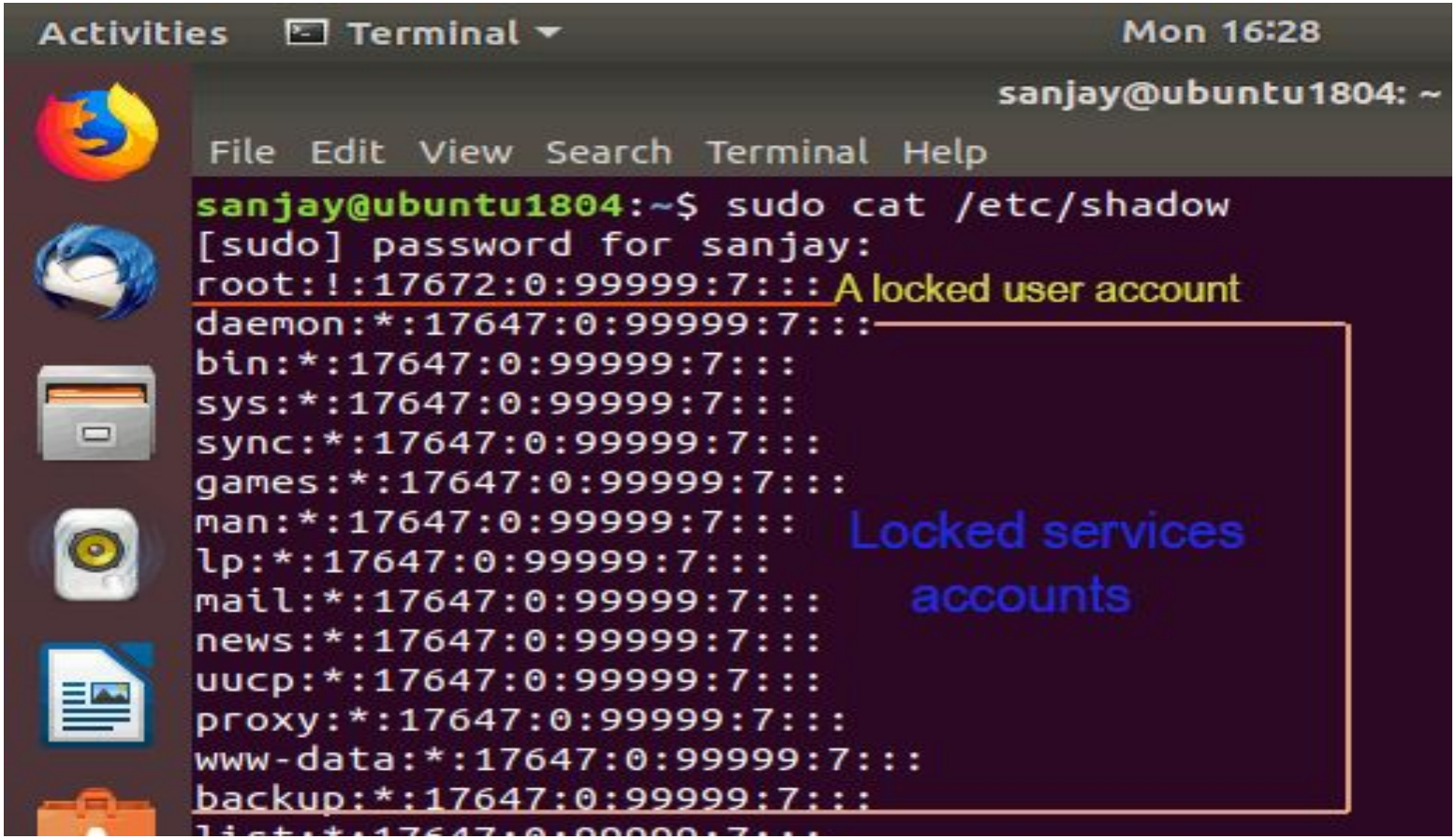
Features of Endpoint Security

uniserve
IT SOLUTIONS

Shadow Passwords

A shadow password file, also known as /etc/shadow, is a system file in Linux that stores encrypted user passwords and is accessible only to the root user, preventing unauthorized users or malicious actors from breaking into the system.

Improves system security by moving encrypted password hashes from the world-readable /etc/passwd file to /etc/shadow , which is readable only by the root user.


Activities
Terminal
Mon 16:28
sanjay@ubuntu1804: ~
File Edit View Search Terminal Help
sanjay@ubuntu1804:~$ sudo cat /etc/shadow
[sudo] password for sanjay:
root:!:17672:0:99999:7:::
A locked user account
daemon:*:17647:0:99999:7:::
bin:*:17647:0:99999:7:::
sys:*:17647:0:99999:7:::
sync:*:17647:0:99999:7:::
games:*:17647:0:99999:7:::
man:*:17647:0:99999:7:::
lp:*:17647:0:99999:7:::
mail:*:17647:0:99999:7:::
news:*:17647:0:99999:7:::
uucp:*:17647:0:99999:7:::
proxy:*:17647:0:99999:7:::
www-data:*:17647:0:99999:7:::
backup:*:17647:0:99999:7:::
Locked services accounts

SUDO users

sudo users are regular users who have been granted special privileges to perform administrative tasks. They can use the "sudo" command to temporarily elevate their privileges and execute commands as a superuser (root) without logging in as the root user.

Sudo is a command in Linux that allows users to run commands with privileges that only root user have. It helps users to do tasks with administrative power without logging in as the root user, though sometimes it can be risky.

Steps to create a new sudo user on Ubuntu

First add the user, run: sudo adduser <UserNameHere>

Add the user to sudo group by typing the command in terminal for Ubuntu version 12.04 and above: sudo adduser <UserNameHere> sudo

In an older version of Ubuntu (version 12.04 and older), run:

sudo adduser <UserNameHere> admin

Verify it: id <UserNameHere>


Thank
you!