UNIT 4 NETWORK MANAGEMENT AND SECURITY

Structure **Page Nos.**

4.0 INTRODUCTION

Network management includes the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network Operation deals with keeping the network up and running smoothly. It includes monitoring the network to diagnose and identify problems as soon as possible, ideally before users are get affected. Network administration deals with keeping track of resources or components in the network and how these resources are assigned and do necessary steps to keep the network under control. Network maintenance is concerned with performing repairs and upgrades. For example, when the equipment must be replaced, when a router needs a patch for an operating system image and when a new switch is added to a network and so on. Maintenance also involves corrective and preventive measures to make the managed network run "better", such as adjusting device configuration parameters. Network provisioning is concerned with configuring resources or components in the network to support a given service. For example, this might include setting up the network so that a new customer can receive voice service.

A common way of characterizing network management functions is FCAPS- Fault, Configuration, Accounting, Performance and Security. Functions that are performed as part of network management include controlling, planning, allocating, deploying, coordinating, and monitoring the resources of a network. Network planning, frequency allocation, predetermined traffic routing to support load balancing, cryptographic key distribution authorization, configuration management, fault management, security management, performance management, bandwidth management, route analytics and accounting management are some of the key managerial activities that are to be performed for effective network management and ensure security. A network management system (NMS) is combination of hardware and software used to monitor and administer a computer network or networks.

Data for network management is collected through several mechanisms, including agents installed on network infrastructure, synthetic monitoring that simulates transactions, logs of activity, sniffers and real user monitoring. In the past, network management mainly consists of monitoring whether devices in the network were up or down, but today performance management has become a crucial part of the IT team's role.

As usage of Systems/Applications/ Services through network is increasing day by day, at same time Hackers/Attackers are playing a vital role to destruct the system resources and deface the Websites , etc. Security is essential to protect the resources of systems, services and applications from Hackers or Attackers and in turn protect the sensitive information and data.

Security management is an activity that includes a set of functions that are to be performed to protect telecommunications networks and systems from unauthorized access by persons, acts, or influences. Security functions are for creating, deleting, and controlling security services and mechanisms; distributing security-relevant information; reporting security-relevant events; controlling the distribution of cryptographic keying material; and authorizing subscriber access, rights, and privileges.

4.1 OBJECTIVES

After going through this unit, you will be able to:

- understand the network management and security;
- know how user management can be done in a security perspective;
- understand disk management in a security perspective;
- find account policies and specially password policy;
- find various user permissions and restrictions; and
- understand troubleshooting of network and available tools.

4.2 NETWORKS AND SECURITY

A computer network is a telecommunications network that allows computers to exchange data. The physical connection between networked computing devices is established using either cable media or wireless media. The best-known computer network is the Internet.

Network devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as servers and personal computers, as well as networking hardware. Computer networks support applications such as access to the World Wide Web, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications.

Networks established either through wired or wireless technologies. Wired networks can be established by using twisted pair, coaxial cable and optical fiber. Wireless networks can be established by using terrestrial microwave communications, communication satellites, cellular and PCS systems, radio and spectrum technologies. All these technologies use different network components that are to be used for routing, switching the data traffic for successful transmission. Some of the routing and switching devices involved in any communication network are the routers, switches, bridges, repeaters, hubs, etc. As many network devices will participate during data transmission from source to destination, ensuring secure communication is a challenging task.

Why do we need Security?

Security is the degree of resistance to, or protection from, harm. It applies to any vulnerable and valuable asset, such as Information Technology infrastructure, a computer network, a person, dwelling, community, nation, or organization. Due to rapid developments in internet technologies, usage of network services for ecommerce applications, banking, education and many such areas are increasing day by day and at same time hackers are also playing a vital role to destruct services and data. Security is essential to protect the network resources and in turn ensure secure data transmission.

Security services

The following are various security services or parameters to enhance the security of a systems, applications, data and are intended to counter security attacks.

- Authentication
- Authorization & Access Control
- Availability
- Confidentiality
- Integrity
- Nonrepudiation

Authentication is the act of establishing or confirming something (or someone) as authentic. It confirms the identity of a person or a system and permits one system to determine the origin of another system. It is essential in online community, where two systems are usually not directly connected

Authorization and Access Control is the level of access control that is permitted to use systems and services

Availability ensures that the system or an Application or a Service is always available to the authorized parties when needed

Confidentiality provides the secrecy of information and allows only authorized users to have access to information.

Integrity ensures that only authorized parties are able to modify computer system assets and transmitted information and provides the correctness of information.

Nonrepudiation ensures that neither the sender nor receiver of a message be able deny the transmission. It is a kind of system that includes authentication, integrity and non-repudiation should be able to detect tampered information and prevent valid information from being falsely rejected.

Deviation in any of the above security services is a breach in security.

4.3 USER SECURITY MANAGEMENT

User Management is an authentication feature that provides administrators with the ability to create users on a system or a service identify and control the state of users logged into the system and even network. User management includes the ability to query and filter users those are currently logged into the system or network, manually log out users, and control user login counts and login times.

Why do you need User Management?

Most security-conscious enterprises today implement some form of authentication and authorization for accessing network resources. In this process, user permissions can be verified before granting access to resources, and user activity can be monitored through various logging mechanisms. In typical authentication and authorization deployments, administrators have various options available with regard to how users are authenticated, but have little control over how often users are authenticated. User Management enables administrators to control the frequency of user authentication, to ignore cached browser credentials and force the user to re-enter credentials, or to require more frequent authentication only if the user is accessing critical resources. This kind of flexibility allows administrators to implement authentication-based policies that more closely match their network security policies.

The User Management logout capability also provides more secure control over the state of users. For example, when using IP authentication mode, users are identified by the specified IP address until the IP surrogate time expires. If another person were to use that computer before the IP surrogate time expired, they would be treated as the original user. The common solution for preventing this scenario is to decrease the IP surrogate expiry time, causing the user to be challenged more often. Another key benefit of User Management is visibility into active user sessions. Using the Management Console and CLI, administrators can view all active users and filter display data by user, IP address, or realm for easier viewing. This can be useful for identifying the general login status of users or for making real-time decisions such as immediately logging off a user.

How does User Management work?

User Management is based on the concept of users logging in and logging out of a system or a network. A login is the combination of a unique IP address with a unique username in a unique domain. A user is considered logged in when first authenticated to the system or a network. Identifying users as logged in, or active, allows administrators to create flexible User

Management policies to fine tune user access and control.

The majority of User Management is done by framing and introducing a policy. Using policy, administrators can create, delete, modify users and also enforce controls on logging ins, logouts, number of login attempts and other such related.

The following are some of the policies implemented as part of user management in a security perspective:

- Create genuine user-names on a system or network or a service.
- Frequently monitor unauthorized users, if any created, logged in or connected.
- Introduce timestamps on logins and logouts of users and monitor in case of odd timings, if any activities performed.
- Keep tracking on users , who login in long time.
- Clearly add expiry date of a user at the time of user creation itself.
- Enforce policy to deactivate automatically after expiry.
- Introduce multi-level authentication such as authentication with username and password; username, password and IP address; username, password, MAC-address, etc.
- Limit the number of IP addresses associated with a single username.
- Limit the number of logins associated with a single IP address.
- Force a re-authentication to gain access to a particular network resource.
- Limit the login session time allowed in a particular timeframe.

4.4 DISK SECURITY MANAGEMENT

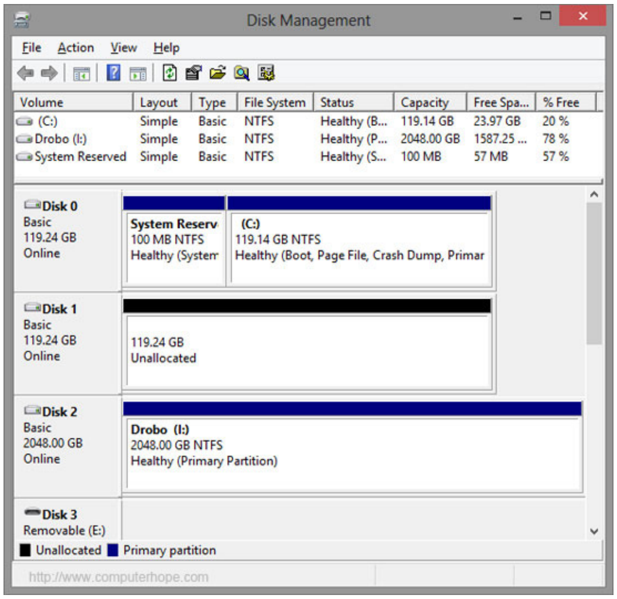
Disk Management is an activity to manage the drives installed in a computer like hard disk drives (internal and external), optical disk drives, and flash drives. Disk Management activities are like partition drives, format drives, assign drive letters, and other such related. For disk management can be done either with help of a tool or with a command to manage system disks, both local and remote.

The following are some of Disk Management functions:

- Create partitions, logical drives, and volumes.
- Delete partitions, logical drives, and volumes.
- Format partitions and volumes.
- Mark partitions as active.
- Assign or modify drive letters for hard disk volumes, removable disk drives, and CD-ROM drives.
- Obtain a quick visual overview of the properties of all disks and volumes in the system.
- Create mounted drives on systems using the NTFS file system.
- Convert basic disks to dynamic disks.
- Convert dynamic to basic disks, although this is a destructive operation.
- On dynamic disks, create a number of specialty volumes including spanned, striped, mirrored, and RAID-5 volumes.

Disk Management

Microsoft Windows utility that was introduced with Windows XP as a replacement to the fdisk command that enables users to view and manage the disk drives installed in their computer and the partitions associated with those drives. Figure 1 shows the snapshot of disk management utility in windows XP. Each drive is displayed followed by the layout, type, file system, status, capacity, free space, % free space, fault tolerance and overhead.



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (B...	119.14 GB	23.97 GB	20 %
Drobo (I:)	Simple	Basic	NTFS	Healthy (P...	2048.00 GB	1587.25 ...	78 %
System Reserved	Simple	Basic	NTFS	Healthy (S...	100 MB	57 MB	57 %

Disk 0
Basic
119.24 GB
Online

System Reserv
100 MB NTFS
Healthy (System

(C:)
119.14 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primar

Disk 1
Basic
119.24 GB
Online

119.24 GB
Unallocated

Disk 2
Basic
2048.00 GB
Online

Drobo (I:)
2048.00 GB NTFS
Healthy (Primary Partition)

Disk 3
Removable (E:)

■ Unallocated ■ Primary partition

Figure 1: Disk Management in Windows XP

The following is the procedure to open Windows Disk Management

- Click Start, Settings, Control Panel.
- Double-click on Administrative Tools if in Classic View or click Performance and Maintenance and then Administrative Tools if in Category View. Note: If you do not have admin rights to the computer this will not be available.
- Once in the Administrative Tools window double-click Computer Management and then click Disk Management under the Storage section.

Similarly, disk management utilities are available in Linux environment (fdisk command) too to perform various activities as being done in Windows environment.

Disk Management in a security perspective

The following are to be followed for secure disk management:

- Create adequate number of disk partitions
- Allocate adequate storage space in each disk partition as per requirement
- Ensure minimum free space al the times
- Set password for each disk partition or a disk drive
- Scan each disk partition or a disk drive at regular intervals for viruses or worms, etc
- Enforce standard anti-virus software to check and clean viruses in a file before storing into a particular disk partition.
- Update Anti-virus software, periodically
- Disk partitions or disk drives should not be in sharing mode (put in sharing mode only on demand)
- Introduce RAID concept
- Disable disk remote access.
- Apply data encryption at disk storage level too apart from during data transmission
- Implement dish quotas by enforcing upper limits and warning alerts in case reaches to upper limit
- Disk defragmentation to be done, periodically
- Allow disk indexing service

Check Your Progress 1

1. What are various security services or parameters?

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

2. List the Disk Management functions.

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

4.5 SECURITY CONFIGURATION AND ANALYSIS

Configuring networked systems and components with adequate security controls in any organization to run or access through network is a critical task. Once, installations, configurations are done, it is very essential to look at the configurations and analyze the setting by keeping security issues in mind before deployment or immediately after deployment.

Security Configuration and Analysis can be done either manually with a check list or with help of a tool that can be used to analyze and configure computer security. Generally, users can use the tool to import one or more saved configurations to a private security database. Importing configurations builds a machine-specific security database that stores a composite configuration. One can apply this composite configuration to the computer and analyze the current system configurations against the stored composite configuration stored in the database.

Best practices for Security Configuration and Analysis

The following are the best security practices to be followed to ensure security in any networked system domain of an organization:

Restrict physical access to computers, especially domain controllers to trusted personnel

> Physical access to a server is a high security risk. Physical access to a server by an intruder could result in unauthorized data access or modification as well as installation of hardware or software designed to circumvent security. To maintain a secure environment, you must restrict physical access to all servers and network hardware.

For administrative tasks, use the principle of least privilege

> Using the principle of least privilege, Administrators should use an account with restrictive permissions to perform routine, non-administrative tasks and use an account with broader permissions only when performing specific administrative tasks.

Define groups and their membership

> At the time of creation of users, the administrator has to define the user under a specific group depending on type of resources or applications where the user needs access.

Secure data on computers

Ensure that the system files and the registry are protected using strong access control lists.

Use strong passwords throughout your organization

Authentication methods require the user to provide a password to prove their identity. These passwords are normally chosen by the user, who may want a simple password that is easily remembered. In most cases, these passwords are weak and may be easily guessed or determined by an intruder. Strong passwords tend to be more difficult for an intruder to detect. Using strong passwords always help to provide an effective defense of resources.

Do not download or run programs that come from untrusted sources

Programs can contain instructions to violate security in a number of ways including data theft, denial of service and data destruction. These malicious programs often masquerade as legitimate software and can be difficult to identify. To avoid these programs, one should only download and run software that is guaranteed authentic and obtained from a trusted source. It is always better to ensure a current virus scanner is installed and functioning in case this type of software does inadvertently wind up on your computer.

Keep virus scanners up to date

Virus scanners frequently identify infected files by scanning for a signature, which is a known component of a previously identified virus. The scanners keep these virus signatures in a signature file, which is usually stored on the local hard disk. Because new viruses are discovered frequently, this file should also be updated frequently for the virus scanner to easily identify all current viruses.

Keep all software patches up to date

Software patches provide solutions to known security issues. Check software provider Web sites periodically to see if there are new patches available for software used in your organization.

Use some available security configuration and analysis tools (for example: secedit.exe is a Windows security configuration editor command tool) to configure, verify and analyze the network settings. This kind of tools can be used for the following:

- For frequent analysis of a large number of computers, as with a domain-based infrastructure,

- To configure security areas not affected by Group Policy settings. It includes the areas such as security on local files and folders, registry keys, and system services. Otherwise, Group Policy settings will override the local settings.

- Do not use such tools, when you are configuring security for a domain or an organizational unit.

4.6 ACCOUNT POLICIES

User accounts or simply login IDs are required to access any system's or network resources, if resources access configured in such a way that they are entry controlled. The system or network administrator has to create usernames on systems depending on need and deed. The administrator has to have a policy on user administration in terms of user account creation, deletion, modification, expire and also have a password policy in terms of password length, complexity, minimum and maximum password aging, etc.

A user account policy is a document which outlines the requirements for requesting and maintaining an account on computer systems or networks, typically within an organization. It is very important for large sites where users typically have accounts on many systems. Some sites have users read and sign an account policy as part of the account request process.

Introduction to user and Group in Linux

Unix/Linux is a multi user and multi tasking Operating system. Redhat Linux uses User Private Group (UPG) scheme where user always get created with primary group. There is only one primary group per user.

When a user is created in Linux, the following are created

Home directory (home/username)

Mail account (/var/spool/mail/username)

Unique UID & GID

Types of Accounts

Generally, accounts fall into two types such as System accounts(system users) and Normal accounts (normal users). When an user account is created in Linux, the details are stored in the following files:

/etc/passwd
/etc/shadow
/etc/group

where

/etc/passwd contains database of all users created.

Example entry in a /etc/passwd file

```
u1:x:500:550:prog:/home/u1:/bin/bash
```

Where
u1 is User ID
X is mask password
500 is UID (user ID)
550 is GID (group ID)
prog is user ID comment field (generally it could be name of user)
/home/u1 is home directory of user ID and

/bin/bash is a shell

The /etc/shadow file contains the encrypted user passwords assigned by the password binary file. Password's are encrypted through DES (Data Encryption Standard) or MD5 (Message Digest Ver.5) Algorithm.

The/etc/group file contains Group name and GID of the group.

Managing Users

A system administration can manage a user's account. The various tasks that a system administrator can perform include adding, modifying and deleting user account.

User account Creation

To create a user, use the useradd command. The syntax is

root# useradd <option> <userID>

-u is UID

-g is primary/group name/GID

-o is : Override

-G is Secondary group

-c is Comment

-d is Home directory

-s: is Shell

Example:

root# useradd murli , it creates user ID murli and assign some default values against UID, GID, and other

user ID can also create by using all options along with the command useradd as specified above.

User ID Modification

To modify a user, use the usermod command. The syntax is:

root# usermod <options> <userID>
The options to usermod command are:
-l is Change user account
-L is to Lock the account
-U is to Unlock the account

Example

Root# usermod murli

User Deletion

To delete a user, use the userdel command. The syntax is

root# userdel <options> <userID>

The option to userdel command is
-r is recursively delete

Example

root# userdel murli

Managing Groups

System administrator can manage a group’s account. The various tasks that a system administrator can perform include adding, modifying and deleting group account.

The following are various the commands:

- groupadd command is for group creation
- groupmod command is for group modification
- groupdelcommand is for group deletion

Account Policies

Account policies are required to manage users effectively. Account Policies contains the following:

Password Policy: These policy settings are used for domain or local user accounts. They determine settings for passwords, such as enforcement and lifetimes.

Account Lockout Policy: These policy settings are used for domain or local user accounts. They determine the circumstances and length of time that an account will be locked out of the system.

Account UID policy: Normal user accounts should not have UID (UserID) value 0(zero). Any account has UID value 0 will get root privileges automatically. System administrators should pay attention on UIID values at the time of account creation.

Account GID policy: Normal user accounts should not have GID (User groupID) value 0(zero). Any user account has GID value 0 will get root privileges automatically. System administrators should pay attention on GIID values at the time of user account creation.

Account creation policy: Policy should be implemented on account creation. Account will be created automatically when a user joined in the organization and needs to access on systems.

Account termination policy: Policy should be implemented on account termination. Account will be terminated automatically with or without grace period, when user superannuated or left or expired.

Kerberos Policy: These policy settings are used for domain user accounts. They determine Kerberos-related settings, such as ticket lifetimes and enforcement. Kerberos policy settings do not exist in local computer policy.

Password Policy

Password policy implementation is very essential to secure accounts and at same time secure the systems, the network and the services. The following are some of the parameters to be enforced as part of setting a password policy:

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Password strength (must meet complexity requirements)

The Passwords must meet complexity requirements policy setting determines whether passwords must meet a series of guidelines that are considered important for a strong password. Enabling this policy setting requires passwords to meet the following requirements:

- The password is at least six characters long
- Store password using reversible encryption for all users in the domain
- The password contains characters from three of the following four categories
    - English uppercase characters (from A through Z)
    - English lowercase characters (from a through z)
    - Base 10 digits (from 0 through 9)
    - Non-alphanumeric characters (for example: !, $, #, or %)

Account Lockout Policy

Someone who attempts to use more than a few unsuccessful passwords while trying to log on to a system might be a malicious user attempting to determine an account password by trial and error. Account Lockout Policy settings control the threshold for this response and the actions to be taken after the threshold is reached. Generally, the number of login attempts to access any critical systems such as banking or any ecommerce applications systems are not more than three attempts. If any user fails to access such systems 3 times, system will automatically lock such account for a particular period. The lockout period depends on system sensitivity or organization. The following are the parameters to be enforced as part of account lockout policy:

- Account lockout threshold
- Account lockout duration
- Reset account lockout counter after

4.7 PERMISSIONS AND RESTRICTIONS

Privilege is defined as the delegation of authority over a computer system r a network or a service. A privilege is a permission to perform an action on a system or its resources. Examples of various privileges include the ability to create a file in a directory, or to read or delete a file, access a device, or have read or write permission to a socket for communicating over the internet. Users who have been delegated absolute control are called privileged. Users who lack most privileges are defined as unprivileged, regular, or normal users.

On Unix-like systems, the superuser (commonly known as 'root') owns all the privileges. Ordinary users are granted only enough permissions to accomplish their most common tasks.

Unprivileged users usually cannot perform the following tasks:

- Adjust kernel options.
- Modify system files, or files of other users.
- Change the owner of any files.
- Change the runlevel (on systems with System V-style initialization).
- Adjust disk quotas.
- Start or stop daemons.
- Signal processes of other users.
- Create device nodes.
- Create or remove users or groups.
- Mount or unmount volumes
- Execute the contents of any `sbin/` directory

Principle of least privilege

In security perspective, the principle of least privilege also known as the principle of minimal privilege requires that in a particular abstraction layer of a computing environment, every module such as a process, a user or a program depending on the subject must be able to access only the information and resources that are necessary for its legitimate purpose.

The following are the benefits of the principle of least privilege:

Better system stability

For example, applications running with restricted rights will not have access to perform operations that could crash a machine, or adversely affect other applications running on the same system.

Better system security

For example, running a system or a service in standard user mode increases protection against inadvertent system-level damage caused by attacks, malware, such as root kits, spyware, and undetectable viruses.

Ease of deployment

In general, the deployment of any application with fewer privileges is easy.

Superuser

The superuser is a special user account, which has all privileges and is used for system administration. Depending on the operating system, the actual name of this account might be the root, administrator or supervisor. In some cases the actual name is not significant, rather an authorization flag in the user's profile determines if administrative functions can be performed.

In Unix-like computer operating systems, root is the conventional name of the user who has all rights or permissions (to all files and programs) in all modes (single- or multi-user). Regardless of the name, the superuser always has user ID (UID) 0 (zero). The root user can do many things an ordinary user cannot, such as changing the ownership of files or directories and many such others. The superuser account always point at root’s home directory.

Filesystem permissions

Most current file systems have methods of assigning permissions or access rights to specific users and groups of users. These systems control the ability of the users to view or make changes to the contents of the filesystem.

Traditional permissions

Permissions on Unix-like systems are managed in three distinct classes such as s user, group, and others. When a file or directory is created, its permissions are restricted by the umask of the process that created it. Files and directories are owned by a user. The owner determines the file's owner class. Distinct permissions apply to the owner. Files and directories are assigned a group, which define the file's group class. Distinct permissions apply to members of the file's group members. The owner may be a member of the file's group. Users who are not the owner or not a member of the group, such users treated under file’s others class. Distinct permissions will apply to others.

The effective permissions are determined based on the user's class. For example, the user who is the owner of the file will have the permissions given to the owner class regardless of the permissions assigned to the group class or others class.

Permissions

The following are the three specific permissions (read, write and execute) on Unix-like systems (flavors of UNIX like all Linux versions and others) that apply to each class:

- The *read* permission grants the ability to read a file. When set for a directory, this permission grants the ability to read the names of files in the directory

- The *write* permission grants the ability to modify a file. When set for a directory, this permission grants the ability to modify entries in the directory. This includes creating files, deleting files, and renaming files.

- The *execute* permission grants the ability to execute a file. This permission must be set for executable binaries (for example a compiled C++ program) or shell scripts (for example a Perl program) in order to allow the operating system to run files. When set for a directory, this permission grants the ability to access file contents.

When permission is not set, the rights it would grant are denied. Files created within a directory will not necessarily have the same permissions as that directory.

Changing permission behavior

Unix-like systems typically employ three additional modes. These are actually attributes but are referred to as permissions or modes. These special modes are for a file or directory overall, not by a class.

- The *set user ID* or *setuid*, or SUID mode. When a file with setuid is executed or is on, the resulting process will assume the effective user ID given to the owner class. It enables users to be treated temporarily as root.

- The *set group ID or setgid* or SGID mode. When a file with setgid is executed or on, the resulting process will assume the group ID given to the group class. When setgid is applied to a directory, new files and directories created under that directory will inherit the group from that directory

- The *sticky bit* mode. The typical behavior of the sticky bit on executable files encourages the kernel to retain the resulting process image in memory beyond termination. On a directory, the sticky permission prevents users from renaming, moving or deleting contained files owned by users other than themselves, even if they have write permission to the directory. Only the directory owner and superuser are exempt from this.

These modes are also referred to as *setuid bit*, *setgid bit*, and *sticky bit*, due to the fact that they each occupy only one bit.

Notation of traditional file permissions

Symbolic notation

There are several ways by which permissions are represented. The most common form is symbolic notation as shown by the command `ls -l`.

For example, the following is the output after executing a command ls –l:

```
[murli@imssit etc]$ ls -l |more
-rw-r--r--   1 root   root    15276  Oct 10  2006  a2ps.cfg
-rw-r--r--   1 root   root     2562  Oct 10   2006  a2ps-site.cfg
drwxr-xr-x 4 root   root     4096  Apr 24  2009  acpi
-rw-r-----   1 root   root      450   Jan 26   2009   auditd.conf
```

The first character indicates the type(is file or directory, etc) and is not related to permissions. The remaining nine characters are in three sets, each representing a class of permissions as three characters. The first set represents the *user* class. The second set represents the *group* class. The third set represents the *others* class.

Each of the three characters represent the read, write, and execute permissions:

`'r'` if reading is permitted, `'-'` if it is not.
`'w'` if writing is permitted, `'-'` if it is not.
`'x'` if execution is permitted, `'-'` if it is not

The following are some examples of symbolic notation:

-rwxr-xr-x a regular file whose user class has full permissions and whose group and others classes have only the read and execute permissions.

crw-rw-r-- a character special file whose user and group classes have the read and write permissions and whose others class has only the read permission.

dr-x------ a directory whose user class has read and execute permissions and whose group and others classes have no permissions.

Numeric notation

Another method for representing Unix like permissions is an octal (base-8) notation. This notation consists of at least three digits. Each of the three rightmost digits represents a different component of the permissions: owner, group, and others.

The following shows file permissions in numeric notation (in Octal)

0000	no permissions
0111	execute
0222	write
0333	write and execute
0444	read
0555	read and execute
0666	read and write
0777	read, write and execute

4.8 CONFIGURING NETWORK SETTINGS

Setting up an ideal network in any organization requires the computer systems to host the applications; the network gateway level components such as the routers and switches; the security devices such as the firewall, the intrusion detection or prevention systems (IDS/IPS); the Anti-virus software to protect from viruses; a policy document that facilitates to implement and enforce various policies for effective usage of system resources and network services; the network design document.

For effective implementation of networked systems in any organization, all the required and involved systems or components shall be installed and configured properly. The network services/applications such as Email, DHCP, DNS, NFS, Web servers, etc will have a configuration files with default values. The system or the network administrator has to study each configuration file and set the required values in place of default values at each configuration files. It includes the IPaddresses connected with systems and services, blocking of unnecessary ports, mapping services with allowed ports, netting of public IPs with private IPs in creation of special Demilitarized Zones(DMzs), enforcing proper Access Control Lists at Firewalls, etc. Configuring the network with proper settings in any networked environment ensures right services at right time always by protecting the environment from hackers or attackers.

4.9 ADVANCE TROUBLESHOOTING

Problem diagnosis and troubleshooting is critical activity which has to be done either manually or automatically (with help of scripts) for effective maintenance of systems and networks and their resources. It can be done locally or remotely.

Problems occur at the network level where systems are connected- due to improper configuration settings done at network components and services; at system level- the physical hardware, the installed operating systems and the system resources.

Basic network issues and troubleshooting tools

Network problems occur due to lack of network connectivity, improper software installations and configurations, insufficient or non-working network hardware, power fluctuations or no power, insufficient or no security devices (firewalls, IDS/IPS- intrusion detection or prevention system) installed in a network, network bandwidth issues, no anti-virus software or not updated anti-virus, and many such related.

Network troubleshooting tools are a necessity for every network administrator. When getting started in the networking field, it is important to have number of tools that can be used to troubleshoot a variety of different network problems and conditions.

Ping

The most commonly used network tool is the ping utility. This utility is used to provide a basic connectivity test between the requesting host and a destination host. This is done by using the Internet Control Message Protocol (ICMP) which has the ability to send an echo packet to a destination host and a mechanism to listen for a response from this host. Simply stated, if the requesting host receives a response from the destination host, this host is reachable. This utility is commonly used to provide a basic picture of where a specific networking problem may exist. For example, if an internet connection is down at an office, the ping utility can be used to figure out whether the problem exists within the office or within the network of the internet provider.

Tracert/traceroute

Once the ping utility has been used to determine basic connectivity, the tracert/traceroute utility can used to determine more specific information about the path to the destination host including the route the packet takes and the response time of these intermediate hosts The tracert utility and traceroute utilities perform the same function but operate on different operating systems, Tracert for Windows machines and traceroute for Linux based machines.

Ipconfig/ifconfig

One of the most important things that must be completed when troubleshooting a networking issue is to find out the specific IP configuration of the variously affected hosts. Sometimes this information is already known when addressing is configured statically, but when a dynamic addressing method is used, the IP address of each host can potentially change often. The utilities are ipconfig on Windows machines and the ifconfig utility on Linux.

Nslookup

Some of the most common networking issues revolve around issues with Dynamic Name System (DNS) address resolution issues. DNS is used by everyone using the internet to resolve commonly known domain names (i.e. google.com) to commonly unknown IP addresses (i.e. 74.125.115.147). When this system does not work, most of the functionality that people are used to goes away, as there is no way to resolve this information. The nslookup utility can be used to lookup the specific IP address(es) associated with a domain name. If this utility is unable to resolve this information, there is a DNS issue. Along with simple lookup, the nslookup utility is able to query specific DNS servers to determine an issue with the default DNS servers configured on a host.

Netstat

Netstat utility is used to display the currently active ports on a Linux machine. This is very important information to find for a variety of reasons. For example, when verifying the status of a listening port on a host or to check and see what remote hosts are connected to a local host on a specific port. It is also possible to use the netstat utility to determine which services on a host that is associated with specific active ports.

Putty

Putty utility is used to connect different systems remotely. Putty is being used to connect to a host via SSH.

Nmap

The nmap utility is one of the most versatile of network tools that is available. Regardless of how much experience a network engineer has, the nmap utility should always be available. Nmap utility can be used for the following:

- port scanning (TCP/UDP)
- version detection
- OS detection
- ping sweeps

Wireshark/tcpdump

Wireshark/tcpdump utilities are the packet scanners that have the ability to capture and analyze individual packets that are sent across a network.

Wireshark includes many different functions that provide the ability to perform a number of different analysis including filtering by conversation (i.e. IPv4, TCP, UDP..) and protocol analysis (HTTP, VoIP protocols (RTP, SIP, H.225..).

Tcpdump is another packet scanner that is available that provides the ability to analyze network traffic and is very easy to configure. Tcpdump is used on a Linux machine (various flavors) and is available for Windows as Windump.

inSSIDer

The inSSIDer utility can be used to not only scan for different networks within the 2.4 and 5 GHz ranges but also list the current signal strengths of different wireless networks within range.

Syslog server

A simple syslog server can be installed in the field to receive network events from key network elements. This information can then be recorded over time and help in determining the cause of a networking problem.

PTRG Network Monitor

The PTRG network monitor utility offers the ability to track the status of different sensors over a period of time. These sensors monitor anything from simple reachability (ping) to the response time of specific services (i.e. HTTP or POP).

System level issues and activities to be done

Generally, system level problems are due to system hardware components, improper operating system installations, improper configuration settings and other such related.

The following are some of the activities to be done by a system administrator:

- Periodically update the Operating system patches, if any
- Remove unnecessary accounts created by default
- Close all ports except the ports required to allow the services
- Harden the operating system
- Regularly monitor the system resources such as the file system, the storage, the log files and analyze.
- Regularly monitor the users and their activities
- Update Anti-virus patches, periodically

Best practices to be followed for ideal networked environment

Organizations require ideal networked systems to be established to run and access various network services or applications. The following points may be kept in mind for the purpose:

- The systems or servers should have adequate resources in terms of processing speed, memory, storage, etc
- Use the Routing and Switching devices with adequate resources
- Configure Firewall Device with proper ACLs(Access Control Lists) to control the network traffic
- Configure IDS/IPS for effective detection of intrusions/intruders
- Configure network configuration files properly for various network services such email, DNS, DHCP etc
- Implement VLANs and enforce traffic limits
- Use appropriate network monitoring tools for effective network monitoring
- Do periodic system and network performance auditing
- Do periodic security audit at system and network level
- Policy to be framed and implemented for effective usage of systems and network resources

Check Your Progress 2

1. Write the standard minimum requirement to create a strong password.

   ……………………………………………………………………………………

   ……………………………………………………………………………………

   ……………………………………………………………………………………

   ……………………………………………………………………………………

   ……………………………………………………………………………………

2. What is the significance of Nmap utility.

   ……………………………………………………………………………………

   ……………………………………………………………………………………

   ……………………………………………………………………………………

   ……………………………………………………………………………………

   ……………………………………………………………………………………

4.10 SUMMARY

The unit emphasized on network management and security issues in a network. The user management and disk management in a security perspective are clearly and comprehensively explained. Various user account policies along with the parameters to be set for a password file are explained. The file permissions are explained with different examples. Finally, the need of problem diagnosis and troubleshooting along with available tools was also discussed.

4.11 ANSWERS TO CHECK YOUR PROGRESS

Check Your Progress 1

1. The following are various security services or parameters
   - Authentication
   - Authorization & Access Control
   - Availability
   - Confidentiality
   - Integrity
   - Nonrepudiation
2. The following are some of Disk Management functions:
   - Create partitions, logical drives, and volumes.
   - Delete partitions, logical drives, and volumes.
   - Format partitions and volumes.
   - Mark partitions as active.
   - Assign or modify drive letters for hard disk volumes, removable disk drives, and CD-ROM drives.

- Obtain a quick visual overview of the properties of all disks and volumes in the system.
- Create mounted drives on systems using the NTFS file system.
- Convert basic disks to dynamic disks.
- Convert dynamic to basic disks, although this is a destructive operation.
- On dynamic disks, create a number of specialty volumes including spanned, striped, mirrored, and RAID-5 volumes.

Check Your Progress 2

1. To set strong password, password contains characters from three of the following four categories and minimum 8 characters.

   - English uppercase characters (from A through Z)
   - English lowercase characters (from a through z)
   - Base 10 digits (from 0 through 9)
   - Non-alphanumeric characters (for example: !, $, #, or %)

2. **Nmap** utility is one of the most versatile of network tools and can be used for the following:

   - port scanning (TCP/UDP)
   - version detection
   - OS detection
   - ping sweeps

4.12 FURTHER READINGS

1. Computer Networks by Andrew S Tanenbaum , Fifth Edition
2. SA2, Redhat System Administration I & II, Student Workbook
3. Cisco Certified Network Associate Study Guide, Seventh Edition by Todd Lammle
4. Redhat Enterprise Linux System Administration
5. Fundamentals of network security by Eric Maiwald, Dreamtech publisher
6. Linux system security, the Administrators guide to open source security tools by Scott Mann. Ellen L. Mitchell, Second edition, Pearson Education.
7. http://en.wikipedia.org/wiki/security