B.E.

Seventh Semester Examination, 2009-2010

System and Network Administration (IT-403-E)

Note : Attempt any *five* questions.

Q. 1. (a) Write the goals and scope of system and network administration.

Ans. Network administration is a modern professional responsible for the maintenance of computer hardware and software that comprises a computer network. This normally includes the deployment, configuration, maintenance and monitoring of active network equipment. A related role is that of the network specialist or network analyst who concentrates on network design and security.

The network administrator is usually the level of terminal/network staff in an organisation and will rarely be involved with direct user support.

It will look after overall health of the network, server deployment, security and ensuring that the network connectivity through a company's LAN/WAN infrastructure is on par with technical considerations at the network level of an organisation hierarchy.

Role of Network Administrator : The actual role of network administrator will vary from company to company but will commonly include activities and tasks such as network address assignment, assignment of routing protocols and routing table configuration as well as configuration of authentication and authorization directory services.

It includes maintenance of network's authorization infrastructure as well as network back up systems.

Q. 1. (b) Which file contains information about password policies such as expiry date? Modification date, etc.? Which tool will change password policies?

Ans. Files Containing Password Policies Information :

File	Description
/etc/group	Contains the names of all the groups on the system.
/etc/gshadow	Contains (optionally) password associated to a group.
/etc/login.defs	Contains predefined values needed when adding a new user such as the minimum and maximum UID and GID, the minimum password length etc.
/etc/passwd	Passwd (5), a text file that contains a list of the systems accounts, giving for each account some useful information like user ID, group ID, home director, shell etc.
/etc/shadow	Shadow (5) contains the encrypted password information for user's accounts and optional the password aging information.
/etc/skel/	Directory containing files and directories to be copied into the home directory of every newly created user.

The purpose of password policy is to establish a standard for creation of strong passwords, the protection of those passwords and frequency of change.

Some Policies :

(i) All system level passwords must be changed on atleast at quarterly basis.

(ii) All user-level passwords must be changed at least every 6 months.

(iii) User accounts that have system level privileges granted through group memberships or programs such as 'sudo' must have a unique password from all other accounts held by that user.

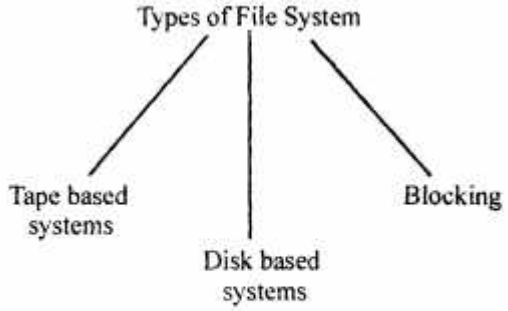
Q. 2. (a) What is the risk involved in retaining the default user name and password?

Ans. Passwords are the important aspect of the computer security. They are the front line of protection for user accounts. A poorly choosen password may result in the compromise of <company name>'s entire corporate network. As such, all <company name> employees (including contractors and vendors with access to <company name> systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Since the user name and password can be assumed to be well known, anyone can access the management console with the administrator privileges. By accessing as root, he gains administrative privileges to the server. This coupled with fact that IP based restriction has not been enabled to access management console, can make server vulnerable for privileged access from any where in the intranet.

Q. 2. (b) What is a file system? Compare the file system of windows and UNIX.

Ans. A file is a collection of related information defined by its creator. Each file in a file system has a unique name for identification. A file name can be splitted in 2 parts–a name and extension.



Comparison of UNIX & Windows :

Factor	UNIX	Windows
Total cost of ownership business value	Higher costs across the board	Market leading TCD & business value.
Mission critical Needs	Scalable, reliable and secure if maintained.	Enterprise class reliability and performance
Applications, partners and choice	Niche solutions, hard to find specialists	Benefit from the world's largest ecosystem
Next generation technologies	Old technology out dated version.	Though leadership for future needs

Q. 3. (a) What information do the shortest job first (SJF) and shortest remaining time first (SRTF) algorithms require about each job or process? How can this information be obtained?

Ans. CPU scheduling deals with the problem of deciding which of the problem in the ready queue is to be allocated the CPU.

Shortest-Job-First (SJF) is a different approach to CPU scheduling. This algorithm associates with each process the length of the latter's next CPU burst when the CPU is available, it is assigned to the process that has the smallest next CPU burst. It the 2 processes.

If 2 processes have the same length of CPU burst then FCFS scheduling algorithms is followed.

As scheduling is done by examining the length of the CPU burst of a process rather than its total length so it is also called shortest next CPU burst scheduling algorithm.

The key concept of this algorithm is "CPU is allocated to the process with least CPU burst time." This algorithm is considered to be an optimal algorithm as it gives the minimum average waiting time as a result.

Prediction Formula Used :

$$\tau_{n+1} = \alpha t_n + (1-\alpha)\tau_n$$

Where t_n contains our most recent information; and τ_n stores the past history in prediction.

If $\alpha = 0$, then $\tau_{n+1} = \tau_n$

$\Rightarrow$ recent history.

Q. 3. (b) Give one advantage and one disadvantage of non-preemptive scheduling.

Ans. Under non-preemptive scheduling once the CPU has been allocated to a process the process keeps the CPU until it releases the CPU either by terminating or by switching to waiting state.

Which is preemptive scheduling execution of a process is preempted before the completion of burst time of the process and only other process may starts its execution whose priority is higher than the first arrived process in the system.

Q. 3. (c) Explain what happens if the scheduler selects a thread to run that has had its suspend ( ) method invoked.

Ans. Threads represent a software approach to improving performance of operating systems by reducing the overhead of process switching.

The SUSPEND service is called as SLEEP or BLOCK in some systems. The designated process is suspended in definitely and placed in the suspended state. It does, however, remain in the system i.e., not terminated or deleted OR destroyed.

A process may suspend itself or another process when it is authorized to do so, by the virtue of its level of privilege, priority OR family membership.

When the running process suspends itself, it in effect voluntarily surrenders control to the OS. The OS responds, by inserting the target process's PCB into the suspended queue and updating PCB state field accordingly.

Q. 4. (a) For a given IP address 172.16.10.22 and mask 255.255.255.240, answer the following :

(i) What is the subnet IP address?

(ii) What is the broadcast IP address?

(iii) What is a valid range for hosts IP addresses?

Ans. (i) Subnet IP Address :

172.16.10.16.

(ii) Broadcast IP Address :

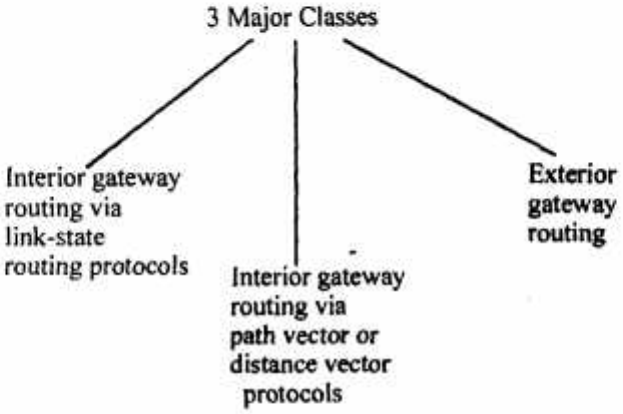
172.16.10.31

(iii) Valid Range :

1st host (172.16.10.17) to last host (172.16.10.30).

Q. 4. (b) What are routing protocols? Also write the different metrics used by the routing protocols.

Ans. Routing Protocols : A routing protocol is a protocol that specifies how routes communicate with each other, disseminating information that enables them to select routes that any 2 nodes on a computer network, the choice of the route being done by routing algorithms.



Distance vector routing protocols are simple and efficient in shall networks and require little, if any management. However, distance vector algorithms do not scale will (due to the count-to-infinity problems) have poor convergence properties and are based on a 'hop count' metric rather than a 'link-state' metric thus they ignore bandwidth (a major drawback) when calculating the best path.

This has led to the development of more complex but more scalable algorithms for use in large networks.

Q. 4. (c) How do UNIX and WINDOWS traceroute differ?

Ans. Trace route is a computer network tool used to show the route taken by the packets across an IP network. An IPv6 variant, traceroutes is also widely available.

The UNIX/LINUX 'traceroute' command and the Microsoft windows 'tracert' commands both accomplishes the task of having network paths but they do it is slightly different ways.

Both of these tools for tracing network routes sends out a packet with TTL (Time to Live) set to) and report its destination. Then they send out a packet with TTL+ 2 and report its destination they continue until the packets reach their final destinations.

The difference is that UNIX 'traceroute' user UDP (User Datagram, Protocol) while Microsoft Windows user ICMP (Internet control message protocol).

Q. 4. (d) What is the difference between a packet and a frame?

Ans. Differences in Frame and a Packet : A packet and a frame are both packages of data moving through a network.

But their working is different.

A packet exist at layer 3 of OSI model.

Whereas a frame exists at layer 2 of the OSI model.

Layer 2 is the Data link layer where layer 3 is the Network Layer.

Data link layer of sending machine adds additional header and trailer to bus and it becomes a frame, then it is passed on to the upper layer which is network layer that will add other information and attach it to the frames which then becomes a packet.

Q. 5. (a) Write the steps for configuring a remote PPP dial up connection.

Ans. Configure a Remote PPP Dial-up Connection : Use the following universal connection wizard procedure to create a dial-up universal connection from a remote server through a server, a partition or an HML that acts as a connecting point to IBM support services to AT & T Global Network Services (AGNs).

(i) Ensure that the Iseries^{TM} Access for windows and issues navigator exist on your personal computer as described in the iseries access for windows : Installation and setup logic.

(ii) Ensure that you install all of the latest service pack for iseries Navigator.

(iii) Ensure that TCP/IP is active.

(iv) You must have security officer authority with (i)A[LOB], (i) IOSYSCFG and (i)SICADM speed authorities in your OS/400 (R) user profile and (i) USE authority to WKK (CNTINF in order to configure the connection using the universal connection wizard.

(v) You must instance the TCP/IP connectivity utilities.

(vi) You must install the cryptograph product 5722–AC3 and Digital Certificate Manager (DCM) Base option 34.

(vii) Ensure that the QRETSVRSEC system value is set to 1.

(viii) The connection point should have been configured on the system or HMC where the modem is attached.

Q. 5. (b) What is Network Address Translation? Explain its working in detail.

Ans. In computer networking, Network Address Translation (NAT) is the process of modifying network address information in datagram (IP) packet headers while in transit over a traffic routing device for the purpose of remapping a given address space into another.

In the mid-1990s NAT became a popular tool for alleviating the IPv4 address exhaustion. It has became a standard indispensable feature in routers for home and small office Internet connections.

NAT observes an internal network's structure : all traffic appears to outside parties as if it originated from the gateway machine.

Types of NAT : NAT is implemented in a variety of schemes of translating addresses and port numbers each affecting application communication protocols differently.

(i) Full Cone NAT : One-to-one NAT

Once an internal address (iAddr: iPort), is mapped to an external address (eAddr : ePort) any packets from iAddr : iPort will be sent through eAddr : ePort.

Any external host can send packets to iAddr : iPort by sending packets to eAddr : ePort.

(ii) (Address) Restricted Cone NAT.

(iii) Port-Restricted cone NAT.

(iv) Symmetric NAT : Each request from the same internal IP address and port to a specific destination IP address and port is mapped to a unique external source IP address and port (this is ambiguous).

Q. 6. (a) What is a Domain Name Server? Write the various steps of configuring a domain name server.

Ans. The DNS servers distribute the job of mapping domain names to IP addresses among servers

allocated to each domain.

Each second-level domain must have atleast one domain name server responsible for maintenance of information about that domain and all subsidiary domains and response to queries about those domains from other computers on the Internet.

Resources : The following references provide additional information about DNS servers :

(i) NSLOOK UP : Provides reports on DNS.

(ii) BIND : The standard DNS server application maintained by the Internet software consortium.

Configuration of DNS :

(i) Start the configure your server wizard. To do so, click start, point to All programs, point to Administrative tools and then click configure your server wizard.

(ii) On the server role page, click DNS server and then click Next.

(iii) On the summary of selections page, view and confirm the options that you have selected. The following items should appear on this page.

(i) Install DNS.

(ii) Run the configure a DNS wizard to configure DNS.

If the summary of selections page lists these 2 items, click Next. If the summary of selections page does not list these 2 items, click **Back** to return to the **Server Role** page, click DNS and then click **Next.**

(iv) When you configure your server wizard installs the DNS service, it first determines whether the IP addresses for this server is static or is configured automatically. If your server is currently configured to obtain its IP address automatically, the configuring components page of the windows components wizard prompts you to configure this server with a static IP address.

Q. 6. (b) What is a TCP Wrapper? How does it provide access control? Write the limitations of the TCP wrapper.

Ans. TCP Wrapper : TCP wrapper is a host based networking ACL system, used to filter network access to Internet protocol servers on (UNIX-File) operating systems, such as LINUX or BSD.

It allows host or subnetwork IP addresses, names and/or ident query replies to be used as token on which to monitor filter for access control protocols.

The original code was written by Dutchman Wieste Veuana in 1990 to monitor a cracker's activities on UNIX workstations at the Dept. of math and computer science at the Endhoven University of Technology. He maintained in until 1995, and on 9 June 1, 2001, released it under its own BSD-style license.

Limitations :

(i) When a new request comes, in the UDP daemons linger around for a while after servicing the request. In the /etc/in etd.conf files, these daemons are registered like the "wait" -options.

(ii) The wrapper do not work with the RPC services over TCP. These services are registered as rpc/tcp in/etc./inetd.conf file.

(iii) Some RPC request like swall, risers et at appear to come from server host.

(iv) The user name look up feature of TCP wrappers uses idented to identify the username of the remote host.

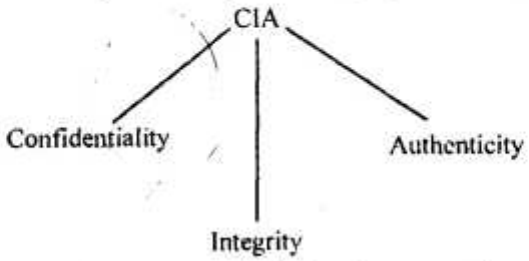
Q. 7. (a) What is computer security? Why is it important? How does CERT refer to it?

Ans. Computer Security : Computer security is a branch of technology known as information security as

applied to computers and networks.

The objective of computer security includes protection of information and property from theft, corruption or natural disaster, while allowing the information and property to remain accessible and productive to its intended users.

The major technical areas of computer security are usually represented by initials CIA :



Confidentiality : (Sercecy or privacy) means that information cannot be access by unauthorized parties.

Integrity : Means that information is protected against unauthorized changes that are not detectable to authorized users.

Authentication : Means that users are who they claim to be.

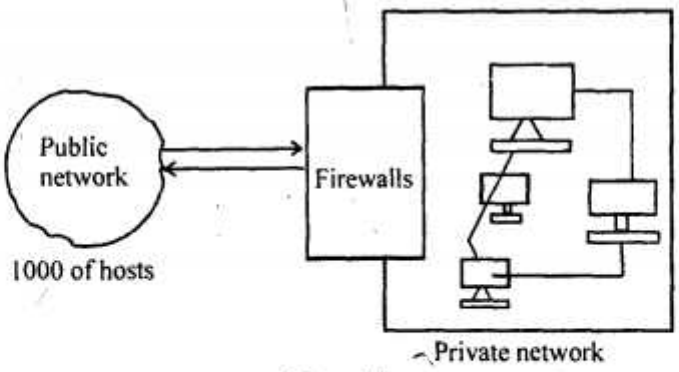
While CIA are the most important aspect of computer security manager, privacy is perhaps the most important aspect of computer security.

CERT : The CERT coordination center was created by DARPA in November 1988 after the Morris worm struck. It is a major coordination center in dealing with internet security problems.

The CERT/CC is run by the federally funded Pittsburgh based Software Engineering Institute (SET) at Cornegie Melon University.

Q. 7. (b) What are firewall? What different types of firewalls exist? Also write what firewalls can block and what they cannot block?

Ans. Firewalls : A firewall is a combination of hardware and software to protect the private network of an organisation from an public networks users.



Firewalls

A basic task of a firewall is to regulate some of the flow of traffic between computer networks of different trust levels.

Typical examples are the internet which is a zone with no trust and an internal network which is a zone of

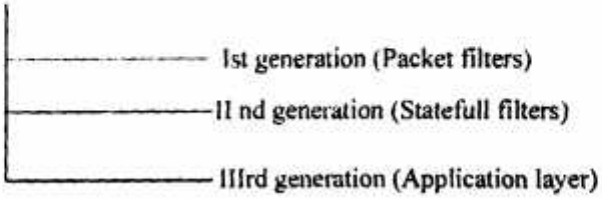
higher trust.

A firewall function within a network is same to firewalls with fire door in building construct.

In former case, it is used to prever :twork intrusion to the private network.

In latter case, it is intended to contain and delay structural fire from spreading to adjacent networks.

Generations of Firewalls :



Types of Firewalls :

(a) Packet Filter : Looks at each packet entering or leaving the network and accepts or rejects it based on the user-defined rules packet filtering is fairly effective and transparent to users but it is difficult to configure.

(b) Application Gateway : Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective but can impose a performance degradation.

(c) Circuit-Level Gateway : Applies security mechanism when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

(d) Proxy Server : Intercepts all message entering and leaving the network. The proxy server effectively hides the true network addresses.

What a Firewalls do?

A firewall examines all traffic routed between the 2 networks to see if it meets certain criteria. If it does; it is routed between outbound traffic.

(i) It filters both inbound and outbound traffic.

(ii) It can also manage public access to private networked resources such as host applications.

Q. 8. Write short notes on any two :

(i) UFS, NFS and NTFS

(ii) System performance tuning

(iii) Use of Make option

.ıs. (i) UFS, NFS and NTFS :

UFS (Unix File System) : UFS is a file system used by many UNIX and UNIX-Like operating systems. It is also called the Berkeley Fast File system, the BSD Faist File System or FFS. It is a distant descendant of the original file system used by version 7 UNIX.

UFS is composed of following parts :

(a) A Few blocks at the beginning of the partition reserved for boot blocks.

(b) A superblock, containing a magic number identifying this as a UNIX file system and some other vital numbers describing this file system's geometry and statistics and behavioural turning parameters.

(c) A collection of cylinder groups.

NFS (Network (File System) : It is a network file system protocol originally developed by Sun Microsystems in 1984, allowing a user on a client computer to access files over a network in a manner similar to how local storage is accessed. NFS, like many other protocols, builds on the Open Network Computing Remote Procedure Call (ONC RPC) system. The Network File System is an open standard defined in RFCs, allowing anyone to implement the protocol.

Versions of NFS :

(a) Original NFS version defined in RFC 1094.

(b) NFSV2 defined in RFC 1094, March 1989, originally operated entirely over UDP.

Rusty Sandberg, Bob Lyon, Bill Joy and Sleve Kleiman created it.

(c) NFSVS : Designed in RFC 1813, June 1995 support for 64-bit file sizes and offsets to handle files larger than 2. gigabytes (GB).

(d)Version 4 : Designed in RFC, 3010, December 2000 (revised in RFC 3530, April 2003). influenced by AFS and CIFS, includes performance improvements mandates strong security.

NFIS : New Technology File System (NTFS) is the standard file system of windows NT, including its later version windows 2000, Windows XP, Windows server 2003, 2008, windows Vista and windows 97.

NTFS supersets the FAT file system as the preferred file system for Microsoft's windows OS.

Developer	Microsoft
Introduced	July 1993 (Windows NT 3-1)
Full Name	New Technology File System
Partition	OXO 7 (MBR)
Identifier	EBDOADA2-B9E5-4433-87CD-6886B7269967 (GPT)

(ii) System Performance Tuning : Performance turning is the improvement of system performance. This is typically an application, but the same methods can be applied to economic markets, bureaucracies or other complex systems. The motivation for such activity is called a performance problem, which can be real or anticipated.

Most system will respond to increases load with some degree of decreasing performance. A system's ability to accept higher load is called scalability and modifying a system to handle a higher load is synonymous to performance tuning.

(iii) Use of Make Option : We can use the make options preference page to create a customised set of make options for each target environment.

For Example : You can use this preference page to specify different sets of options to pass to make.

Using the Make Options, you can :

(a) Create a new set of make options.

(b) Rename an existing set of make options.

(c) Remove an existing set of make options.

(d) Import a set of make options from another location.

(e) Export a set of make options to another location.

(f) Configure a set of make options.