Question 3:

a) Discuss the tasks performed by LinuxConf package. **(5 Marks)**

Linuxconf configuration tasks

Under the configuration section in linuxconf are tasks for setting up your network, creating user accounts, working with file systems, initializing system services, and choosing boot modes. Networking tasks are divided into those that apply to your computer as a client and those that apply to it as a server.

Linuxconf networking tasks

Client networking tasks enable you to view and configure information associated with your computer's host name, the network interfaces that are attached to your computer, and the routes that you can use to get to other hosts and networks. Click the plus sign (+) next to Client tasks and select Basic host information. From the window that appears, here are some of the items that you can change:

- **Host name** — Your host name is how other computers on the network identify yours. It can contain the full`hostname.domainname` form.
- **Adaptor** — The network interfaces (that is, Ethernet cards, PPP dial-up connections, and so on) that give you access to the network can be viewed by clicking the Adaptor tabs on the Basic host information form. The information that you would need to enter in this form is described in detail in Chapter 15, "Setting Up a Local Area Network."

Your system resolves Internet host names into IP addresses by identifying DNS servers that can perform name-to-address resolution. Click the Name Server Specification (DNS) task to add your default domain and one or more name servers. You can also indicate in which domains to search for addresses.

Under Routing and Gateways, you can define how your networking requests are routed across gateway machines (those that are connected to your subnetwork and another subnetwork) to reach beyond your local network. You can also specify routes to other local area networks.

Other network services that you can configure include the Network Information Service (NIS), IPX interface, and serial IP connections (PPP, SLIP, and PLIP). NIS is a way of having a central server store the information that each client computer needs to start up. IPX is a networking interface protocol that is popular with NetWare servers, and PPP, SLIP, and PLIP are ways to connect by using Internet protocols across modems, direct connections, and other serial lines.

If you make any changes to your network configuration, you can activate those changes by clicking the Act/Changes button. You can either preview what needs to be done to activate the changes or click Activate the Changes for the changes to be implemented and the network to be restarted.

Under Server tasks, you can share your file systems with other computers on the network (by using NFS) and set up IP aliases for virtual hosts. You also find tasks for configuring a mail server and an Apache Web Server.

Other Linuxconf configuration tasks

Besides networking tasks, you can select from several other basic system tasks in linuxconf. Under User Accounts, you can add normal user accounts, special user accounts, e-mail aliases, and policies regarding user accounts. Under File Systems, you can add definitions of mountable local drives or NFS file systems (from remote systems) that can later be added to or removed from your system (by using mount and unmount tasks described in the Control section). Finally, you can add parameters that affect how your Linux system boots.

Linuxconf control tasks

The Control section of linuxconf enables you to work with Linux features that change the on-going operation of your Red Hat Linux system. Here are some of the tasks that you can do from this section:

- **Activate configuration** — For changes that you make to take effect, some services must be stopped and restarted. This task checks what needs to be restarted, based on the changes that you have made, and then restarts those services after you say that you are ready.
- **Shutdown/reboot** — Use this task to either shut down and halt your computer or reboot it.
- **Control service activity** — You can enable or disable a variety of network services by selecting this task.
- **Mount/Unmount file systems** — Any local or NFS file systems that you configured to be mountable (in the Configuration section) can be mounted or unmounted by using these tasks.
- **Configure superuser schedule** — You can add commands that are run at a set schedule (by using the cron facility) as the root user by adding entries under this task.
- **Archive configurations** — With this task, you can archive the configuration files that you have set up so that you can recall these saved configuration files later. This task can be used to get you back to a sane state if your configuration files get wrecked.
- **Switch system profile** — You can recall a past archive of configuration files (and save the current configuration files) by using this task.
- **Control files and systems** — Select tasks from this section to change the way that configuration files, commands, file permissions, modules, system profiles, and linuxconf add-ons are configured and used in linuxconf.
- **Date & time**— Change the date, time, and time zone from this task.
- **Features** — Modify the keyboard mapping used for your Linux computer, the language, or several features associated with how HTML is used on your computer.

After you have made changes to any configurations that require programs to be restarted, you can click Act/Changes. Then click the Activate the Changes button that appears. If errors are reported, click Yes to view those messages. Then you can view the log that was created from the changes.

Linuxconf subsection commands

Instead of using linuxconf, you can use commands to go directly to particular configuration sections. commands:

- **Filesystem configurator**— Configures the file systems that your computer can access. This can include local drives and NFS volumes (mounted from remote computers). It also enables you to configure swap files and partitions and set the quota Filesystem configurator window (see Figure 2).

  Figure 2: Mount local and remote file systems by using the Filesystem configurator.

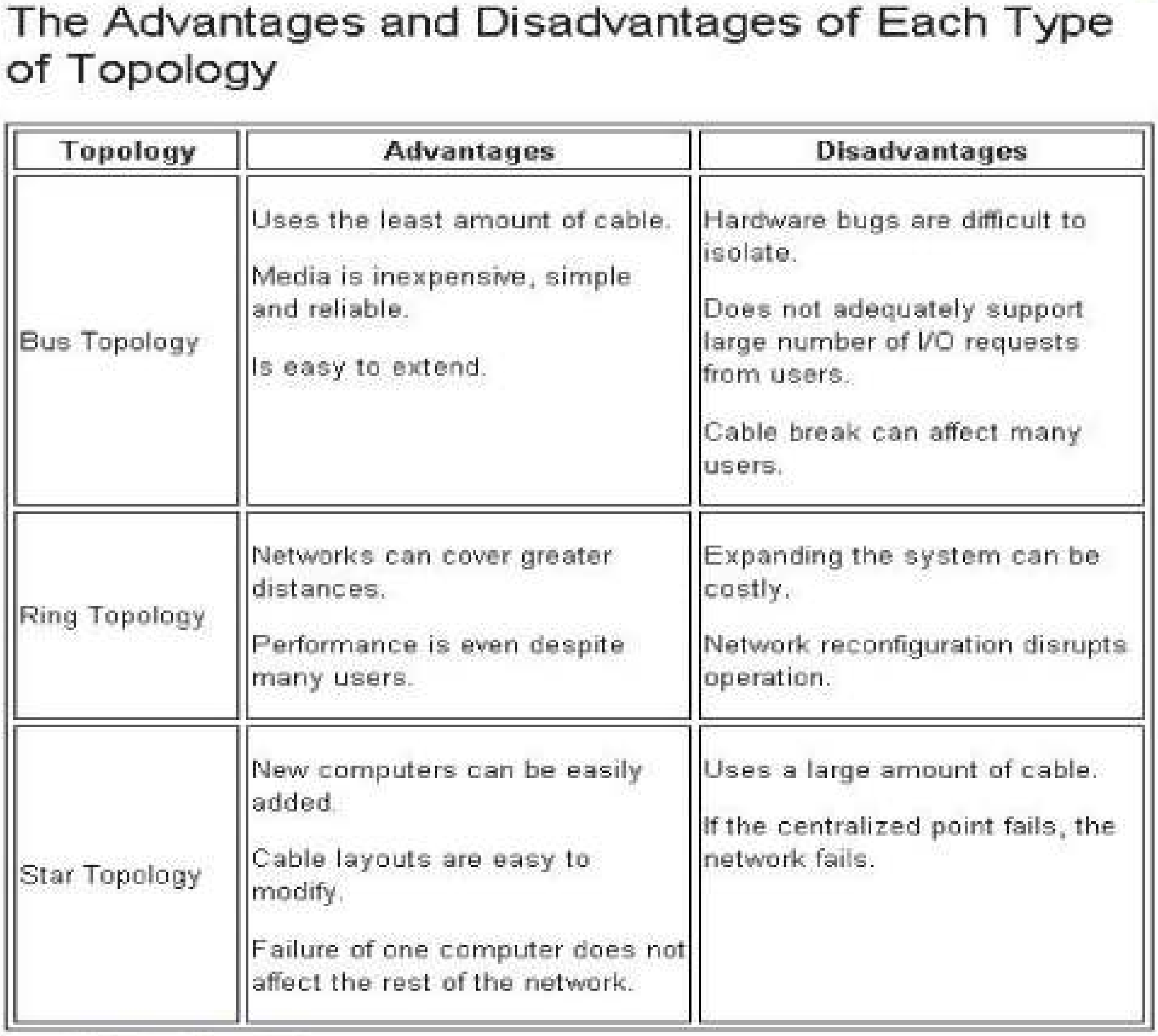
- **Network configurator** (`netconf`) — Configures your TCP/IP network. It enables you to add everything that you need to create connections to modems and Ethernet LANs. You can set up the Domain Name System (DNS), routing and gateways, and serial communications (PPP, SLIP, or PLIP). Figure 3 shows the Network configurator window.

Figure 3: Set up TCP/IP network connections by using the Network configurator.

- **User Account configurator** (userconf) — Manages your computer's user accounts. It enables you to add regular user and group definitions and then assign passwords to users. You can also add special user accounts, such as those that enable you to automatically log in and start a PPP, SLIP, UUCP, or POP connection. Figure 4 shows the User account configurator window.

Figure 4: Add regular and special user accounts in the User account configurator window.

b) Explain the advantages and disadvantages of different LAN topologies. **(5 Marks)**



The Advantages and Disadvantages of Each Type of Topology

Topology	Advantages	Disadvantages
Bus Topology	Uses the least amount of cable. Media is inexpensive, simple and reliable. Is easy to extend.	Hardware bugs are difficult to isolate. Does not adequately support large number of I/O requests from users. Cable break can affect many users.
Ring Topology	Networks can cover greater distances. Performance is even despite many users.	Expanding the system can be costly. Network reconfiguration disrupts operation.
Star Topology	New computers can be easily added. Cable layouts are easy to modify. Failure of one computer does not affect the rest of the network.	Uses a large amount of cable. If the centralized point fails, the network fails.

c) Assume a University has 150 LANs operating in the country with 100 hosts in each LAN. Suppose it has one class B address. Design an appropriate subnet addressing scheme. **(5 Marks)**

Network protocolsnearethethestandardsrulesthatfor deficommunication between network hosts .Examples of protocols used

1.Transmission Control Protocol/Internet Protocol 2.Network Basic Input Output System (NetBIOS) 3.NetBIOS Enhanced E**U**serI). Interface (NetB

TCP/IP is a suite of protocols including Internet **network addressing.**

Each computer, network printer or other network ho –just the same m**a**sileda lettertoyou thatthroughis Australia Post you. These IP addresses can be either configured m operating system. In this esses,wewillandlookhowatnetworksheform other by using subnet masks. To fully understand h binary numbers such as 10001000 to decimal numbers

An IP addresstslongis and32 bimade up of two components, a address is used to identify the network and is co node) address is used totachid**e**ntifydto theaparnetworkicular. Thd represented using-decimalthenotation,doted where 32 bits are d be represented in a decimalWhenform**a**t,computerseparatedredtois useconfbyd IP address each time it *Static*powers .*IP*up,In*addre*thiscontrasist,knownin computer's IP address is assigned*Dynamic* automatically,*IP*The*add*cu**r***ess,*rentveri protocolIPversionis 4 (IPv4) & IP version 6 (IPv6).

Example:-Anof Ipv4 address(dotted decimal notation)

10101.00011000000.11111110.00000001

172 16 254 1

One byte = 8 Bits

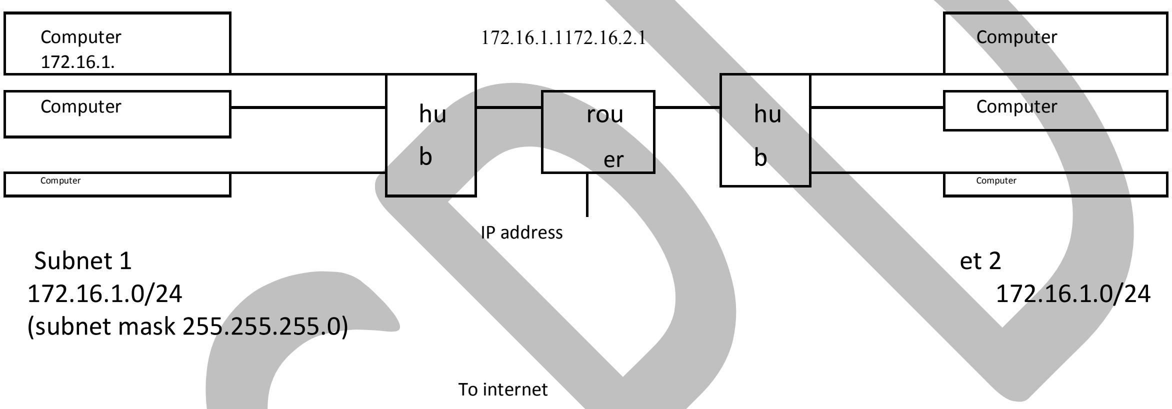
,

So, four byte = 8*4=32

Subnetallows administratorsnetwork to subdivide a single cl networks, allowing allowing the more efficient us standard class full

host number field–**the** into**subnet**wo**ID**onp**and**rts **the host ID** that subnet..

In each of IP address first two bytes (172.16)are



NOTE:-Subnet-Determinemasks whichinthebithost address are the sub

d) Explain the use of different command line tools to perform network monitoring**(5** in**Marks)**Linux.

1. –TopLinux Process Monitoring

Linux **Top** command is a performance monitoring program which is used frequently by many system administrators to monitor Linux performance and it is available under many **Linux/Unix**like operating systems. The top command used to dipslay all the running and active real-time processes in ordered list and updates it regularly. It display **CPU usage**, **Memory usage**, **Swap Memory**, **Cache Size**, **Buffer Size**, **Process PID**, **User**, **Command**s and much more. It also shows high **memory** and **cpu** utilization of a running processess. The top command is much userful for system administrator to monitor and take correct action when required. Let’s see top command in action.

2. VmStat – Virtual Memory Statistics

Linux**VmStat**command used to display**virtualmemory**statistics,**kernerlthreads**,**disks**of,**system processes**,**I/Oblocks**,**interrupts**,**CPUactivity**and much more. By default v available under Linux systems **syssthat**youneed includestoinstall vmsap
common usage of command format is.

3. Lsof – List Open Files

Lsofcommandused in**Linux/Unix**manylike system that is used to displ processes. The open**diskfiles**,**networksockets**included,**pipes**,**devices**areand**processes**.One o the main reason for using notthisbecommandunmountedis whenand displadisk being used or opened. With this commmand you can eas

format for this command is.

4. Tcpdump – Network Packet Analyzer

Tcpdumpone of the mousted widelycommand-li**networkpacketanalyzer**or**packets sniffer**program that is used**TCP/IP**packetscapture thatorfilterreceived or tran over a network. It also provides a optionanalysistosave.tcpdumcap
available in all major Linux distributions.

5. Netstat – Network Statistics

Netstatisa command line **incomi**tola**nfoutgonetworkg**drmingoringpackets statist interface statisticsor. everyItis systemveryusefuladministratortoolf to m troubleshoot network related problems.

6. Htop – Linux Process Monitoring

Htopis a much advanced interactive and real time Linu Linux**topcommand**but it has some **userfriendlyinterfacetomanage**richfeatureslike **process**,**shortcutkeys**,**verticalandhorizontalviewoftheprocesses**and much more. Hto party tool and doesn't included in**YUM**Linuxpackagesystems,manageryout

7. Iotop – Monitor Linux Disk I/O

Iotopis also much**topcommand**siilandrHtop**rogram**,but it has accountin and display**DiskI/O**rea**l**nd**proc**time**sses**.This tool is much usefulrocessforand used disk read/writes of the processes.

8. Iostat – Input/Output Statistics

IoStatis simple tool that w**input**llandc**outpu**llectstorageand showdevicesystemstat often used to trace storageesincluding,devices**localdisks**perfor,**remotedisks**ancesuchissu as**NFS**.

9. IPTraf – Real Time IP LAN Monitoring

IPTrafis an open source-based realconsoletime**IPLAN**)networkmonitoring(**Linux**.tilityItcollf variety of informationtorsuchthataspassesIPtrafficover themoninetwork ICMP details, TCP/UDP traffic breakdowns, TCP connect of general and detaled interface-IP,statisticsIPcksumcheerrors,ofTCP,intU

etc.

10. Psacct or Acct – Monitor User Activity

psacct or acct tools are very useful for monitoring background and keeps a closeachwatchuserononthetheoverallsystem ac are being consumed by them.

These tools are very useful for system administrators commands they issued, how much resourcestheyare **a**rectiveusedonbyth For installation and example usage**MonitorUserActiv**ofcommands**withpsacctory**read

acct

11. Monit – Linux Process and Services Monitoring

Monitis a free open source and web based process superv system processes, programs, files, directories, permi

It monitorsservices like Apache, MySQL, Mail, FTP, ProFTP,
viewed from the command line or using it own web inte

12. NetHogs – Monitor Per Process Network Bandwidth

NetHogsis an open source mn**i**larce smalltop**command**Linuxprogram)that(sikeeps a tab on activity on your system. It also keeps a track of real time

13. iftop – Network Bandwidth Monitoring

iftopis anotheral-bast**e**drminfree open source system monitoring utilit bandwidth utilization (source and destination hosts) that considered for atnetwork**top'**doesusage,forCPUwh**top**usage'family.iftoptoolisthat' monito

displays a current bandwidth usage between two hosts.

14. Monitorix – System and Network Monitoring

Monitorixisa free lightweight r**u**tilitynand monitorthatis systemdesignedandtonetw possibleLinux/Unixservers. It**HTTP**hasweba serverbuilt inthat regularly collect and display them in**systemloadaverageandusage**graphs.ItMonitors,**memoryalocation**,**diskdriver health**,**systemservic**,**networkportss**,**mailstatistics**(**Sendmail**,**Postfix**,**Dovecot**,etc),**MySQLstatistics**and many more. It designed to monitor overall system performa
activities etc.

15. Arpwatch – Ethernet Activity Monitor

Arpwatchis a kind of program that is designed**MAC**and**IP**toaddressmonitorcha of**Ethernet**work traffic on a Linux network. It continuouslyproduces a of**IP**and**MAC**address pair changes along with a timestamps on a n administrator, when a pairing added**ARP**orspoofingchangeson. Ita networkisvery.

Question 4:

(a) What is a networking management system? Explain. **(4 Marks)**

-

A network management system (NMS) is a set of hardw supervise the individual components toffreameworknetwork. wi

Network management system components assist with:

- Network device-identifyingdiscoverywhat devices are present

- Network device-monitoringat the device level to de and extentthe to which their performance-enterprisematches-levelserviccap agreementsSL)As. (

- Network performance-trackinganalysisperformancedicatorsbandsuchwidthutilization,inaspacket lo,sslat,encyavailabilityrou,tersswitchesandandouptimeher ofSimplenagementNetworkProMa (SNMP)-enabled devices.
- Intelligent-conotificationsfigurablealerts that will respond emailing, calling or texting a network administra

(b) Explain the role and importance of following tools for quota management in Linux:

quotacheck

quotacheck examines each filesystem, builds a table of current disk usage, and compares this table against that recorded in the disk quota file for the filesystem (this step is ommitted if option **-c** is specified). If any inconsistencies are detected, both the quota file and the current system copy of the incorrect quotas are updated (the latter only occurs if an active filesystem is checked which is not advised). By default, only user quotas are checked. **quotacheck**expects each filesystem to be checked to have quota files named *[a]quota.user* and*[a]quota.group* located at the root of the associated filesystem. If a file is not present,**quotacheck** will create it.

If the quota file is corrupted, **quotacheck** tries to save as much data as possible. Rescuing data may need user intervention. With no additional options **quotacheck** will simply exit in such a situation. When in interactive mode (option **-i**) , the user is asked for advice. Advice can also be provided from command line (see option **-n**) , which is useful when **quotacheck** is run automatically (ie. from script) and failure is unacceptable.

quotacheck should be run each time the system boots and mounts non-valid filesystems. This is most likely to happen after a system crash.

It is strongly recommended to run **quotacheck** with quotas turned off on for the filesystem. Otherwise, possible damage or loss to data in the quota files can result. It is also unwise to run **quotacheck** on a live filesystem as actual usage may change during the scan. To prevent this, **quotacheck** tries to remount the filesystem read-only before starting the scan. After the scan is done it remounts the filesystem read-write. You can disable this with option **-m**. You can also make **quotacheck** ignore the failure to remount the filesystem read-only with option **-M**.

repquota

repquota prints a summary of the disc usage and quotas for the specified file systems. For each user the current number of files and amount of space (in kilobytes) is printed, along with any quotas created with **edquota**(8).

quota

quota displays users' disk usage and limits. By default only the user quotas are printed.

quota reports the quotas of all the filesystems listed in **/etc/mtab**. For filesystems that are NFS-mounted a call to the rpc.rquotad on the server machine is performed to get the information.

(6 Marks)

(c) Write the purpose of VPN and name the VPN technologies supported by Windows 2000. **(5 Marks)**

Purpose?

VPN is an abbreviation for Virtual Private Network, commonly referred to as VPN network. It allows for secure connection between networks and computers by means of dangerous and untrusted media which include the Internet, radio connections and leased lines. Although the connections are not secured, the transmission between the networks and computers uses secured and encrypted virtual channels.

Remote access is not at all extraordinary or de luxe for many users. It is much more of a necessity which grants access to files and other resources of the local network (e.g. the company network) when one is at home or on the road. Miles of new cables that would be needed to access the company network are thus replaced with the virtual network, i.e. the existing infrastructure of public network. Such a network becomes private for its definite users by using encryption protocols and other types of security measures which make the private network inaccessible for other users of the public network. To put it more precisely, data is transmitted as TCP/IP protocol data packets within the data packets of the secure IPSec protocol. For this reason, VPN networks are called tunnel connections since IPSec protocol creates a secure tunnel for transmitting TCP/IP data packets. Appropriate telecommunications software is necessary for encrypting and transmitting these types of data

packets. There are other protocols that allow for creating tunnel connections. The most popular ones include PPTP, L2TP, IPSec and SSL.

Communication operators often use such networks. They can also be supported by special telecommunications software. For instance, Telekomunikacja Polska (Polish national telecommunications provider) activated a service for companies with several or up to twenty branches. The new service is based on telecommunications software for VPN networks and allows for free connections between all the company branches spread over large areas. When customers purchase this service, they also receive a server with the software for managing IP telephony and a set of IP telephones. The service also includes repairs and administration of the provided devices.

name the VPN technologies supported byWindows 2000

ADSL, Cable vision , ATM or Frame Relay CISCO VPN, Freeswan VPN, et

(d) Compare the security features/mechanism of Windows2000 and Linux operating**(5** systems**Marks)**.

fundamental changes in Linux and Windows security

For users, the evolution of Linux and Windows has all the trappings of a muscle car drag race. Users may have their favorite but at the same time continue to assess the competition. Microsoft has shown a great willingness -- no doubt spurred on by industry cynicism and the growing adoption of Linux -- to dedicate massive resources to Windows security. Microsoft will make advances in Windows security within the next few months when it releases Service Pack 2 for Windows XP. This service pack enhances Windows security by turning off some services by default and will also provide new patch management tools. For example, the Alterer and Messenger service has been turned off to reduce the amount of spam received. In many cases, turning off features is good since it makes a system more secure. However, the challenge is to enable to security without a tradeoff in key functionality or flexibility.

What is most outstanding is Microsoft's focus on enhancing security through improved usability. For example, a number of Microsoft security exploits in 2003 were the result of an email attachment launching as an executable (e.g., MyDoom). Service Pack 2 features an attachment execution service that will have a central place for attachments to be accessed by Outlook/Exchange, Windows Messenger, and Internet Explorer. This will reduce the risk of an end user enabling a virus or worm by launching an executable. Also, disabling execution of data pages will limit the potential for buffer-overflow exploits. Still, rather than actually fixing Windows' broken infrastructure and secure communications, Microsoft leaves the burden on the user.

Microsoft's focus is clearly on shoring up application security. There are a number of Service Pack 2 enhancements that specifically target Outlook/Exchange and Internet Explorer. For instance, there will be an intelligent MIME-type review in Internet Explorer that will check the content type of an object and let the user know if is a potentially harmful executable. This raises the question of whether the software will be able to distinguish a virus from a colleague's spreadsheet extension.

Another new feature in Service Pack 2 is the ability to uninstall additions to a browser, which potentially places more responsibility on the end user who may have to look at many plug-ins and uninstall the right ones. Outlook/Exchange will have the ability to preview email messages, so a user can delete a message without actually opening it. A further application security enhancement is a firewall that starts prior to the network stack. For software developers, the changes to remote procedure call permissions will make it a harder to write code that is not secure.

Service Pack 2 will offer many flashy new features for Windows users, but the question remains: Will these features burden system administrators, and possibility end users, with more complexity, rather than addressing the security of Windows operating system code?

Open source, shared source

A purely philosophical difference between Linux and Windows is the approach to code transparency. Linux is licensed under the GNU General Public License, which means it is possible for users to copy, modify, and redistribute the source code. Windows is a closed source operating, which is why its security methodology is often characterized as "security through obscurity." In 2001, Microsoft responded to the demands of its customers and critics with the Shared Source Initiative, which provides access to Windows source code. Today, the Shared Source Initiative has one million participants, and source code is available for Windows 2000, Windows XP, Windows Server 2003, Windows CE 3.0, Windows CE .Net, and the C#/CLI implementations, as well as components of ASP .Net and Visual Studio .Net. Shared Source Initiative licensees include corporate customers, governments, partners, academics, and individuals.

To a large degree Microsoft's Shared Source Initiative is a policy of "look but don't touch." The rare exception is the Windows CE Shared Source Premium Licensing Program available to companies, which brings Windows CE-based devices and solutions to market. This is the only Windows program under the Shared Source Initiative that provides original equipment manufacturers (OEMs), silicon vendors, and systems integrators full access to Windows CE source code. All licensees have complete access to the source code and the right to modify the code; however, only OEMs can commercially distribute those modifications in Windows CE-based devices. All other shared source licensees have to make a trip to Microsoft in Redmond, Wash., to access source code that is not available through the program.

Although some users may find the Shared Source Initiative useful for debugging applications, the requirement to be physically at Microsoft headquarters to do a build is a significant limitation. Despite Microsoft's efforts to add more transparency, this inability to do a build makes it difficult, if not impossible, to know whether the code will work when implemented in an actual IT environment.

The restrictions against modifying and recompiling Windows source code reduce the incentive for people with access to the Windows Shared Source to look for security vulnerabilities.