LINUX & NETWORK SECURITY

Submitted by:

Ch.Gowthami,
IV/II C.S.E,
E-mail id:gowthami.ch@gmail.com.

V.Indira Priyadarshini,
IV/II C.S.E,
E-mail id:priyavcse@rediffmail.com.

ST. ANN'S COLLEGE OF ENGINEERING & TECHNOLOGY
CHIRALA

ABSTRACT

Security is a perennial concern for IT administrators. Linux provides more security capabilities. Linux has more advantages than other operating systems. Linux is an operating system which is widely using now-a-days. Most of the IT companies such as Sun Microsystems,IBM etc., prefer to use Linux operating system as it was the most economical one.

In this paper we are introducing Linux by explaining its features, properties and current applications. Various threats to Network security are mentioned and why we need security is explained. Network security in Linux is explained by using Firewall and Intrusion detection techniques. With the rapid popularization of the Internet, the term firewall is more commonly used in computer networking. Without a firewall, intruders on the network would likely be able to destroy, tamper with or gain access to the files on your computer. A firewall is a system or router that sits between an external network (i.e. the Internet) and an internal network. Intrusion Detection Systems are designed to catch what might have gotten past the firewall. Several advantages of Linux are explained and it is compared with Windows operating system

1:Introduction to Linux

Linux is a member of the UNIX family but is different than most UNIX implementations because it provides a great UNIX server/workstation environment at a low cost, can be run on a wide variety of platforms, and contains no proprietary code.

Linux supports a full and high quality implementation of the TCP/IP networking protocols. With a network interface card or a modem and PPP, one can connect a machine to a local area network or the Internet and have access to many additional services and network utilities. Linux provides two methods of establishing host-network services. Servers can either run stand-alone or under the control of a program called inetd. Heavily used services will usually run stand-alone. This means the service does all the management and listening on a socket or port. The most common stand-alone services are inetd, syslogd, portmapper, named, and routed.

1.1:Linux is an Open Source Operating system

The idea behind Open Source software is rather simple: when programmers can read, distribute and change code, the code will mature. People can adapt it, fix it, debug it, and they can do it at a speed that dwarfs the performance of software developers at conventional companies. This software will be more flexible and of a better quality than software that has been developed using the conventional channels, because more people have tested it in more different conditions than the closed software developer ever can.

1.2:Properties of Linux:

- Linux is free
- Linux is portable to any hardware platform
- Linux was made to keep on running
- Linux is secure and versatile
- Linux is scalable

1.3:Current application of Linux systems

Today Linux has joined the desktop market. Linux developers concentrated on networking and services in the beginning, and office applications have been the last barrier to be taken down. Linux, an acceptable choice as a workstation, providing an easy user interface and MS compatible office applications like word processors, spreadsheets, presentations and the like.

On the server side, Linux is well-known as a stable and reliable platform, providing database and trading services for companies like Amazon, the well-known online bookshop, US Post Office, the

German army and such. Especially Internet providers and Internet service providers have grown fond of Linux as firewall, proxy- and web server, and we would find a Linux box within reach of every UNIX system administrator who appreciates a comfortable management station.

Clusters of Linux machines are used in the creation of movies such as "Titanic", "Shrek" and others. In post offices, they are the nerve centers that route mail and in large search engine, clusters are used to perform internet searches.These are only a few of the thousands of heavy-duty jobs that Linux is performing day-to-day across the world.

Linux is the only operating system in the world covering such a wide range of hardware.

2:Introduction to Network Security

A network is defined as any set of interlinking lines resembling a net, *a network of roads i.e.,* an interconnected system, *a network of alliances*. A computer network is simply a system of interconnected computers.

2.1:Why Do We Need Security

In the ever-changing world of global data communications, inexpensive Internet connections, and fast-paced software development, security is becoming more and more of an issue. Security is now a basic requirement because global computing is inherently insecure. As your data goes from point A to point B on the Internet, for example, it may pass through several other points along the way, giving other users the opportunity to intercept, and even alter, it. Even other users on your system may maliciously transform your data into something you did not intend. Unauthorized access to your system may be obtained by intruders, also known as "crackers", who then use advanced knowledge to impersonate you, steal information from you, or even deny you access to your own resources.

2.2:Threats to Network security

- Threat is typically from someone with motivation to gain unauthorized access to your network or computer. You must decide whom you trust to have access to your system, and what threat they could pose.

  There are several types of intruders, and it is useful to keep their different characteristics in mind as you are securing your systems.

  - The Curious - This type of intruder is basically interested in finding out what type of system and data you have.

- The Malicious - This type of intruder is out to either bring down your systems, or deface your web page, or otherwise force you to spend time and money recovering from the damage he has caused.

- The High-Profile Intruder - This type of intruder is trying to use your system to gain popularity and infamy. He might use your high-profile system to advertise his abilities.

- The Competition - This type of intruder is interested in what data you have on your system. It might be someone who thinks you have something that could benefit him, financially or otherwise.

- The Borrowers - This type of intruder is interested in setting up shop on your system and using its resources for their own purposes. He typically will run chat or irc servers, porn archive sites, or even DNS servers.

- The Leapfrogger - This type of intruder is only interested in your system to use it to get into other systems. If your system is well-connected or a gateway to a number of internal hosts, you may well see this type trying to compromise your system.

3:Network Security in Linux

You will learn how to set up a Linux server and how to configure name resolution and dial-in network access using the X window system. You will also be exposed to file sharing technologies such as the Network File System (NFS), NetWare's NCP file sharing, and the File Transfer Protocol (FTP). Finally, you will be introduced to network security, including concepts such as firewalls, encryption, and network intrusion detection. In order to reinforce the material, the course provides a range of laboratory and hands-on assignments that puts you in the role of a problem solver, requiring you to apply concepts presented in the modules to situations that might occur in a real-life work environment.

3.1:Firewall:

Firewall is a vague term that can mean anything that acts as a protective barrier between us and the outside world, generally the Internet. A firewall can be a dedicated system or a specific application that provides this functionality. Or it can be a combination of components, including various combinations of hardware and software. Firewalls are built from "rules" that are used to define what is allowed to enter and/or exit a given system or network.

After disabling unnecessary services, we now want to restrict accepted services as to allow only the minimum required connections. A fine example is working from home: only the specific connection between your office and your home should be allowed, connections from other machines on the Internet should be blocked.

3.1.1 Packet filters

The first line of defense is a *packet filter*, which can look inside IP packages and make decisions based on the content. Systems running the **ipchains** firewall are based on 2.2 kernels. Newer systems (2.4 kernel) use **iptables**, a next generation packet filter for Linux, and the Gnome Lokkit tool. This tool was only created to provide an easy interface for normal users. It sets up a basic firewall configuration for a desktop, a dial-up or cable modem connection, and that's about it. It should not be used in larger environments.

One of the most noteworthy enhancements in the newer kernels is the *stateful inspection* feature, which not only tells what is inside a packet, but also detects if a packet belongs or is related to a new or existing connection.

Development is ongoing, so it is best to check with each new version of a distribution which system is being used.

3.1.2. TCP wrappers

TCP wrapping provides much the same results as the packet filters, but works differently. The wrapper actually accepts the connection attempt, then examines configuration files and decides whether to accept or reject the connection request. It controls connections at the application level rather than at the network level.

TCP wrappers are typically used with **xinetd** to provide host name and IP-address-based access control. In addition, these tools include logging and utilization management capabilities that are easy to configure.

The advantages of TCP wrappers are that the connecting client is unaware that wrappers are used, and that they operate separately from the applications they protect.

The host based access is controlled in the `hosts.allow` and `hosts.deny` files. More information can be found in the TCP wrapper documentation files in `/usr/share/doc/tcp_wrappers-<version>/` and in the man pages for the host based access control files, which contain examples.

3.1.3:Proxies

Proxies can perform various duties, not all of which have much to do with security. But the fact that they are an intermediary make proxies a good place to enforce access control policies, limit direct connections through a firewall, and control how the network behind the proxy looks to the Internet.

3.1.4:Access to individual applications

Some servers may have their own access control features. Common examples include Samba, X11, Bind, Apache and CUPS. For every service you want to offer check which configuration files apply.

3.1.5:Log files

If anything, the UNIX way of logging all kinds of activities into all kinds of files confirms that "it is doing something." Of course, log files should be checked regularly, manually or automatically. Firewalls and other means of access control tend to create huge amounts of log files, so the trick is to try and only log abnormal activities.

3.1.6:Types of Firewalls

There are two types of firewalls.

1. Filtering Firewalls - that block selected network packets.

2. Proxy Servers (sometimes called firewalls) - that make network connections for you.

Packet Filtering Firewalls

Packet Filtering is the type of firewall built into the Linux kernel.

A filtering firewall works at the network level. Data is only allowed to leave the system if the firewall rules allow it. As packets arrive they are filtered by their type, source address, destination address, and port information contained in each packet.

Many network routers have the ability to perform some firewall services. Filtering firewalls can be thought of as a type of router. Because of this you need a deep understanding of IP packet structure to work with one.

Because very little data is analyzed and logged, filtering firewalls take less CPU and create less latency in your network.

Filtering firewalls do not provide for password controls. User can not identify themselves. The only identity a user has is the IP number assigned to their workstation. This can be a problem if you are going to use DHCP (Dynamic IP assignments). This is because rules are based on IP numbers you will have to adjust the rules as new IP numbers are assigned. I don't know how to automate this process.

Filtering firewalls are more transparent to the user. The user does not have to setup rules in their applications to use the Internet. With most proxy servers this is not true.

Proxy Servers

Proxies are mostly used to control, or monitor, outbound traffic. Some application proxies cache the requested data. This lowers bandwidth requirements and decreases the access the same data for the next user. It also gives unquestionable evidence of what was transferred.

There are two types of proxy servers.

1. Application Proxies - that do the work for you.

2. SOCKS Proxies - that cross wire ports.

Application Proxy

The best example is a person telneting to another computer and then telneting from there to the outside world. With a application proxy server the process is automated. As you telnet to the outside world the client send you to the proxy first. The proxy then connects to the server you requested (the outside world) and returns the data to you.

Because proxy servers are handling all the communications, they can log everything they (you) do. For HTTP (web) proxies this includes very URL they you see. For FTP proxies this includes every file you download. They can even filter out "inappropriate" words from the sites you visit or scan for viruses.

Application proxy servers can authenticate users. Before a connection to the outside is made, the server can ask the user to login first. To a web user this would make every site look like it required a login.

SOCKS Proxy

A SOCKS server is a lot like an old switch board. It simply cross wires your connection through the system to another outside connection. Most SOCKS server only work with TCP type connections. And like filtering firewalls they don't provide for user authentication. They can however record where each user connected to.

3.1.6:Firewall Architecture

There are lots of ways to structure your network to protect your systems using a firewall.If you have a dedicated connections to the Internet through a router, you could plug the router directly into

your firewall system. Or, you could go through a hub to provide for full access servers outside your firewall.

(i)Dial-up Architecture

You may be using a dialup service like an ISDN line. In this case you might use a third network card to provide provide a filtered DMZ. This gives you full control over your Internet services and still separates them from your regular network.

(ii)Single Router Architecture

If there is a router or cable modem between you and the Internet. If you own the router you could setup some hard filter rules in the router. If this router is owned by your ISP so you may not the have the needed controls. You can ask your ISP to put in filters.

(iii)Firewall with Proxy Server

If you need to monitor where users of your network are going and your network is small, you can intergrate a proxy server into your firewall. ISP's some times do this to create interest list of their users to resell to marketing agencies.

We can put the proxy server on your LAN as will. In this case the firewall should have rules to only allow the proxy server to connect to the Internet for the services it is providing. This way the users can get to the Internet only through the proxy.

(iv)Redundant Internet Configuration

If you are going to run a service like YAHOO or maybe SlashDot you may want to make your system by using redundant routers and firewalls.

By using a round-robin DNS techniques to provide access to multiple web servers from one URL and multiple ISP's, routers and firewalls using High Avaibility technics you can create a 100% uptime service.It is easy to let your network get out of hand. Keep control of every connection. It only takes a user with a modem to compromise your LAN.

3.2:Intrusion detection

Intrusion Detection Systems are designed to catch what might have gotten past the firewall. They can either be designed to catch an active break-in attempt in progress, or to detect a successful break-in after the fact. In the latter case, it is too late to prevent any damage, but at least we have early awareness of a problem. There are two basic types of IDS: those protecting networks, and those protecting individual hosts.

For host based IDS, this is done with utilities that monitor the file system for changes. System files that have changed in some way, but should not change, are a dead give-away that something is amiss. Anyone who gets in and gets root access will presumably make changes to the system somewhere. This is usually the very first thing done, either so he can get back in through a backdoor, or to launch an attack against someone else, in which case, he has to change or add files to the system.

Network intrusion detection is handled by a system that sees all the traffic that passes the firewall (not by portscanners, which advertise usable ports). Snort is an Open Source example of such a program.

3.2.1:Recovering from intrusion

The following actions in this order:

- Disconnect the machine from the network.
- Try to find out as much as you can about how your security was breached.
- Backup important non-system data.
- Re-install the system.
- Use new passwords.
- Restore from system and data backups.
- Apply all available updates.
- Re-examine the system: block off unnecessary services, check firewall rules and other access policies.
- Reconnect.

4:Advantages of Linux Operating systems

1.Linux source code is freely distributed. Tens of thousands of programmers have reviewed the source code to improve performance, eliminate bugs, and strengthen security. No other operating system has ever undergone this level of review. This Open Source design has created most of the advantages listed below.

2.Linux has the best technical support available. Linux is supported by commercial distributors, consultants, and by a very active community of users and developers. In 1997, the Linux community was awarded InfoWorld's Product of the Year Award for Best Technical Support over all

commercial software vendors.

3.Linux has no vendor lock-in. The availability of source code means that every user and support provider is empowered to get to the root of technical problems quickly and effectively. This contrasts sharply with proprietary operating systems, where even top-tier support providers must rely on the OS vendor for technical information and bug fixes.

4.Linux runs on a wide range of hardware. Most Linux systems are based on standard PC hardware, and Linux supports a very wide range of PC devices. However, it also supports a wide range of other computer types, including Alpha, Power PC, 680x0, SPARC, and Strong Arm processors, and system sizes ranging from PDAs (such as the PalmPilot) to supercomputers constructed from clusters of systems (Beowulf clusters).

5.Linux is exceptionally stable. Properly configured, Linux systems will generally run until the hardware fails or the system is shut down. Continuous up-times of hundreds of days (up to a year or more) are not uncommon.

6.Linux has the tools and applications you need. Programs ranging from the market-dominating Apache web server to the powerful GIMP graphics editor are included in most Linux distributions. Free and commercial applications meet are available to meet most application needs.

7.Linux interoperates with many other types of computer systems. Linux communicates using the native networking protocols of Unix, Microsoft Windows 95/NT, IBM OS/2, Netware, and Macintosh systems and can also read and write disks and partitions from these and other operating systems.

8.Linux has a low total cost of ownership. Although the Linux learning curve is significant, the stability, design, and breadth of tools available for Linux result in very low ongoing operating costs.

9.Linux: ``all for one and one for all All changes one makes in Open Source software will benefit each and everyone, all over the world. Without exceptions or constraints.

10.Linux is fun.

5.Comparison of Linux to Windows

Linux is fundamentally more secure than Windows. Linux is some bulletproof wonder of security. Linux more secure than Windows because Linux is open source. Any cracker who wants can hunt for security holes all day long. Microsoft is closed source. If closed source is so much better for security, why is my virus detector still yelping every few minutes as the latest Windows virus, Swen

tries to e-mail it way in.

Indeed, what some security lunkheads claim is a flaw in Linux, its open source nature, has proven to be a security virtue. Potential security holes are spotted and fixed in Linux much faster than they are in Windows.

Windows has always been insecure because of basic design flaws. Microsoft's own fundamental operating system principles of enabling data and programs to work together at a low level has provided both the ability for programs to interoperate with each other over the network, from Windows for Workgroups' dynamic data exchange (DDE) to Server 2003's ActiveX, while simultaneously giving crackers the ability to break into and corrupt Windows systems.

More than one person can log on to X-Windows simultaneously, each with their own separate copy of windows - each copy can be password protected - you can then switch between these two or more copies as necessary.

6.Conclusion

Linux is a project that is never finished, that is true, but in an ever changing environment,it is also a project that continues to strive for perfection. To do security right, you have to be updating your programs and operating systems constantly. Windows, Linux, whatever. If you want your systems to be trouble-free, you need to take a lot of trouble. Hard work and constant diligence are the only real security answer. It's just that with Linux, you see, you don't have to work so hard.

References

Books:

1.Linux complete

2.RedHat Linux

Web-sites:

1.http://www.linux.iguana.be

2.http:www.linuxsecurity.com

3.http://linuxjournal.com

4http://linux.com

5.http://linux.ittoolbox.com