Linux vs windows vulnerabilities

Linux architecture

Windows architecture

Password policy

Types of computer environments

NTFS Permissions,

Understanding Local Group Policy Objects, Understanding Domain Group

Policy Objects,

Deploying package management strategies, Understanding other tools

Configuring and monitoring logs, logging with syslog and alternatives, parsing and filtering

Hardening and Securing Linux Services:

1. Linux is yours, Windows is still theirs.

\* The EULA for Windows clearly states that Microsoft maintains full access to your Windows system and any personal data stored with it. They reserve the right to change any software or settings at any time. The user is leasing the software; they do NOT own it. Attempting to change or redistribute Windows in any way is a violation of copyright law and you can be put in jail for it. Much of the system is off-limits to users. Although Windows does employ the use of administrative access levels, MS is in essence a “hyper-user” because code can be executed by them remotely without local approval. This leaves doors open to nefarious third parties who want to add malicious software to Windows systems.

\* Linux users with administrator privileges must approve the installation of all software, authorize any changes to the system and are encouraged to customize it to make the system more useful for them. Re-distribution of Free and Open Source software is encouraged. Linux users have full access to every part of the system. No code can be executed or access granted to a Linux system without the express permission of the “root user.”

2. Linux Desktops do NOT need any antivirus software, Windows is still vulnerable even with antivirus installed.

\* It is not simply a matter of Linux having less users that makes it more secure; the system is inherently secure. Case in point: Linux web servers that are continually “banged on” by would-be hackers. Linux is the safest choice for desktop computer users. While no OS is totally secure, the chances of Linux users getting a virus are very, very small.

\* Windows users are encouraged to install and pay for antivirus software that is only about 20 percent effective. On-screen widgets and constant nags constitute “Security Theater.” Antivirus software severely limits system performance.

\* Linux security depends on stringent observance of user privileges and file permissions along with keeping the system up to date with the latest security patches.

3. Linux uses a centralized software approach, Windows does not.

\* Most Linux software is available from distribution-specific online “repositories.” Linux users have access to thousands of free programs that can be installed from graphic software managers or with simple commands at a terminal.

\* Windows also has a “store” but most Windows users still think in terms of downloading software from independent web sites, some of which contains malicious code.

\* The novice Linux user should never have to build software from source code. Reputable software vendors will provide proper packaging for Linux. Avoid those who do not.

\* In addition to distributions repositories: Linux users can download software from third party package management systems like Snappy and Flatpak. Ubuntu offers Private Package Archives (PPA) and some software is distributed for direct download in package formats like .deb and .rpm.

\* Most new-user-friendly Linux distributions come with the most needed software already installed.

\* Linux software is installed in predetermined directories. It cannot be moved or installed elsewhere.

4. Linux has built-in hardware support, Windows requires users to find and install drivers.

\* Hardware with Linux support usually just works without the need for users to do anything.

\* Proprietary drives are available through on-line repositories for hardware that requires them. Many distributions automatically install them during setup or make them available to users through special graphic driver manager applications.

\* Many Windows based driver packages include unwanted software or adware.

5. Linux Updates everything at once, Windows does not

\* Most Linux systems look for updates automatically and alert users when they are available.

\* Linux updates ALL software installed from repositories, PPA’s and Snappy packages and Flatpaks.

\* Windows only updates Windows and some select MS software.

\* Windows is notorious for downloading and install updates and then restarting the machine without user’s consent.

\* Linux does not require programs to run in the background to “listen” for updates.

\* Linux will NEVER restart the computer without your permission!

6. Linux uses /dev for drives, Windows uses ABC’s

\* Linux treats all storage devices and network storage as directories.

\* Windows assigns arbitrary letters to identify storage devices and network connections.

22

Linux operating system

An operating system can be described as an interface among the computer hardware and the user of any computer. It is a group of software that handles the resources of the computer hardware and facilitates basic services for computer programs.

An operating system is an essential component of system software within a computer system. The primary aim of an operating system is to provide a platform where a user can run any program conveniently or efficiently.

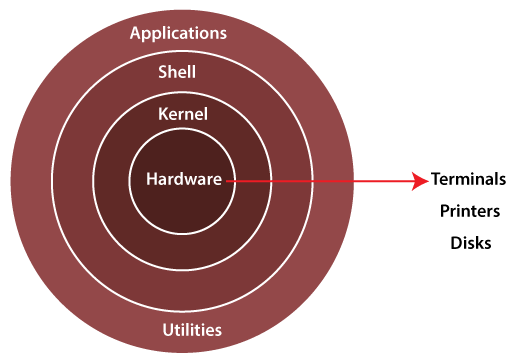
On the other hand, [Linux](https://www.javatpoint.com/linux-tutorial) OS is one of the famous versions of the UNIX OS. It is developed to provide a low-cost or free OS for several personal computer system users. Remarkably, it is a complete OS Including an **X Window System, Emacs editor,** [**IP/TCP**](https://www.javatpoint.com/computer-network-tcp-ip-model)**, GUI** (graphical user interface), etc.

Linux operating system history

In 1991, the Linux history started with the starting of a particular project by the Finland student **Linus Torvalds** for creating a new free **OS kernel**. The final Linux Kernel was remarked by continuous development throughout the history since then.

* Linux was proposed by the Finland student Linus Torvalds in 1991.
* HP-UX (**Hewlett Packard**) 8.0 version was published.
* Hewlett Packard 9.0 version was published in 1992.
* FreeBSD 1.0 version and **NetBSD**8 version was released in 1993.
* Red Hat Linux was proposed in 1994. Caldera was detected by Ransom love and Bryan Sparks and NetBSD 1.0 version published.
* HP-UX 10.0 version and FreeBSD 2.0 version was released in 1995.
* K Desktop Environment was established by **Matthias Ettrich** in 1996.
* HP-UX 11.0 version was released in 1997.
* The IRIX 6.5 version, i.e., the fifth SGI UNIX generation, Free BSD 3.0 version, and Sun Solaris 7 OS was released in 1998.
* The **Caldera System** agreement with professional services division and SCO server software division was released in 2000.
* **Linus Torvalds** published the Linux version 2.4 source code in 2001.
* **Microsoft** filed the Trademark collection against Lindows.com in 2001.
* Lindows name was modified to Linspire in 2004.
* The first publication of **Ubuntu** was published in 2004.
* The openSUSE project started a free distribution from the community of **Novell** In 2005.
* **Oracle** published its Red Hat distribution in 2006.
* **Dell** begun laptop distribution with Ubuntu which was pre-installed on it in 2007.
* Linux kernel version 3.0 was released in 2011.
* Linux-based android of Google insisted 75% of the market share of the Smartphone, based on the number of phones exported in 2013.
* Ubuntu insisted on 20000000+ users in 2014.

Architecture of Linux system



The Linux operating system's architecture mainly contains some of the components: **the Kernel, System Library, Hardware layer, System,** and **Shell utility**.

**1. Kernel:-** The kernel is one of the core section of an operating system. It is responsible for each of the major actions of the Linux OS. This operating system contains distinct types of modules and cooperates with underlying hardware directly. The kernel facilitates required abstraction for hiding details of low-level hardware or application programs to the system. There are some of the important kernel types which are mentioned below:

* Monolithic Kernel
* Micro kernels
* Exo kernels
* Hybrid kernels

AD

**2. System Libraries:-** These libraries can be specified as some special functions. These are applied for implementing the operating system's functionality and don't need code access rights of the modules of kernel.

**3. System Utility Programs:-** It is responsible for doing specialized level and individual activities.

**4. Hardware layer:-** Linux operating system contains a hardware layer that consists of several peripheral devices like [CPU](https://www.javatpoint.com/central-processing-unit), [HDD](https://www.javatpoint.com/hdd), and [RAM](https://www.javatpoint.com/ram).

**5. Shell:-** It is an interface among the kernel and user. It can afford the services of kernel. It can take commands through the user and runs the functions of the kernel. The shell is available in distinct types of OSes. These operating systems are categorized into two different types, which are the **graphical shells** and **command-line shells**.

The graphical line shells facilitate the graphical user interface, while the command line shells facilitate the command line interface. Thus, both of these shells implement operations. However, the graphical user interface shells work slower as compared to the command-line interface shells.

There are a few types of these shells which are categorized as follows:

* Korn shell
* Bourne shell
* C shell
* POSIX shell

33.architecture of [Windows](https://en.wikipedia.org/wiki/Windows_NT)

The architecture of [Windows NT](https://en.wikipedia.org/wiki/Windows_NT), a line of [operating systems](https://en.wikipedia.org/wiki/Operating_system) produced and sold by [Microsoft](https://en.wikipedia.org/wiki/Microsoft), is a layered design that consists of two main components, [user mode](https://en.wikipedia.org/wiki/User_space) and [kernel mode](https://en.wikipedia.org/wiki/Protection_ring#SUPERVISOR-MODE). It is a [preemptive](https://en.wikipedia.org/wiki/Preemption_(computing)), [reentrant](https://en.wikipedia.org/wiki/Reentrancy_(computing)) [multitasking](https://en.wikipedia.org/wiki/Computer_multitasking) operating system, which has been designed to work with [uniprocessor](https://en.wikipedia.org/wiki/Uniprocessor_system) and [symmetrical multiprocessor](https://en.wikipedia.org/wiki/Symmetric_multiprocessing) (SMP)-based computers. To process [input/output](https://en.wikipedia.org/wiki/Input/output) (I/O) requests, they use packet-driven I/O, which utilizes [I/O request packets](https://en.wikipedia.org/wiki/I/O_request_packet) (IRPs) and [asynchronous I/O](https://en.wikipedia.org/wiki/Asynchronous_I/O). Starting with [Windows XP](https://en.wikipedia.org/wiki/Windows_XP), Microsoft began making [64-bit](https://en.wikipedia.org/wiki/64-bit_computing) versions of Windows available; before this, there were only [32-bit](https://en.wikipedia.org/wiki/32-bit) versions of these operating systems.

Programs and subsystems in user mode are limited in terms of what system resources they have access to, while the kernel mode has unrestricted access to the system memory and external devices. Kernel mode in Windows NT has full access to the hardware and system resources of the computer. The Windows NT [kernel](https://en.wikipedia.org/wiki/Kernel_(operating_system)) is a [hybrid kernel](https://en.wikipedia.org/wiki/Hybrid_kernel); the architecture comprises a [simple kernel](https://en.wikipedia.org/wiki/Architecture_of_Windows_NT#Kernel), [hardware abstraction layer](https://en.wikipedia.org/wiki/Hardware_abstraction) (HAL), drivers, and a range of services (collectively named [Executive](https://en.wikipedia.org/wiki/Architecture_of_Windows_NT#Executive)), which all exist in kernel mode.[[1]](https://en.wikipedia.org/wiki/Architecture_of_Windows_NT#cite_note-FOOTNOTEFinnel2000Chapter_1:_Introduction_to_Microsoft_Windows_2000,_pp._7%E2%80%9318-1)

User mode in Windows NT is made of subsystems capable of passing I/O requests to the appropriate kernel mode [device drivers](https://en.wikipedia.org/wiki/Device_driver) by using the I/O manager. The user mode layer of Windows NT is made up of the "Environment subsystems", which run applications written for many different types of operating systems, and the "Integral subsystem", which operates system-specific functions on behalf of environment subsystems. The kernel mode stops user mode services and applications from accessing critical areas of the operating system that they should not have access to.

The Executive interfaces, with all the user mode subsystems, deal with I/O, object management, security and process management. The kernel sits between the hardware abstraction layer and the Executive to provide multiprocessor synchronization, [thread](https://en.wikipedia.org/wiki/Thread_(computing)) and interrupt scheduling and dispatching, and trap handling and exception dispatching. The kernel is also responsible for initializing device drivers at bootup. Kernel mode drivers exist in three levels: highest level drivers, intermediate drivers and low-level drivers. [Windows Driver Model](https://en.wikipedia.org/wiki/Windows_Driver_Model) (WDM) exists in the intermediate layer and was mainly designed to be binary and source compatible between [Windows 98](https://en.wikipedia.org/wiki/Windows_98) and [Windows 2000](https://en.wikipedia.org/wiki/Windows_2000). The lowest level drivers are either legacy Windows NT device drivers that control a device directly or can be a [plug and play](https://en.wikipedia.org/wiki/Plug_and_play) (PnP) hardware bus.

4.Password policy

A password policy defines the password strength rules that are used to determine whether a new password is valid.

A password strength rule is a rule to which a password must conform. For example, password strength rules might specify that the minimum number of characters of a password must be 5. The rule might also specify that the maximum number of characters must be 10.

A password policy sets the rules that passwords for a service must meet, such as length and type of characters allowed and disallowed. Additionally, the password policy might specify that an entry is disallowed if the term is in a dictionary of unwanted terms. To select this choice in the user interface, you must first load a dictionary.ldif file into the IBM® Security Privileged Identity Manager.

You can specify the following standards and other rules for passwords:

* Minimum and maximum length
* Character restrictions
* Frequency of password reuse
* Disallowed user names or user IDs
* Specify a minimum password age