NAMA : Fikri Anggra Berlian

NIM : L200174090

KELAS : X

OPERATION SYSTEM

1.

**Advantages and Disadvantages of windows**  
**Advantages**  
• Stability: Windows 7 is the most stable Windows Operating systems ever.  
• Software Library: Windows OS has the largest sized software library than any other OS. This indicates that the bulk of programs, applications, and games out there are designed for Windows. Production Packages like Microsoft Office are generally offered on Windows first.   
• Technical Support: You would not have any difficulties finding support.

**Disadvantages**  
• Viruses: You could need to purchase an anti-virus software.  
• Slow: Windows, especially Vista and 7, needs a lot of computer sources (memory, processor, disk space), and thus, runs slower.  
• You're going to require service.

**Advantages and Disadvantages of Mac**  
**Advantages**  
• Viruses: Apple Macs get nearly no viruses. This is mainly due to Window's outstanding business.  
• Reliability: Macs only run on Apple computers, and as a result, fewer prone to hardware and software crashing.  
• Looks: Most of the time, Mac just looks better as compared to Windows.

**Disadvantages**  
• Stability: OS X can crash just as frequently as a Windows OS. In fact, OS X crashes much more when you're running non-Apple authorized software like Adobe Flash or Audacity.  
• More pricey upfront than other options. Some would say this is offset by less maintenance required over the life of the device.  
• More complex than Windows due to its UNIX base. This actually isn’t a major disadvantage because OSX really does a good job of hiding this complexity from the end user.  
• Less support. You need to visit Apple for all your hardware issues.  
Mac has never been known for its gaming compatibility, even though the computers are greatly powerful. Moreover, several some other applications usually do not run on the Mac PC.

**Advantages and Disadvantages of Linux**  
**Advantages**  
• Price: Linux is FREE. You can download it, install it, use it, modify it... All for a whopping 0$.  
• Viruses: Although being more vulnerable to viruses than Mac (because it is open source), Linux still has very few viruses. (more secure than Windows XP and even OSX)  
• Full access to the totally free open source library of software. Excellent full featured, compatible, and no cost replacements for your proprietary software.  
• Much more options than any other system.

**Disadvantages**  
• Compatibility: The latest and greatest hardware is usually slower to reach Linux.  
• Vendors: You will not find plenty of vendors selling Linux computers. Generally, you will just end up having to purchase Windows computer, reformatting the hard drive, and installing Linux yourself.  
• Linux is fairly more complex than Mac or Windows.

**Advantages and Disadvantages of Sun Solaris**  
**Advantages**

• Free Redistribution so that everyone can buy or give to others

• Derived Work, the user can change the existing code on Sun Solaris and redistribute to the public

• No Discrimination in the code must be made available to everyone in order to be developed and refined

• ZFS is a system restore which is almost similar to the restore on windows

• Can integrate with AMP stack (Apache, MySQL and PHP) to run a web server

Stable file system for data base   
  
**Disadvantages**

• The price is quite expensive commercial operating system

• Driver hardware unfavorable

• Sun Solaris operating system is not as good as free sun solaris operating

• Systems are commercial (paid)

2.

**Worms**  
This malicious program category largely exploits operating system vulnerabilities to spread itself. The class was named for the way the worms crawl from computer to computer, using networks and e-mail. This feature gives many worms a rather high speed in spreading themselves.   
  
**Viruses**  
Programs that infected other programs, adding their own code to them to gain control of the infected files when they are opened. This simple definition explains the fundamental action performed by a virus - infection.  
  
**Trojans**  
Programs that carry out unauthorized actions on computers, such as deleting information on drives, making the system hang, stealing confidential information, etc. This class of malicious program is not a virus in the traditional sense of the word (meaning it does not infect other computers or data). Trojans cannot break into computers on their own and are spread by hackers, who disguise them as regular software. The damage that they incur can exceed that done by traditional virus attacks by several fold.  
  
**Spyware**  
Software that collects information about a particular user or organization without their knowledge. You might never guess that you have spyware installed on your computer.  
  
**Riskware**  
Potentially dangerous applications include software that has not malicious features but could form part of the development environment for malicious programs or could be used by hackers as auxiliary components for malicious programs.  
  
**Rootkits**  
Utilities used to conceal malicious activity. They mask malicious programs to keep anti-virus programs from detecting them. Rootkits modify the operating system on the computer and alter its basic functions to hide its own existence and actions that the hacker undertakes on the infected computer.

3.

**Windows**

Windows Defender Advanced Threat Protection (Windows Defender ATP) is a unified platform for preventative protection, post-breach detection, automated investigation, and response. Windows Defender ATP protects endpoints from cyber threats; detects advanced attacks and data breaches, automates security incidents and improves security posture.

**Linux**

The latest Linux threats highlight the importance of securing the system just like any other system in the enterprise network. Server administrators and system admins should use a multi-layered approach as it is not enough to exclusively rely on network security; endpoint attack vectors such as smartphones must also be secured where possible. [Trend Micro Server Protect](https://www.trendmicro.com/us/enterprise/cloud-solutions/server-protection/) effectively protects against malware, rootkits, and other data-stealing malware while simplifying and automating security operations on Linux servers, and storage systems.

[Trend Micro Deep Security](https://www.trendmicro.com/us/enterprise/cloud-solutions/deep-security/index.html) can also protect Linux servers from attacks like [Fairware](http://blog.trendmicro.com/web-site-offline-new-server-focused-fairware-ransomware/). It protects enterprise file servers—which house large volumes of valuable corporate data from attacks via a compromised end user, alerting administrators, and stopping suspicious activity in its tracks. It also provides early detection of an attack, including brute force and lateral movement from server to server, enabling immediate action to be taken to mitigate the potential impact.

**Mac OS**

[Defendpoint for Mac](https://www.avecto.com/resources/%7BlocalLink:4724%7D) addresses the challenge of enterprise Mac management by introducing [Privilege Management](https://www.avecto.com/resources/%7BlocalLink:4693%7D) and [Application Control](https://www.avecto.com/resources/%7BlocalLink:4717%7D) on OS X. With this [least privilege approach](https://www.avecto.com/resources/%7BlocalLink:4693%7D), Mac devices can achieve the same level of protection available in the Windows environment.

With Defendpoint for Mac, users are able to run admin tasks and privileged applications without the need for an admin account. [Admin rights](https://www.avecto.com/resources/%7BlocalLink:4786%7D) are assigned directly to the applications, tasks and content as and when they are needed. This allows businesses to regain control of applications with pragmatic whitelisting rules that trust the build, ensuring that only known good applications are able to run while users have the freedom and flexibility to perform everyday tasks.

**Sun Solaris**

System administrators can detect possible attacks on their systems by monitoring for changes to file information. In the Oracle Solaris 10 OS, binaries are digitally signed, so administrators can track changes easily, and all patches or enhancements are embedded with digital signatures, eliminating the false positives associated with upgrading or patching file integrity-checking software.

The Oracle Solaris 10 OS also introduces the Basic Audit and Reporting Tool (BART), a file integrity-checking application for data files and customer applications. The BART utility allows a customer to create snapshots of their own data, applications and critical system files and periodically scan for changes to these files. Additionally, the Solaris Fingerprint Database project, previously hosted by Sun on the SunSolve Web site, provides digital fingerprints for all files shipped in the Solaris OS, spanning many previous generations of the operating system. The Solaris Fingerprint Database offers free online verification utilities that allow you to check the integrity of Solaris files on any existing system to ensure that no hacker has modified critical system files. Used individually or together, these file integrity tools provide powerful, flexible ways to monitor for changes to your operating system platform.