OLD DOMINION UNIVERSITY

CYSE 601 ADVANCED CYBERSECURITY TECHNIQUES AND OPERATIONS

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Security Measures and Weaknesses in Linux, Windows, and MacOS

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Steven Latino, 01160745

2020 Spring

**Abstract**

**Introduction**

As technology continues to advance faster every day; security and vulnerabilities become much more relevant in today's society! Modern computers require modern security configurations to protect computers from vulnerabilities. Windows, macOS, and Linux have their own security configurations to make the Operating System stronger. Some of these security configurations are different from others. These configurations can start from the computer boot up with BitLocker and Luks, to in the middle of validating a website. While security improves over time, new vulnerabilities are being developed too. That is why patching your system and having a virtual private network (VPN) available can help secure a user's computer.

**Linux**

In the Linux operating system, it uses group and user ownership to control who has access to certain files. Linux also has several firewalls available to use such as UFW, Iptables, firewalld, and others. These filter traffic coming into the computer and traffic that is going out of the computer. SELinux is also a very helpful security feature in Linux. It provides FIPS security to help increase the security of the Linux Operating System. Services should usually be turned on if needed. If a service is turned on, but not used, this could be an exploit for a hacker to use. Linux is usually a strong operating system but has come with some security vulnerabilities over the past couple of years such as EvilGnome and ShellShock. These vulnerabilities harm the Linux system by using some bash commands to hurt the Linux Operating System.

**macOs**

With the macOS Operating System, as long as you have your firewall on and your anti-virus running Mac also has a feature of finding your computer if it is stolen by enabling the Find My Mac program. Users use internet browsers too. That's why a Macintosh user should use private mode to protect your privacy and a VPN so none of the user's traffic gets captured by someone maliciously. You should also create a secondary account, so a malicious user doesn't have full access to your computer. Some features can be potentially vulnerable if manipulated correctly such as the AutoFill feature. When the Autofill packets are captured they can be manipulated to paying for different things or generating a pass-code for Multi-Factor authentication.

**Windows**

Windows is a closed-source operating system. One of the security features in this operating system includes its firewall, which helps filter certain things coming in and out of the computer. Another is the anti-virus which helps protect the Windows computer from malicious activities. Windows also has a GUI administrative tool called AppLocker that controls the permissions of files and folders. Bitlocker is also an important tool in Windows security. This tool helps encrypt the hard drive so malicious hackers can't change anything in the firmware settings. Windows also has security issues. Reverse-shells are one issue that hackers exploit on Windows systems. These reverse-shells can be created by using malicious programs to create a Windows executable file. This doesn't automatically guarantee administrative access, but it gets the attacker a starting point. Software coded incorrectly or not with security in mind can create zero-day attacks. These types of attacks could completely ruin the computer itself and make it unusable. This is why patching the system is a great way to avoid any vulnerabilities.

**Summary of Articles**

**Linux**

***Security***

Linux security comes from how you configure the Linux Operating system. You could use firewalls or IPtables to configure what packets go through the system and what comes out. Other services, such as ssh, samba, or an LDAP server, are very similar by configuring security for that service. You have to go into a file and edit the features that serve the best security for you and/or the company.

**Firewalls.** Firewalls are set up to allow things to pass through and out of your computer like a filter. The two common command-line interface (CLI) firewalls that you can set up for Linux are firewalld, and Iptables. There is also graphical user interface (GUI) options such as the UFW which makes adding firewall rules easier for new Linux users. IPtables is a more complicated firewall more for the use of servers. With firewalld, the service will start automatically and block most protocols. You can change this by adding a port through the command line or using the GUI. An example of this command would be firewall-cmd –permanent –add-port=*portnumber/tcp/|udp*. With iptables, there is an input filter and an output filter. The input filter controls the incoming connections while the output filter controls the connections going out. When configuring iptables, you have to specify certain characteristics with the command such as if the rule is input or output, what port it is using, the domain or IP address, and rather or not to accept it or drop it. So an iptable command would look something like the following: iptables -A INPUT|OUTPUT -p tcp -d bigmart.com -s 10.0.3.1 --dport 22 -j ACCEPT|DROP. (open-source, 2018)

**SElinux and Permissions.** Most services require some configuration changes since scanners look for default configuration to manipulate and gain access to. These configuration changes on services can be ssh, LDAP, smb, or others. A lot of this can be safely configured by using SELinux. SELinux is the security implementation that enhances the security of the Linux computer. If the said computer is breached, it will stop the attack from spreading further. SELinux has three modes: Disable, Permissive, and Enforcing. If SELinux is disabled, SELinux is then turned off. If it's in permissive mode, SELinux will only monitor interactions with the computer it is on. Enforcing SELinux will filter with configured security policies and create logs. (IEEE, 2020) Switching modes will require a reboot. Configuring roles for files and folders will allow certain users specified to access the information.

***Vulnerabilities***

While Linux is a very secure Operating System, it is capable of having vulnerabilities within it. Two vulnerabilities that have happened in the past decade are EvilGnome and Shellshock. EvilGnome is a remote code vulnerability that executes code to gain information about the machine while shellshock can execute shell commands if an attacker intercepts some packets. A remote code execution attack is a cyberattack that can change the computer's configuration without the computer's owner knowing and without authorization. This attack is very dangerous.

**EvilGnome.** In 2019, the Gnome Linux desktop environment experienced a malicious attack in its environment called EvilGnome. The payload file starts in a single file that contains 522 lines of shellcode. What this script does is What payloads do. If the EvilGnome self-extractor runs, there should be a directory in the ~/.cache/gnome-software/ called gnome-shell-extensions. In it, there will be two malicious files called gnome-shell-ext and gnome-shell-ext.sh. The gnome-shell-ext is a C++ program which has three function: takeSound(), takeScreenshot(), and scanFolder(). The takeSound function records audio and uploads it, the takeScreenshot takes screenshots of the victim's machine, and the scanFolder looks for files to steal. The ShooterKey function is the most dangerous function within EvilGnome. It communicates back to the hacker and can download new malware and execute it. This allows the payload to make a zombie out of the victim's machine. EvilGnome also creates a cronjob that runs every time it crashes or is killed. It looks like the following: **0-59 \* \* \* \* /.cache/gnome-software/gnome-shell-extensions/gnome-shell-ext.sh**. What you need to do is remove the cronjob and any processes or files that have the gnome-shell-ext in it. (Sophos, 2019)

**Shellshock.** Shellshock or CVE-2014-6271 was a Linux vulnerability in 2014 that causes bash to execute commands from variables unintentionally. This means this vulnerability is a remote code execution exploit. How this exploit works is the hacker sends commands through HTTP requests from the webserver. Once the webserver receives the requests, it will execute the bash commands. An example of a malicious HTTP request looks like the following :

GET http://shellshock.testsparker.com/cgi-bin/netsparker.cgi HTTP/1.1  
User-Agent: Netsparker  
Host: shellshock.testsparker.com  
Referer: () { :;}; echo "NS:" $(</etc/passwd)

Once the webserver receives the HTTP request it will send the output of the command to the HTTP website. (netsparker, 2017)

**MacOS**

***Security***

In the Mac Operating System, there are different but similar features compared to the Linux and Windows Operating Systems. A virtual private network (VPN) is a strong way to encrypt your packets from one machine to another. This is a great option if you are using public wifi and don't want your data stolen. Macs are vulnerable to viruses because it has become a popular Operating System. This is why Mac users need to have a good Anti-virus installed. You could choose an antivirus such as McAfee, Norton, Bitdefender, or others to protect your computer from trojans and worms. You should also turn on your firewall. You can do this by going to the **System Preferences => Security & Privacy** tab. Click on the **Firewall** tab. Then click on the lock icon in the bottom left corner of the window and enter your administrator password. Then click **Turn On Firewall**. (macpaw, 2019) Mac users should also create a firmware password to secure their computers. If a malicious person has access to the firmware settings, they could change just about anything on the victim's computer. A Mac user should also create a secondary account besides root to use. If the root account is compromised, then root could add or delete files, folders, users, and groups that may not be able to recover. An example account that most system administrators do is create a user called sysadmin that is very similar to root. Mac computers have a software feature called Find My Mac. This feature allows you to track your computer if a criminal(s) stole it. (Computerworld, 2020) To do this you need to first turn on Location Services. Then to setup Find My Mac go to **System Preferences** and click **Apple ID**. Click **iCloud**, and then select **Find My Mac**. If you are asked to use the location of your mac, select **Allow**.

***Vulnerabilities***

While security in macOS is better than Windows, macOS is still capable of being vulnerable to attacks. A man-in-the-middle attack is where the hacker secretly relays and/or alters the packets between the sent party and the receiving party. The user sending the packet has no idea anything is being intercepted. The Autofill vulnerability is a man-in-the-middle attack that is capable of stealing money or an access code.

**Autofill.** The Mac Operating System has a SecurityCode Autofill feature that can be used to automatically fill in security codes and payment information. In this scenario, the SecurityCode AutoFill was used in a manipulated in a man-in-the-middle attack. In a man-in-the-middle attack, the hacker is in the middle of the network traffic and either edits or replaces certain packets. In this scenario, the attacker intercepts the SecurityCode AutoFill packet that was being used to pay for Item A and then uses it to pay for item B that the hacker may want. The vulnerability exposed only affected Mac's with an iOS of 12 or below. (discovery.ucl.ac.uk, 2019)

**Windows**

***Security***

The article made by Microsoft talks about ways to protect a Windows computer. A firewall is a good way to filter traffic coming out of a user's computer and traffic that is coming to your computer. On the Windows Operating systems, only Windows 8 and up have it built-in by default. You can add or edit the default rules on the Windows firewall. An administrator should always keep the workstation or server's software up to date with patches. Unpatched software can be exploited by hackers by using port scanners. For emails, make sure to not open anything that has suspicious attachments. Hackers use fake attachments to create reverse-shells for them to exploit the Operating System. You should also keep a strong password. The weaker the password is, the faster a hacker can decrypt it and use it to login into said user. Also having a good anti-virus and scanning your system can help remove and protect your system from malicious trojans and worms. (support.microsoft, 2020)

**AppLocker.** AppLocker is a Windows program that makes software restriction policies. This program allows you to make software restriction policies. These policies either allow or deny applications based on a certain criterion of a file(s) or application(s). Some technology researchers put a malicious program on a Windows machine. When they used AppLocker, it blocked the virus 100% of the time. (IEEE, 2017)

**BitLocker.** Bitlocker is Microsoft's, proprietary encryption program to encrypt a computer's hard drive, as well as protect the firmware-level from malicious malware. It's available on Windows Vista and up. You need to have two partitions and a Trusted Platform Module (TPM) installed. The standard version of Windows doesn't come with BitLocker. To setup Bitlocker, go to **Control Panel**, and then **System and Security**. The user would then need to select **BitLocker Drive Encryption**. You would then click **Turn on BitLocker** to start configuring the BitLocker encryption. (PCWorld, 2016)

***Vulnerabilities***

Windows is a popular Operating System which is known to have vulnerabilities with it. Some vulnerabilities within this operating system only work depending on how much the user is aware of the exploit. In a reverse shell, an attacker can create a fake file to exploit the system. Some other vulnerabilities don't require much of the user and can be exploited because of the way it was programmed because the code was never addressed correctly. This vulnerability situation is called a Zero-Day attack.

**reverse-shell.** Users in the Windows Operating System usually have to be careful about reverse-shell attacks. Hackers can use Metasploit to gain remote access by creating a malicious program. A Hacker can create a fake .exe program by either using just msvenom or adding Shelter to this process. With Shelter, it allows the malicious .exe to not be detected by any of the anti-viruses installed on the target Windows computer. Usually, when hackers do this, they will create a fake website for the victim, so they can download the malicious payload. Once the payload is executed, the hacker gains access. The user then has to do more hacks to escalate to a higher privileged user. Once the hacker has privileged access, the hacker creates new user accounts and a backdoor to have a way to remote in forever.

**Zero-Day Attack.** Windows can be attacked by zero-day vulnerabilities too. In a recent vulnerability, Adobe Type Manager (ATM) could create a zero-day exploit on Windows computers. Attackers could exploit this by persuading users to open a malicious document. The payload can still be exploited by using the Windows File Explorer file manager preview feature. As of the article's published date, there is not any patch available to fix this exploit, but there is a workaround to stop the File Explorer's preview feature from being exploited. The workaround was done by going to **File Explorer** and clicking the **View** tab. You then need to deselect both the **Details** and **Preview** panes to turn them off. The user then needs to click **Options** and then click **Change folder and search options**. You then click the **View** tab again. The user then needs to select **Advanced settings** and check then check the **Always show icons, never thumbnails** box. The next step is disabling the WebClient. You go to the **Windows Services** application and click on the **WebClient** service. You then change the startup to **Disabled** and **stop** the service if it's already running. (Sophos, 2020)

**Your Thoughts**

**Linux**

Because Linux is open-source, the quickness of finding a vulnerability and patching it is quicker than other Operating Systems (OS) on the market. Instead of just limiting to a certain amount of people in a business, such as Microsoft and Apple, Linux has a whole community all around the world that can add and/or edit code and verify things. This is the true meaning of open-source. If a user doesn't like a security feature the desktop comes by default, Linux has other security solutions for that user to use. One of the security options that come with different programs is the Linux firewall. Besides the different firewalls, Linux has different desktop environments, anti-viruses, LDAP servers, and more. This is very useful in determining how an administrator would like to configure the security of the program. While Linux is not the most popular desktop environment, the firewall and anti-virus helps to keep it secured better. When an Operating System becomes more popular, more people use it and can discover more bugs and vulnerabilities in a program or operating system faster. This could be a factor in why the market statistics have shown that Linux is more secure than others. While the desktop environment may not be that popular to a regular user, Linux is more capable of handling being a common desktop environment. This is because of the community that Linux has in trying to make the OS the most secure and best operating system is the best on the market. Because Windows is closed-source, they are limited to just patching vulnerabilities and adding features within the Microsoft company, which might be the eventual downfall of the Windows desktop.

**MacOS**

macOS is a closed-source operating system made by Apple. This operating system was oringally open-source, but when the distro gain popularity, it became closed-source. This Operating System has some unique security features such as FindMyMac, and the firewall. While the firewall is installed automatically, it is not turned on by default, which may cause a security issue in the future. It is turned off because it does not have any ports on the host computer because it isn’t hosting anything. If there was a malicious reverse-shell attack where the hacker installed netcat and turned on as many ports as possible, a regular user would have no idea, and it would be extremely hard to detect. The FindMyMac is an excellent feature in Mac computers. If a user’s Mac computer ever got stolen, you can find it through this program. The program uses GPS to locate the computer. Depending on the view on the super user, this could be both a good or bad thing. A hacker could abuse the GPS tracking of a Mac computer, to track where the user goes. This is what some governments do with phones with GPS turned on. On the positive end, this would be a great feature on other Operating Systems such as Windows and Linux. Mac is very similar to Linux and could have the same security configurations pushed as a Linux server or workstation. While Mac is gaining popularity, there has been an increase in security exploits for that Operating System. Mac, just like Linux, has the potential to end the Microsoft Windows desktop system, but will never, at this point in time, take the lead in server infrastructures. This is because Apple never developed their server Operating System to its full potential.

**Windows**

Windows is a closed-source operating system owned by Microsoft. This operating system was one of the first operating systems to be used on a computer. They have a firewall installed, which is on by default, to protect the system from incoming packets and outgoing packets. You can use Microsoft's Security Essentials antivirus to protect the Windows computer against malware. You can also use other antiviruses to protect the Windows computers against viruses such as McAfee, BitDefender, Avast, and others that are known to be better than Microsoft's anti-virus. Windows is also more likely to receive malware since most malware execute with .exe files. With msfvenom, there will always be some sort of way to create a reverse-shell on a Windows system. Any exe program can be copied to create a malicious exe file. In one case, you could create a fake putty program with a .exe file, and the .exe file will run like normal. The only difference is, there is an extra payload to give the attack a reverse-shell. It would help the Windows operating system if they moved to a shell-based system. If Windows did this, it might hurt the other operating systems that use a shell, since Windows is so popular. If Windows's moved to a shell-based system, this would result in Mac and Linux systems having more vulnerabilities and they would have to create stronger anti-viruses for their systems. Some systems might even take an alternative route and switch from using bash to a different object-oriented language. Zero-Day attacks will always be an issue for any operating system. These are attacks that are new to the public and take time to figure out a solution to the exploit. Because Windows is more widely used, it is more likely in the future that there will be more Zero-Day attacks on the system. There are some applications that can be only used on a Windows system, because of the .exe extension, which is why Microsoft Office and other Microsoft Applications, could see zero-day attacks in the future.

**Potential**

If Linux and the Mac community work together, they could potentially beat out Microsoft. Linux would need some of Mac’s marketing and advertising help, while Mac could use the Linux server software to improve their server infrastructure. Unfortunately for Linux, this won’t happen anytime soon, since the Linux Foundation has Microsoft in it. Because of that, Linux will have to take suggestions from Windows. The only comment made to why Microsoft did this is because they have been putting open-source code out there for a couple of years now. This could also be because they want to incorporate Microsoft features in their Operating System. They have already incorporated Ubuntu for Windows as a software package in their Windows Store. With all that being stated, this could increase Windows security and potentially put Mac out of business since Mac is very similar to Linux. What Microsoft could do to achieve this is to slowly start making their operating system into a shell based system. Then when you first install it, you select the options for a certain firewall, antivirus, mailing application, desktop environment, and others to use for the system. This would make Windows feel like it accomplished a brand new Operating System for Windows users. This could also benefit Linux, by allowing the system to execute .exe files. This could make the .exe file extension securer and would make the Linux OS much more compatible with other applications.   
 If that scenario did come true, this would make Linux, Windows, and macOS all vulnerable to the same exploits. This may be useful having the same features because this will cause every Operating System to quickly patch their system and work together to solve the issue. This might make patching easier on all the Operating System since different developers can split patching the system. Could there be one day unity between Linux, Microsoft, and Mac? Maybe, but it might take a while before anyone truly sees this. If they did combine together, they could combine the best server and desktop capabilities of all their operating systems, and put together an ultimate Operating System for people to use. This big ultimate Operating System however, could create new security issues for them to resolve.

**Conclusion**

To sum everything up, each Operating System has it's own security features and vulnerabilities. When a user or administrator turns on the firewall on Microsoft's Windows, Apple's Mac, or Linux it allows the computer to filter what packets come into the computer and what packets go out of the computer. Some operating systems need Anti-viruses too. With Windows and Apple, you need such protection so no malware can infect and harm your computer. Linux doesn't need this, but it is optional because its code is always updated and secure. There are also many different exploits available to use against the Windows, macOS, and Linux operating systems. A hacker can perform a man-in-the-middle attack and steal money just like the AutoFill exploit security researchers found. And an Operating System code could create a reverse shell to control a target computer such as Shell Shock with Linux. A computer could have software on it that creates a whole new type of exploit such as the Adobe Zero-Day attack on Windows. There will always be security within the computer and there will always be vulnerabilities within them too.

Preferences

**Windows**

Microsoft. (2020) Keep your computer secure at home - Windows Help. Retrieved May 18, 2020, from <https://support.microsoft.com/en-us/help/4092060/windows-keep-your-computer-secure-at-home>

Rohan, Durve. (2020) IEEE Xplore Full-Text PDF:. Retrieved May 18, 2020, from [**https://ieeexplore-ieee-org.proxy.lib.odu.edu/stamp/stamp.jsp?tp=&arnumber=8090399**](https://ieeexplore-ieee-org.proxy.lib.odu.edu/stamp/stamp.jsp?tp=&arnumber=8090399)

Ian Paul. (2016) A beginner's guide to BitLocker, Windows' built-in encryption tool | PCWorld. Retrieved May 30, 2020, from <https://www.pcworld.com/article/2308725/a-beginners-guide-to-bitlocker-windows-built-in-encryption-tool.html>

A Trusted Or. (2020) Critical Vulnerabilities in Microsoft Windows Operating Systems | CISA. Retrieved May 18, 2020, from [**https://www.us-cert.gov/ncas/alerts/aa20-014a**](https://www.us-cert.gov/ncas/alerts/aa20-014a)

Detecting Malicious Signatures. (2020) How to Attack Windows 10 Machine with Metasploit on Kali Linux. Retrieved May 18, 2020, from <https://resources.infosecinstitute.com/how-to-attack-windows-10-machine-with-metasploit-on-kali-linux/>

Dunn, J., Sims, K., Stockley, M., H, J., Ducklin, P., H., J., . . . Violet, A. (2020, March 26). Windows has a zero-day that won't be patched for weeks. Retrieved June 01, 2020, from <https://nakedsecurity.sophos.com/2020/03/25/windows-has-a-zero-day-that-wont-be-patched-for-weeks/>

**Linux**

Microsoft Word - Springer\_Guidelines\_for\_Authors\_of\_Proceedings.doc - pdf. (2020) Retrieved May 18, 2020, from [**https://iopscience.iop.org/article/10.1088/1757-899X/402/1/012062/pdf**](https://iopscience.iop.org/article/10.1088/1757-899X/402/1/012062/pdf)

The Malwares If. (2020) Architectural design for a secure Linux operating system - IEEE Conference Publication. Retrieved May 18, 2020, from <https://ieeexplore-ieee-org.proxy.lib.odu.edu/abstract/document/8299902>

Yueqi Chen, Xinyu Xing. (2020) SLAKE: Facilitating Slab Manipulation for Exploiting Vulnerabilities in the Linux Kernel. Retrieved May 18, 2020, from [**https://dl.acm.org/doi/pdf/10.1145/3319535.3363212**](https://dl.acm.org/doi/pdf/10.1145/3319535.3363212)

Clinton, D. (n.d.). Linux firewalls: What you need to know about iptables and firewalld. Retrieved June 01, 2020, from [https://open-source.com/article/18/9/linux-iptables-firewalld](https://opensource.com/article/18/9/linux-iptables-firewalld)

Ducklin, P., Alejandro, Varghese, S., EarlyMon, Xandronm, Crow, J., . . . Vaas, L. (2019, July 26). EvilGnome – Linux malware aimed at your desktop, not your servers. Retrieved June 01, 2020, from https://nakedsecurity.sophos.com/2019/07/25/evilgnome-linux-malware-aimed-at-your-laptop-not-your-servers/

https://www.netsparker.com/blog/web-security/cve-2014-6271-shellshock-bash-vulnerability-scan/

**MacOS**

Andreas Gutmann, Steven J. Murdoch. (2020) Taken Out of Context: Security Risks with Security Code AutoFill in iOS & macOS - Gutmann\_WAY\_2019.pdf. Retrieved May 18, 2020, from <https://discovery.ucl.ac.uk/id/eprint/10076464/1/Gutmann_WAY_2019.pdf>

Jonny Evans. (2020) Lock it down: The macOS security guide (updated) | Computerworld. Retrieved May 18, 2020, from <https://www.computerworld.com/article/3237187/lock-it-down-the-macos-security-guide-updated.html>

David Nield. (2020) The MacOS Catalina Privacy and Security Features You Should Know | WIRED. Retrieved May 18, 2020, from [**https://www.wired.com/story/macos-catalina-privacy-security-features/**](https://www.wired.com/story/macos-catalina-privacy-security-features/)

Stavniychuk, D. (2019, February 26). What happens when you enable or disable Firewall for Mac? Retrieved June 01, 2020, from <https://macpaw.com/how-to/use-firewall-on-mac>

Default. (2020) Your Mac’s Firewall is Off By Default: Do You Need to Enable It?. Retrieved June 09, 2020, from https://www.howtogeek.com/205108/your-mac%E2%80%99s-firewall-is-off-by-default-do-you-need-to-enable-it/