**Brian Jiang**

CS/IT 3530: Unix Operating System

Bjfkc

Security Issues with UNIX-Like systems

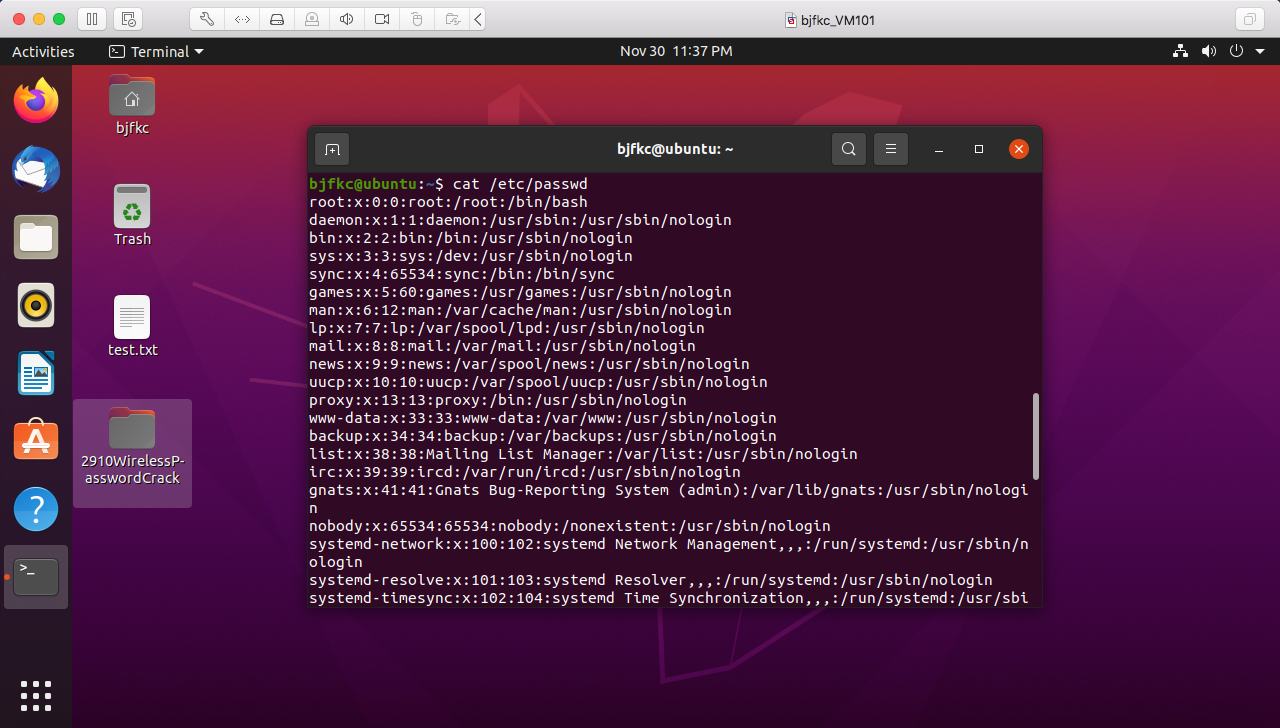
**Topic:**

There has been a variety of issues associated with operating system security. Issues regarding operating system security are common because computer users mess around with the operating system by debugging and programming which causes vulnerabilities in the code. The most common issues regarding operating system security are violations of Confidentiality, Integrity and Availability (CIA triad) where confidential data is being stolen along with compromised source code that can create security vulnerabilities. Security is an important role for Information Technology and that we need to keep our systems protected from vulnerabilities and hackers. For example, the hackers use password cracking tools, network/vulnerability scanners and intrusion detection software for a variety of tasks. So, the topic I chose is about Security issues with UNIX-like systems. UNIX-like systems are better than Microsoft Windows for security, however, there are still security issues for UNIX like Operating systems. This topic is relevant to what I want to do for my career along with my studies because without investigating issues regarding operating system security, the hackers will be out to steal people’s data and information.

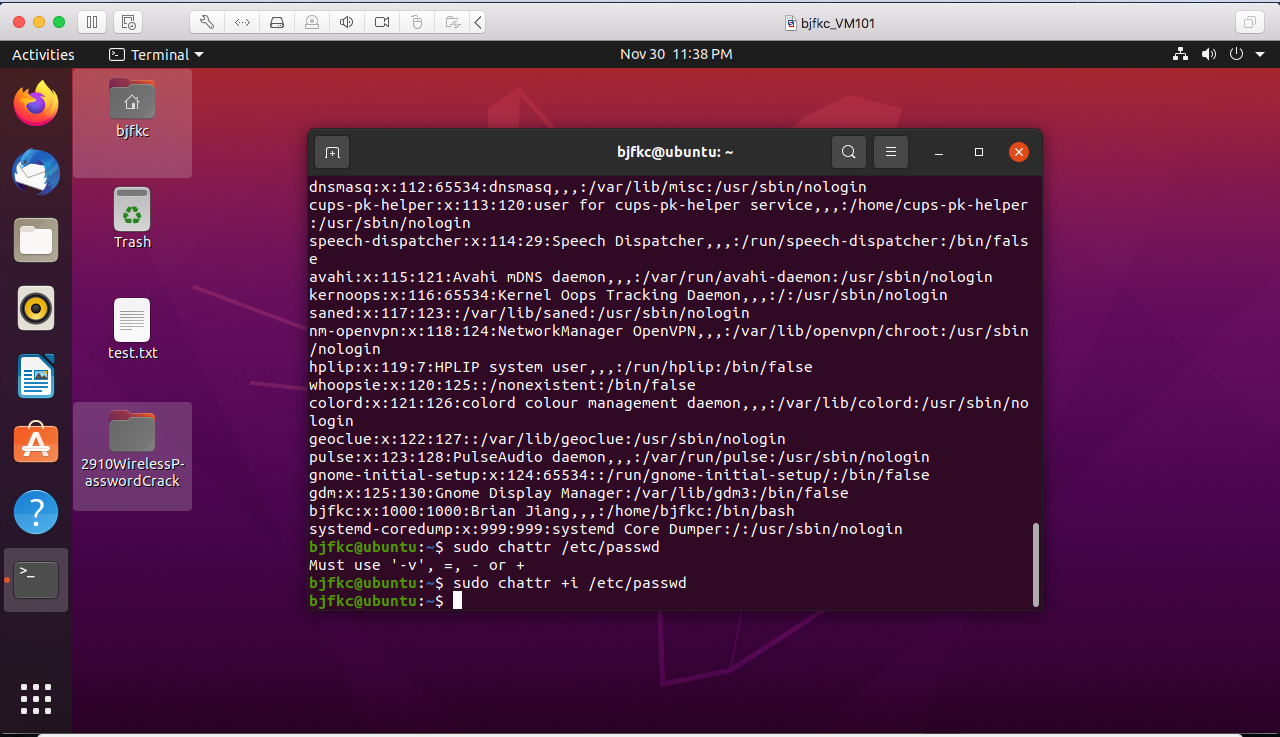
**Research:**

One of the most common risks with UNIX/Linux is that Linux is a very popular operating system for hackers because the source code that is made is available widely and that it’s an open source operating system which makes the operating system more vulnerable to hackers and can be simply modified. The hackers have the ability to utilize tools to utilize vulnerabilities in Linux based applications, software and networks. The most common categories of attacks for the security problems related to UNIX like systems are physical security attacks, social engineering attacks, dumpster-diving attacks and network and phone-based attacks. With physical security, it’s becoming tougher to prevent since the hacker can gain access to privileges that root users have. As a result, the hacker can steal data by logging packets and create analysis to find the user information. if users on your computer signs on to remote systems, the hacker doesn’t need access to the physical network. To resolve physical security, it’s best to check the system administration manual to make sure that you have the ROM-monitor security features that are given to you on your system and not purchase any systems that allow access without permission to the ROM-monitor. With social engineering, it’s gives the hacker an advantage to change one or more files that belong to specific user(s) so that it can have access to the account(s). An example of social engineering is to send emails to users who are not experienced which can result in changing the password to the one that the hacker specified. You can solve social engineering issues by being mindful of risks along with keeping your devices secure and raising your spam filters in addition to keeping your passwords safe. Lastly, we have dumpster-diving attacks where the hacker can have modem numbers that don’t exist along with lists of passwords that belong to the accounts that exist when you search through the company’s trash bins. These issues can be resolved by reviewing the waste paper that’s been trashed, media storage along with computer equipment that has been used at the company. The most important Linux security commands that you should know are sudo, visudo, who/w, last, find, file, which, iptables, ip, iproute, kill, passwd along with chattr. These commands are critical when it comes to performing tasks that an admin user would do. In addition, these commands are important when it comes to stopping the attacks that causes the issues with the security of the operating systems. Along with the security commands, you should protect your devices from application vulnerabilities, configuration vulnerabilities, login portal, insecure servers, network vulnerabilities, and internal compromises. In conclusion, UNIX systems are widely open to the public and that they are very risky for hackers to not use properly and that the threats come from physical access, gathering information along with accessing networks. The security issues with Unix/Linux can be resolved by using detection, prevention, and correction and that security is a process. Security issues can’t be solved with a one-time event, they require the capabilities to detect what’s going on with the security of the operating system.

**Application Portion:**



The password cracking screenshot demonstrates the social engineering attack that’s happening where the password for a user is retrieved using cat /etc/passwd in the command line.



The command chattr is used to protect user accounts from passwords getting cracked and where the social engineering attack is getting stopped.

**References/Sources:**

<https://www.veracode.com/security/linux-hacking>

<https://cmd.inp.nsk.su/old/cmd2/manuals/unix/UNIX_Unleashed/ch12.htm>

<https://mti.com/blog/2017/11/20/security-vulnerability-windows-unix-operating-systems/>

<https://phoenixnap.com/blog/prevent-social-engineering-attacks>

<https://www.mdsny.com/5-ways-to-prevent-social-engineering-attacks/>

<https://www.theamegroup.com/network-security-threats/>

<https://blog.corehealth.global/6-best-ways-to-prevent-privacy-and-security-vulnerabilities-in-wellness-technology>

<https://tipsmake.com/20-essential-linux-security-commands>

<https://linuxhint.com/install_aircrack-ng_ubuntu/>

<http://www2.cs.uic.edu/~jbell/CourseNotes/OperatingSystems/15_Security.html>

<https://www.cyberciti.biz/tips/howto-protect-account-against-password-crack-attack.html>