NORTHEASTERN UNIVERSITY

**Communication / Network Security**  
**TELE7374 / CSYE7374**  
**Fall 2023**

## LAB ASSIGNMENT 01 (DUE SEP 18)

### INTRODUCTION TO SECURITY

**NAME: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Bhavin Bhatia\_\_NUID 002981075\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

NOTE: Please submit screenshots or answers to demonstrate that you have completed the work. You will need a personal computer to complete the task. Good Luck!

**Lab 1.1. Online Research—Social Engineering by Threat Actors**

Task 1:

1. Open your web browser and go to <https://info.phishlabs.com/blog/brain-hacking-social-engineering-effective>.
2. Read the PhishLabs blog article, then list the four human natures that social engineering exploits. Include an example of a social engineering attack using each of the principles.

Answer:

**Reciprocity- Example the attacker may provide some kind of help to the target and in return the target feeling gratefull for thassistance , may become more likely to repay the favor or requests by the attacker. It can be any requests such as sharing personal identifiable information of certain people.**

Liking – Example people get easuly influenced these days . The attacker might use tacticks like sharing pictures of beautiful women to men and try to engage in fridly conversations and then exploit the target.

Consensus – Example Consulting companies sending spam emails that 100% guaranteed job placement , all of the others friends have already been placed into big tech companies.

Unity – Example the attacker may pretend to be your fellow employee or someone superior to gain your trust

Task 2:

1. Use your web browser to go to [www.dhs.gov/blog/2011/07/12/protect-yourself-against-social-engineering-attacks](http://www.dhs.gov/blog/2011/07/12/protect-yourself-against-social-engineering-attacks).
2. Read the guidelines given by the Department of Homeland Security on how to protect yourself from social engineering.
3. Use the list and guidelines to write two additional recommendations you would include in a policy to help protect your organization from a social engineering attack.

Answer:

-Keep strong password and multi factor authentication for important websites.

- educate others about these kinds of attacks . if you are aware of suck attacks then educate others with these kinds of attackers.

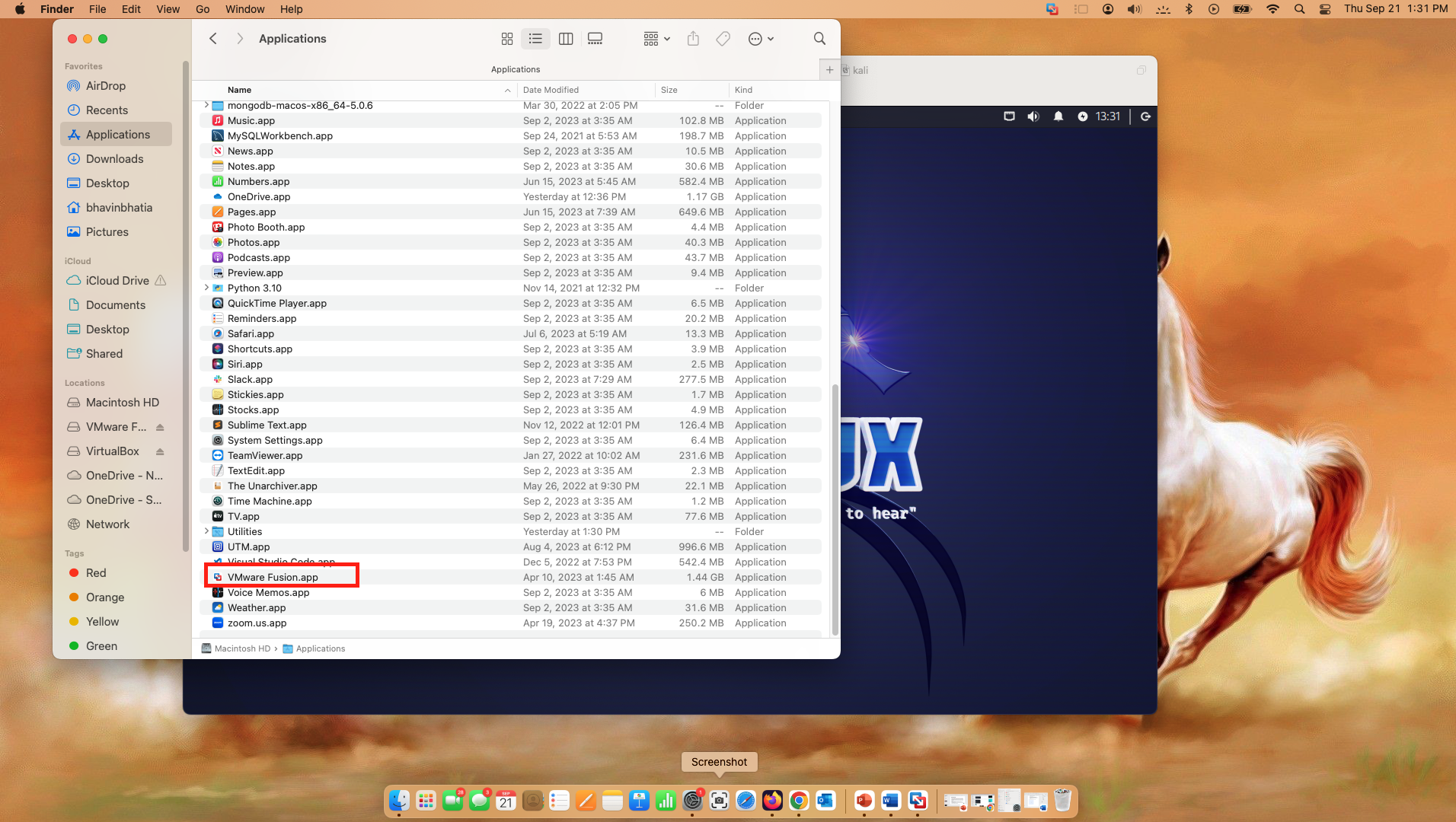
- auditing the security access so that unauthorized people never tailgate

- keep the track on the people enterging the critical rooms like server room in the office

**Lab 1.2. Creating a Windows 10 Virtual Machine for Security Testing**

1. Open your web browser and go to [www.vmware.com/products/workstation-player.html](http://www.vmware.com/products/workstation-player.html).
2. Click the **Download for Free** button.
3. Click **GO TO DOWNLOADS** next to Workstation Player 17.0, then click the **DOWNLOAD NOW** button for the correct operating system. Launch the executable file you downloaded to install VMware Workstation Player.
4. Click **Next** to continue the installation.
5. Check the box to accept the license terms and then click **Next**. Check the box for **Enhanced Keyboard Driver** and **add console tools into the system PATH**. Click **Next** until VMware Workstation Player is installed, and then click **Finish**.
6. Launch VMware Workstation Player, and then click **Continue** and **Finish**. The program prompts you for updates if any are available.
7. Close all windows.

Enter a screenshot of the VMWare Workstation shortcut on your desktop:



**Lab 1.3. Creating a Kali Virtual Machine for Security Testing**

1. Navigate to [www.7-zip.org](http://www.7-zip.org).
2. Click the **Download** link corresponding to your computer operating system, such as 64-bit x64 for Windows, and then save the file on your hard drive.
3. Launch the downloaded executable file for 7-Zip.
4. Click **Install** to install the 7-Zip file archiver, then click Close.
5. Navigate to [www.kali.org](http://www.kali.org).
6. Point to **Documentation** on the navigation bar and click **Kali Linux Documentation**.
7. Click **Introduction** on the Kali Docs page.
8. In the left pane, click **What is Kali Linux?** and then read about Kali Linux.
9. Point to **About Us** on the navigation bar, and click **Kali Press Release** to read more about Kali Linux.
10. Click **Downloads** on the navigation bar.
11. Scroll down to Kali Linux 64-Bit VMware and click **Offensive Security VM Download Page**.
12. Click **Kali Linux VMware 64-Bit** to download a pre-built virtual machine for VMware. Use 7-Zip to extract the files to a folder on your hard drive.
13. Open VMware Workstation Player.

1. In VMware Workstation Player, click **Open a Virtual Machine**.
2. Navigate to where you extracted the Kali virtual machine files, and click **Open**.
3. If prompted about moving or copying, select **I Copied It**.
4. Test the virtual machine by clicking **Kali Linux** in the left pane and selecting **Play Virtual Machine**.
5. Log in to the virtual machine using the username **kali** and password **kali**.
6. Explore the Kali Linux interface and environment and review the available tools.
7. Click **Terminal Emulator** on the Kali menu bar to open a terminal window.
8. Update your list of update repositories (where Linux gets its updates from) by typing **sudo apt update** and then pressing **Enter**.
9. The sudo command allows you to run commands with administrative privileges. Kali Linux will ask for your sudo password, which should be **kali**.
10. Perform a complete update by typing **sudo apt dist-upgrade** and pressing **Enter**.
11. When Kali Linux prompts you to continue, type **y** and press **Enter**; if you receive an additional prompt about restarting services, select **yes** and press **Enter**. Updating may take some time. (The window's lower-right corner shows the estimated time remaining for download.) Your terminal will return to the original prompt when the upgrades are complete.
12. Take a screenshot of the **Kali Linux Window**.
13. Close the VMware Workstation Player.

Enter the screenshot here:

**A screenshot of a computer

Description automatically generated**