# Keylogger

**Estimated Time:** 30 minutes

**Objective:** Explore the features of a keylogger.

**Description:** A keylogger program captures everything that a user enters on a computer keyboard. In this project, you download and use a software keylogger.

**Caution:** The purpose of this activity is to provide information regarding how these programs function in order that adequate defenses can be designed and implemented. These programs should never be used in a malicious fashion against another user.

**NOTE:** Run this lab in your virtual machine.

# Disable Anti Virus

1. Open Settings: Press Windows key + I to open the Settings app.
2. Navigate to Windows Security: Go to Privacy & security > Windows Security.
3. Select Virus & threat protection: Click on Virus & threat protection.
4. Manage settings: Under "Virus & threat protection settings," click Manage settings.
5. Toggle Real-time protection: Switch the Real-time protection toggle to Off and confirm if prompted.

# Keylogger

1. Open your web browser and enter the URL [www.**refog.com**](http://www.refog.com) (If you are no longer able to access the program through the URL, use a search engine to search for “Refog Keylogger.”)
2. Click **Features** to see the features of the product.
3. Click **Home** 🡪 **Download**.
4. Click **Create an account** and enter the requested information.
5. Disable the Anti Virus on your Virtual Machine.
6. **Personal Monitor for Windows** 🡪 Click **Download**.
7. When the file finishes downloading, run the installation program. Note that you may have to enter the password on the previous page to extract the files.
8. Double Click the program installation file to start the installation.
9. **Windows Protected Your PC** 🡪 **More Info** 🡪 **Run anyway**
10. When prompted with **I’m going to use this software to monitor:** select **My own computer**.
11. **Don’t** Click **Hide program icon from Windows tray**. Click **Next**.
12. Click **I Agree**.
13. Click **Select All** and then **Next**.

**NOTE:** If the anti virus grabs your program as a threat 🡪 Go to the security dashboard 🡪 Protection History 🡪 Restore the Threat.

1. Use your account information you created earlier. Click **Activate**.
2. You may receive a message that the subscription has expired. Click **Yes** to install in offline mode.
3. Click **Install**.
4. Click **Restart Now**.
5. The Anti Virus will detect and remove the program. Install it again.
6. This time the program will run after the installation is completed. Don’t worry about the CTRLALTSHIFT business.
7. Click **Tools** and then click **Settings**.
8. Note the default settings regarding what is captured.
9. Click **Back to log**.
10. Minimize Refog Keylogger.
11. Use your computer normally by opening a web browser to surf to a website. Open Microsoft Word and type several sentences. Open and close several programs on the computer.
12. Open a web browser and surf to multiple websites.
13. Under Users,click **Websites visited**. Note the screen captures of the different sites.
14. Maximize Keylogger and note the information that was captured.
15. In the left pane, click through the different items that were captured.
16. Go to refog.com 🡪 Login with your account.
17. Take a screenshot of the recent activity.

Click or tap here to enter text.

1. Click Show All Activity. A little scary isn’t it?
2. What type of information would a software keylogger provide to a threat actor? How could it be used against the victim?

Click or tap here to enter text.

1. In the Keylogger 🡪 Tools 🡪 Uninstall.

# Reenable Anti Virus

1. Open Settings: Press Windows key + I to open the Settings app.
2. Navigate to Windows Security: Go to Privacy & security > Windows Security.
3. Select Virus & threat protection: Click on Virus & threat protection.
4. Manage settings: Under "Virus & threat protection settings," click Manage settings.
5. Toggle Real-time protection: Switch the Real-time protection toggle to On and confirm if prompted.

## Assignment Submission

Attach this completed document to the assignment in Blackboard.