***MN502 Network Security***

**Laboratory 2**: Keylogger and Data breaches

*Acknowledgement: CompTIA Security+ Guide to Network Security Fundamentals, Fifth Edition , 2015, by M. Ciampa*

**Description**:

This manual is for running experiment on software based Key logger – ***Spyrix Keylogger***  and for examining data breaches incidents published by a non-profit organization.

**Exercises 1 : Use a Software Keylogger**

**Pre-work:**

1. **Launch Virtual Box**
2. **Launch your Win8.1 VM**
3. **Do all your exercises in the VM**

**Keylogger**: A key logger program captures everything that a user enters on a computer keyboard. In this project, you will download and use a software key logger.

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

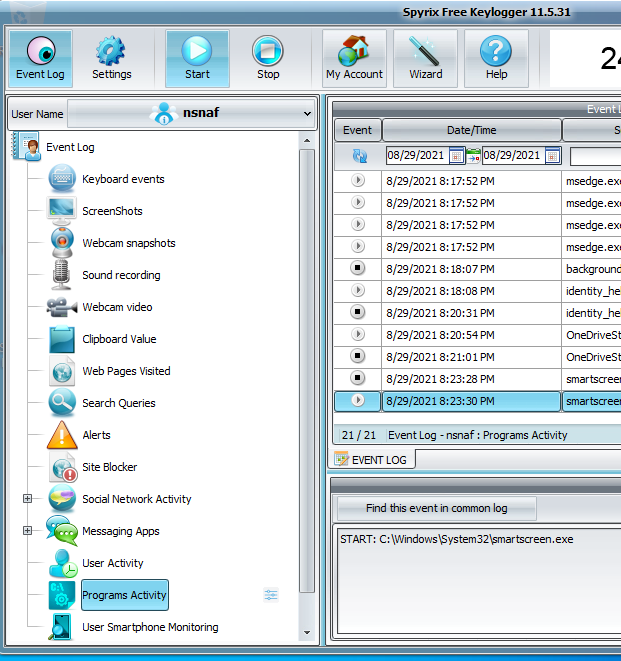
1. Open your web browser and enter the URL: [www.spyrix.com](http://www.spyrix.com)

[*The location of content on the Internet may change without warn- ing. If you are no longer able to access the program through the above URL, use a search engine to search for “Spyrix Personal Monitor”*.]

1. Click **products** and compare the features of the different Spyrix products.
2. Click **download**.
3. Under **Spyrix** **Free** **Keylogger** click **Free** **Download**.
4. When the file finishes downloading, install Spyrix and follow the default installation procedures.
5. Click **Finish** to launch Spyrix.
6. Click **Next** to use the wizard to set the program settings.
7. The **Hide** **everywhere** is not available on the Free Keylogger version but for the other versions this would allow Spyrix to act like a rootkit with no traces available. Click **Next**.
8. Create a strong password and enter it under **Password** to protect access to the program. Click **Next**.
9. Change **Screenshot** **Quality** to **Medium** **Quality** – Medium Size. Click Next.
10. Check **Online** **Monitoring** (via **any** **web**-**browser**) to set up the ability to view activity online. Click **OK**.
11. Enter your email address and create another strong password. Click **Create** **NEW** **Online** **Monitoring** **Account**. When the account is set up a message will appear. Click **OK**.
12. Click **Test secure connection**.
13. Click **Try to send log**.
14. Click **Enter your online monitoring account**.
15. Enter your username and password.
16. Click **Remote computer settings**.
17. Under **Delivery Interval** change the time to 2 minutes. Click **Apply**.
18. Close the web browser to return to the Spyrix
19. Under **Delivery** **Interval** change the time to 2 minutes. Click **Next**.
20. If prompted enter your Spyrix password.
21. Click the Spyrix icon in your system tray and enter the password.
22. Click **Start**.
23. Click **Minimize**.
24. Now use your computer for several minutes as you normally would.
25. Open your web browser and go to **spyrix.net** and enter your username and password.
26. Under **Events** click **ALL** **EVENTS** to view everything that has been done on the computer.
27. Click **Screenshots**. In the **Value** column click a screenshot.
28. Click **Program** **Activity** to view the programs that you were using.
29. Select several other options to view the keylogging and spy features of this program.
30. Close the web browser.
31. Click the Spyrix icon in your system tray and enter the password.
32. Click **Stop** and then **Exit**.
33. Enter your password and click **OK**.
34. Close all windows.

<https://www.spyrix.com/en/manual.php>

Screenshot of the interface



**Exercise 2: Examine Data Breaches**

The Privacy Rights Clearinghouse (PRC) is a non-profit organization whose goals are to raise consumers’ awareness of how technology affects personal privacy and empower consumers to take action to control their own personal information. The PRC maintains a searchable database of security breaches that impact consumer’s privacy. In this exercise, you will gather information from the PRC website.

1. Open a web browser and enter the URL [**www.privacyrights.org/data-breach**](http://www.privacyrights.org/data-breach)**.**

*[The location of content on the internet may change without warning. If you are no longer able to access the site through the above web address, use a search engine to search for “Privacy Rights Clearinghouse Data Breach”]*

1. First spend time reading about the RPC. Click **About Us** in the toolbar.
2. Scroll down to the content under Mission and Goals and also under services. Spend a few minutes reading about the PRC.
3. Click your browser’s **Back** button to return to the previous page.
4. On the **Chronology of Data Breaches** page scroll down and observe the different breaches listed in chronological order.
5. If you cannot access the page, download the database and work on the Excel spreadsheet. Complete the rest of the activities using filtering option.
6. Now create a customized list of the data that will only list data breaches of educational institutions. Scroll back to the top of the page.
7. Under **Select organization type(s)**, uncheck all organizations except **Educational Institutions.**
8. Click **GO!**
9. Scroll down to **Breach Subtotal** if necessary. How many breaches that were made public pertain to educations institutions?
10. Scroll down and observe the breaches for educational institutions.
11. Scroll back to the top of the page. Click **New Search,** locate beneath the **GO!** button**.**
12. Now search for breaches that were a result of lost, discarded, or stolen equipment that belonged to the government and military. Under **Choose the type of breaches to display,** uncheck all types except **Portable devices (PORT) – Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc.**
13. Under Select organization types(s), uncheck all organizations except **GOV – Government and Military**.
14. Click **GO!.**
15. Scroll down to Breach Subtotal, if necessary. How many breaches that were made public pertain to this type?
16. Scroll down and observe the breaches for governmental institutions.
17. Scroll back to the top of the page.
18. Now create a search based on criteria that you are interested in, such as the Payment Card Fraud against Retail/Merchants during the current year.
19. When finished, close all windows.

**Description of the laboratory exercise**:

In this laboratory, student will run and analyse a Keylogger tool. Examining and analysing of data breaches by breach type will be done to have a thorough understanding of the impact of these threats on an organisation.

**Task 1**: Keylogger

After completing all the steps in the manual for exercise one answer the following questions:

1. From your experience, explain what the Keylogger software is used for.

**Keyloggers are used for recording keystrokes entered in a computer. More sceptically to get combinations like passwords and sensitive info etc.**

1. Discuss the potential threat it poses for an organisation.

**They are able to get sensitive information which a hacker could then use to their advantage.**

1. Explain your view of using such software for positive purpose.

**If you want to see the input of what a person does in their day, then its not a bad tracking software. As it will record every keystroke of what someone does and the time that they do it as well.**

**Task 2**: Data breaches

After completing all the steps in the manual for exercise two answer the following questions:

1. From your experience what type of organisations faced more security threats as compared to others.

**Companies that have money or poor security ones.**

1. Regarding question one, provide your opinion about the potential reasons for particular type of organisations.

**Makes easy pickings for cyber criminals to target or get something out of them.**