CSE 4482 : Computer Security Management: Assessment and Forensics

Assignment 4

The exercise in this assignment is adapted from the book "Guide to Computer Forensics and Investigation", by B. Nelson, A. Phillips, F. Enfinger, C. Steuart, by Prof. N. Vlajic.

1. Nessus is a well-known vulnerability scanner that has been around for a long time. It is fast and thorough. Like with any other security tool, Nessus can be used for good or bad. The good/bad part has nothing to do with the tool, and everything to do with the person running the tool. Thus, remember to only scan your own computer(s), and at no point attempt to scan other (people's) computers.

1. Download Nessus 4.4 from http://www.nessus.org/download/.

2. Select Microsoft Windows (operating system) link.

3. Click I Accept.

4. Click on the link labelled Nessus-4.4.0-i386.msi (or Nessus-4.4.0-amd64.msi if you have a 64-bit system).

5. Click Save.

6. Select the C:\security folder.

7. If the program doesn't automatically open, browse to C:\security.

8. Double-click Nessus-4.4.0-i386.msi.

9. Click Next, I Accept, Next, Next, Next, Install, Finish.

10. Click Start, All Programs, Tenable Network Security, Nessus, Nessus Server Manager.

11. Click Obtain an activation code.

12. Click on the link labelled "Register a HomeFeed".

13. Click I Accept.

14. Enter an email address. (You will need to retrieve the access code to get Nessus to work.)

15. Click Register.

16. Open the email that Nessus.com just sent you and copy/paste the access code from the email to the Nessus Server Manager Screen.

17. Click Register.

18. Wait for the plug-ins to update and then close the Nessus Server Manager window.
Note: The plug-in update and installation may take awhile. Plug-ins are what gives Nessus the ability to do an effective vulnerability scan. You only need a large update like this once.

19. Click Start, All Programs. Tenable Network Security, Nessus, Nessus Server Manager.

20. Click Manage Users..., Click +, and then create a new client/user account. Click Save, Close.

21. Click Start Nessus Server.

22. Take a screenshot of the Nessus Server Manager window. Include this screenshot in your final report!

23. Click Start, All Programs. Tenable Network Security, Nessus, Nessus Client. (In case that you obtain "There is a problem with this website's security certificate message", ignore the message, and click "Continue to this website".)

24. In the Nessus Client log-in window, enter the User name and Password information as created in step 21.

25. On the Policies tab, Click + (Add), name the policy First Scan Policy. Click Next, Next, Next, Submit.

26. On the Scans tab, Click + (Add), name the scan First Scan. Under Policy select First Scan Policy. Under Scan Target enter 127.0.0.1 (i.e., localhost). Click Launch Scan. The scan may take up to 5 min.

27. Once the scan is completed, on the Reports tab, Double-click First Scan. Take a screenshot of First Scan's Report Info window. Include this screenshot in your final report!

28. Double-click on Host 127.0.0.1. Take a screenshot of the detailed list of scanned ports. Include this screenshot in your final report!

Now, answer the following questions:
1. Running the scan was fairly easy. Where could you go to get more information about understanding the results from the scan?

2. Who creates the plug-ins for Nessus and how do they decide which vulnerabilities to include?

3. How many vulnerabilities are reported each day?

4. What is Korgo Worm (backdoor) malware? (Hint: you can find information about this and other backdoor programs by researching Nessus Client -> Policies -> Plugins ->Backdoors list.)

2. ProDiscover

For the purposes of this assignment, you will have to download and install a copy of ProDiscover software. ProDiscover is a powerful forensics data analysis tool that enables computer professionals to quickly find all 'data of interest' on a computer disk or any portable memory device, while protecting evidence and creating evidentiary quality reports for use in legal proceedings.

The freeware demo version of ProDiscover (Basic Edition) can be downloaded from: http://www.techpathways.com/demo.htm. It is highly recommended that you download ProDiscover to your C:\security\ directory, and install it from there.

Part I Create and Delete Files on USB Drive

1. On your USB drive create a word file named"Sample4482_____.doc", where the blank should be filled with your name (e.g. Sample4482Alice.doc).

The file should contain the following sentence: "I _____ registered for CSE4482 course on _____." The first blank in the sentence should be filled in with your name and the second blank with the date when you registered for the course.

2. On the same drive create an excel file named "Sample4482_____.xls", where the blank should be filled with your name (e.g. Sample4482Alice.xls).
The file should contain columns: "user name", "YorkU student number", and "year of admission to YorkU". Fill in your data as the first record in the file and save the file.

3. Take a screenshot of your Windows Explorer window showing the content of the USB's folder hosting the two files. Include this screenshot in your final report!

4. Now delete both files, and then take another screenshot of the respective folder's content (after the two files have been deleted). Include this screenshot in your final report!

Part II Use ProDiscover Basic to Acquire an Image of USB Drive

1. To start ProDiscover Basic, click Start, point to All Programs, point to ProDiscover, and click ProDiscover Basic. If the Launch Dialog box opensIn the main window, click click Cancel

2. In the main window, click Action, Capture Image from the menu. (Prior to executing this step, make sure your USB drive is properly inserted/connected to your computer.)

3. In the Capture Image dialog box, click the Source Drive dropdown list, and select the USB drive as used in Part I.

4. Click the >> button next to the Destination text box, then select Choose Local Path option. When the Save As dialog box opens, navigate to your work folder (C:\Security\), and enter the following as the name of the image (.eve file) that you are making: 4482_Asgn4_USB. Click Save to save the file.

5. Next, in the Capture Image dialog box, type your name in the Technician Name text box, and 4482_Asgn4_USB_01 in the Image Number text box. Click OK.
ProDiscover will now acquire an image of your USB drive. This step may take several minutes, depending on the overall amount of data stored on the drive.

6. When ProDiscover is finished, click OK in the completion message box. Click File, Exit from the menu to exit ProDiscover.

Part III Use ProDiscover Basic to Recover Deleted Images
1. Start ProDiscover again. Type '4482_Asgn4_USB' in the Project Number text box and again in the (New) Project File Name text box. See figure below.

2. Select Action -> Add -> Image File, and in the Open dialog box navigate to the folder containing the USB's image (4482_Asgn4_USB.eve). Click on 4482_Asgn4_USB.eve, and then click Open.

3. Select View -> Content View -> Image. (Path)name of your image file 4482_Asgn4_USB.eve should appear in the work area. Take a screenshot of the work area and include it in your final report!

4. From Toolbar click on Search button/option. In the search dialogue box search for your student ID choosing the correct image file - 4482_Asgn4_USB.eve. (The figure below illustrates appropriate parameter setup when searching for student ID = 232425.) Click OK.

5. Once the search is completed, the name of deleted .xls should appear in ProDiscover's work area. Take a screenshot of the work area and include it in your final report!

6. Double-click on the deleted file, to retrieve its content. Take a screenshot of the recovered file and include it in your final report!

7. From Toolbar click on Search button/option. Select option Search for files named:, and in the search dialogue box enter the name of your deleted .doc file (e.g. Sample4482Alice.doc). Click OK.

8. Once the search is completed, the name of deleted .doc should appear in ProDiscover's work area. Take a screenshot of the work area and include it in your final report!

9. Double-click on the deleted file, to retrieve its content. Take a screenshot of the recovered file and include it in your final report!

10. Select View -> Report. Take a screenshot of the Evidence Report that has been created for your project and include it in your final report.
Assignment 4