|  |  |  |
| --- | --- | --- |
| **Sheridan College** | | |
| **Course** | **INFO24178: Computer and Network Security** | |
| **Professor** | **Abdul Mustafa** | |
| **Student Name** |  | |
| **Student ID** |  | |
| **Activity 1: Introduction (Some Diagnostic Utilities)** | | |
| **Performed Date** | *Date: 21st January 2015* | |
| **Instructor's Sign** |  | **(marks)** |

**IMPORTANT**: For all the activities, use of virtual machine recommended.

**Task 1: Investigate Some Windows Diagnostic Tools**

Visit Microsoft’s ‘Windows Sysinternals’ at <http://technet.microsoft.com/en-us/sysinternals> site. It hosts a lot of tools that help to diagnose problems and trouble shoot PCs.

|  |
| --- |
| **Output#1**: List some of the tools you might want to use. State why you think those are important for you. |
|  |

**Task 2: Use SigCheck (Windows Diagnostic Tool)**

SigCheck tool allows you to check is digital signature of a file. Signatures are important while installing software, especially from unfamiliar source.

1. Download **Sigcheck** (<http://technet.microsoft.com/en-us/sysinternals/bb897441>).
   1. Read the instruction in the download page.
   2. Extract the files in an appropriate folder. (For all the similar activities if this course, you can create and use a folder named ‘**utilities**’ in the main hard drive (c:\)
   3. Move **sigcheck.exe** to the **c:\windows** folder. This will allow you to run the tool from any directory in command prompt.
2. Follow the steps below to check if your system folder has any unsigned executable.
   1. Open command window.
   2. **Type sigcheck -u -e c:\windows\system32 >c:\utilities\Sigchecktest1.txt to check for any unsigned program in your system** (make sure the folder **utilities** exits). Open and explore the contents of the file **Sigchecktest1.txt**.
   3. Type **sigcheck –a –h c:\windows >c:\utilities\Sigchecktest2.txt** to check all the files in the windows directory for signature validity.. Open and explore the contents of the file **Sigchecktest2.txt**.

|  |
| --- |
| **Output#2**: Copy/paste contents of ‘Sigchecktest1.txt’ below |
|  |

1. Use the following steps to check the hash value of a downloaded file.
   1. Download **WinScp** from [www.winscp.net](http://www.winscp.net). (You can save the file in **utilities** folder)
   2. Note down the checksums (both MD5 and SHA1)
   3. Now use Check the signature of downloaded file using **sigcheck** and verify if the values matches or not with the values that you noted from the download site. Take a screenshot of your command window showing the run of sigcheck.

|  |
| --- |
| **Output#3:** Hash values |
| 1. Hash values from the site: |
| 1. Sceenshot of your command output: |

**Task 3: Keyboard logging**

1. Try to Download **keyboard collector software** (from [www.softdd.com](http://www.softdd.com)). Depending on your security settings, Windows may block the download. Use older Windows in VM. Notice the warning from google/firefox (if you are using firefox). You might find Sheridan blocking your access to softdd, you can get an alternate location from Download.com: <http://download.cnet.com/Free-Keystroke-Logger/3000-2162_4-75447782.html>
2. But make sure you install it on your VM machines

|  |
| --- |
| **Output#4**: Your observation |
|  |

**Task 4: Try USB Drive Protection Tool**

1. Download and test **Thumbscrew** for write protection of USB storage.
2. Try to do or undo write protection manually using the registry. (Read the download site for help)

|  |
| --- |
| **Output#5:** Your observation |
|  |

**Task 5: Submit the Report**

1. Show your results to the professor.
2. Upload the completed word file in SLATE2 Dropbox. (**IMPORTANT**: Name the file according to your name)