**Shankar Narayan College of Arts and Commerce, Self-Finance Courses**

**POST GRADUATE OF M.Sc.I.T**.

MScIT Part I Sem II Internal Practical Exam – July 2024

Subject : Malware Analysis 50 Marks

Date : 06/07/2024 Time: 02 hr.

|  |  |  |
| --- | --- | --- |
| A. | Files: Lab01-01.exe and Lab01-01.dll.  i. Upload the files to http://www.VirusTotal.com/ and view the reports. Does either file match any existing antivirus signatures? ii. When were these files compiled? iii. Are there any indications that either of these files is packed or obfuscated?  If so, what are these indicators? iv. Do any imports hint at what this malware does? If so, which imports are they?  v. Are there any other files or host-based indicators that you could look for on infected systems?  vi. What network-based indicators could be used to find this malware on infected machines? vii. What would you guess is the purpose of these files? | **40** |
| B. | Journal | **5** |
| C. | Viva | **5** |

**Shankar Narayan College of Arts and Commerce, Self-Finance Courses**

**POST GRADUATE OF M.Sc.I.T**.

MScIT Part I Sem II Internal Practical Exam – July 2024

Subject : Malware Analysis 50 Marks

Date : 06/07/2024 Time: 02 hr.

|  |  |  |
| --- | --- | --- |
| A. | Analyze the file Lab01-02.exe.  i. Upload the Lab01-02.exe file to http://www.VirusTotal.com/. Does it match any existing antivirus definitions?  ii. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.  iii. Do any imports hint at this program’s functionality? If so, which imports are they and what do they tell you? iv. What host- or network-based indicators could be used to identify this malware on infected machines? | **40** |
| B. | Journal | **5** |
| C. | Viva | **5** |

**Shankar Narayan College of Arts and Commerce, Self-Finance Courses**

**POST GRADUATE OF M.Sc.I.T**.

MScIT Part I Sem II Internal Practical Exam – July 2024

Subject : Malware Analysis 50 Marks

Date : 06/07/2024 Time: 02 hr.

|  |  |  |
| --- | --- | --- |
| A. | Analyze the file Lab01-03.exe.  i. Upload the Lab01-03.exe file to http://www.VirusTotal.com/. Does it match any existing antivirus definitions? ii. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.  iii. Do any imports hint at this program’s functionality? If so, which imports are they and what do they tell you? iv. What host- or network based indicators could be used to identify this malware on infected machines? | **40** |
| B. | Journal | **5** |
| C. | Viva | **5** |

**Shankar Narayan College of Arts and Commerce, Self-Finance Courses**

**POST GRADUATE OF M.Sc.I.T**.

MScIT Part I Sem II Internal Practical Exam – July 2024

Subject : Malware Analysis 50 Marks

Date : 06/07/2024 Time: 02 hr.

|  |  |  |
| --- | --- | --- |
| A. | Analyze the file Lab01-04.exe.  i. Upload the Lab01-04.exe file to http://www.VirusTotal.com/. Does it match any existing antivirus definitions? ii. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible. iii. When was this program compiled? iv. Do any imports hint at this program’s functionality? If so, which imports are they and what do they tell you?  v. What host- or network-based indicators could be used to identify this malware on infected machines?  vi. This file has one resource in the resource section. Use Resource Hacker to examine that resource, and then use it to extract the resource. What can you learn from the resource? | **40** |
| B. | Journal | **5** |
| C. | Viva | **5** |

**Shankar Narayan College of Arts and Commerce, Self-Finance Courses**

**POST GRADUATE OF M.Sc.I.T**.

MScIT Part I Sem II Internal Practical Exam – July 2024

Subject : Malware Analysis 50 Marks

Date : 06/07/2024 Time: 02 hr.

|  |  |  |
| --- | --- | --- |
| A. | Analyze the malware found in the file Lab03-02.dll using basic dynamic analysis tools.  i. How can you get this malware to install itself?  ii. How would you get this malware to run after installation? iii. How can you find the process under which this malware is running? iv. Which filters could you set in order to use procmon to glean information? v. What are the malware’s host-based indicators?  vi. Are there any useful network-based signatures for this malware? | **40** |
| B. | Journal | **5** |
| C. | Viva | **5** |

**Shankar Narayan College of Arts and Commerce, Self-Finance Courses**

**POST GRADUATE OF M.Sc.I.T**.

MScIT Part I Sem II Internal Practical Exam – July 2024

Subject : Malware Analysis 50 Marks

Date : 06/07/2024 Time: 02 hr.

|  |  |  |
| --- | --- | --- |
| A. | Analyze the file Lab01-03.exe.  i. Upload the Lab01-03.exe file to http://www.VirusTotal.com/. Does it match any existing antivirus definitions?  ii. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.  iii. Do any imports hint at this program’s functionality? If so, which imports are they and what do they tell you?  iv. What host- or network-based indicators could be used to identify this malware on infected machines? | **40** |
| B. | Journal | **5** |
| C. | Viva | **5** |

**Shankar Narayan College of Arts and Commerce, Self-Finance Courses**

**POST GRADUATE OF M.Sc.I.T**.

MScIT Part I Sem II Internal Practical Exam – July 2024

Subject : Malware Analysis 50 Marks

Date : 06/07/2024 Time: 02 hr.

|  |  |  |
| --- | --- | --- |
| A. | Analyze the file Lab01-04.exe.  i. Upload the Lab01-04.exe file to http://www.VirusTotal.com/. Does it match any existing antivirus definitions?  ii. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.  iii. When was this program compiled?  iv. Do any imports hint at this program’s functionality? If so, which imports are they and what do they tell you?  v. What host- or network-based indicators could be used to identify this malware on infected machines? | **40** |
| B. | Journal | **5** |
| C. | Viva | **5** |

**Shankar Narayan College of Arts and Commerce, Self-Finance Courses**

**POST GRADUATE OF M.Sc.I.T**.

MScIT Part I Sem II Internal Practical Exam – July 2024

Subject : Malware Analysis 50 Marks

Date : 06/07/2024 Time: 02 hr.

|  |  |  |
| --- | --- | --- |
| A. | Analyze the malware found in the file Lab06-01.exe.  i. What is the major code construct found in the only subroutine called by main? ii. What is the subroutine located at 0x40105F? iii. What is the purpose of this program? | **20** |
| B. | Analyze the malware found in the file Lab06-02.exe.  i. What operation does the first subroutine called by mainperform? ii. What is the subroutine located at 0x40117F? iii. What does the second subroutine called by maindo? iv. What type of code construct is used in this subroutine?  v. Are there any network-based indicators for this program? vi. What is the purpose of this malware? | **20** |
| C. | Journal | **5** |
| D. | Viva | **5** |

**Shankar Narayan College of Arts and Commerce, Self-Finance Courses**

**POST GRADUATE OF M.Sc.I.T**.

MScIT Part I Sem II Internal Practical Exam – July 2024

Subject : Malware Analysis 50 Marks

Date : 06/07/2024 Time: 02 hr.

|  |  |  |
| --- | --- | --- |
| A. | Analyze the malware found in the file Lab06-02.exe.  i. What operation does the first subroutine called by mainperform? ii. What is the subroutine located at 0x40117F?  iii. What does the second subroutine called by maindo? iv. What type of code construct is used in this subroutine?  v. Are there any network-based indicators for this program? vi. What is the purpose of this malware? | **20** |
| B. | Analyze the malware found in the file Lab06-03.exe.  i. Compare the calls in main to Lab 6-2’s main method. What is the new function called from main?  ii. What parameters does this new function take? iii. What major code construct does this function contain?  iv. What can this function do?  v. Are there any host-based indicators for this malware?  vi. What is the purpose of this malware? | **20** |
| C. | Journal | **5** |
| D. | Viva | **5** |

**Shankar Narayan College of Arts and Commerce, Self-Finance Courses**

**POST GRADUATE OF M.Sc.I.T**.

MScIT Part I Sem II Internal Practical Exam – July 2024

Subject : Malware Analysis 50 Marks

Date : 06/07/2024 Time: 02 hr.

|  |  |  |
| --- | --- | --- |
| A. | a. Analyze the malware found in the file Lab07-01.exe.  i. How does this program ensure that it continues running (achieves persistence) when the computer is restarted?  ii. Why does this program use a mutex?  iii. What is a good host-based signature to use for detecting this program? iv. What is a good network-based signature for detecting this malware?  v. What is the purpose of this program?  vi. When will this program finish executing? | **40** |
| B. | Journal | **5** |
| C. | Viva | **5** |

**Shankar Narayan College of Arts and Commerce, Self-Finance Courses**

**POST GRADUATE OF M.Sc.I.T**.

MScIT Part I Sem II Internal Practical Exam – July 2024

Subject : Malware Analysis 50 Marks

Date : 06/07/2024 Time: 02 hr.

|  |  |  |
| --- | --- | --- |
| A. | Analyze the malware found in the file Lab07-02.exe.  i. How does this program achieve persistence?  ii. What is the purpose of this program?  iii. When will this program finish  executing? | **20** |
| B. | Analyze the malware found in the file Lab06-03.exe.  i. Compare the calls in main to Lab 6-2’s main method. What is the new function called from main?  ii. What parameters does this new function take?  iii. What major code construct does this function contain?  iv. What can this function do?  v. Are there any host-based indicators for this malware?  vi. What is the purpose of this malware? | **20** |
| C. | Journal | **5** |
| D. | Viva | **5** |

**Shankar Narayan College of Arts and Commerce, Self-Finance Courses**

**POST GRADUATE OF M.Sc.I.T**.

MScIT Part I Sem II Internal Practical Exam – July 2024

Subject : Malware Analysis 50 Marks

Date : 06/07/2024 Time: 02 hr.

|  |  |  |
| --- | --- | --- |
| A. | The file for this lab is Lab10-02.exe.  i. Does this program create any files? If so, what are they?  ii. Does this program have a kernel component? iii. What does this program do? | **20** |
| B. | This lab includes a driver and an executable. You can run the executable from anywhere, but in order for the program to work properly, the driver must be placed in the C:\Windows\System32 directory where it was originally found on the victim computer. The executable is Lab10-03.exe, and the driver is Lab10-03.sys. i. What does this program do?  ii. Once this program is running, how do you stop it? iii.  What does the kernel component do? | **20** |
| C. | Journal | **5** |
| D. | Viva | **5** |

**Shankar Narayan College of Arts and Commerce, Self-Finance Courses**

**POST GRADUATE OF M.Sc.I.T**.

MScIT Part I Sem II Internal Practical Exam – July 2024

Subject : Malware Analysis 50 Marks

Date : 06/07/2024 Time: 02 hr.

|  |  |  |
| --- | --- | --- |
| A. | Analyse the malware found in Lab11-01.exe i.  What does the malware drop to disk?  ii. How does the malware achieve persistence? iii.  How does the malware steal user credentials?  iv. What does the malware do with stolen credentials?  v. How can you use this malware to get user credentials from your test environment? | **40** |
| B. | Journal | **5** |
| C. | Viva | **5** |

**Shankar Narayan College of Arts and Commerce, Self-Finance Courses**

**POST GRADUATE OF M.Sc.I.T**.

MScIT Part I Sem II Internal Practical Exam – July 2024

Subject : Malware Analysis 50 Marks

Date : 06/07/2024 Time: 02 hr.

|  |  |  |
| --- | --- | --- |
| A. | Analyze the malware found in Lab11-02.dll. Assume that a suspicious file named Lab11-02.ini was also found with this malware.  i. What are the exports for this DLL malware? ii. What happens after you attempt to install this malware using iii.  rundll32.exe?  iv. Where must Lab11-02.ini reside in order for the malware to install properly?  v. How is this malware installed for persistence?  vi. What user-space rootkit technique does this malware employ? vii. What does the hooking code do?  viii. Which process(es) does this malware attack and why? ix. What is the significance of the .ini file? | **40** |
| B. | Journal | **5** |
| C. | Viva | **5** |

**Shankar Narayan College of Arts and Commerce, Self-Finance Courses**

**POST GRADUATE OF M.Sc.I.T**.

MScIT Part I Sem II Internal Practical Exam – July 2024

Subject : Malware Analysis 50 Marks

Date : 06/07/2024 Time: 02 hr.

|  |  |  |
| --- | --- | --- |
| A. | Analyze the malware found in the file Lab12-01.exe and Lab12-01.dll. Make sure that these files are in the same directory when performing the analysis. i. What happens when you run the malware executable?  ii. What process is being injected?  iii. How can you make the malware stop the pop-ups? iv. How does this malware operate? | **20** |
| B. | Analyze the malware found in the file Lab12-02.exe. i.  What is the purpose of this program?  ii. How does the launcher program hide execution?  iii. Where is the malicious payload stored? iv. How is the  malicious payload protected? v. How are strings protected? | **20** |
| C. | Journal | **5** |
| D. | Viva | **5** |

**Shankar Narayan College of Arts and Commerce, Self-Finance Courses**

**POST GRADUATE OF M.Sc.I.T**.

MScIT Part I Sem II Internal Practical Exam – July 2024

Subject : Malware Analysis 50 Marks

Date : 06/07/2024 Time: 02 hr.

|  |  |  |
| --- | --- | --- |
| A. | Analyze the malware found in the file Lab15-02.exe. Correct all anti-disassembly countermeasures before analyzing the binary in order to answer the questions.  i. What URL is initially requested by the program?  ii. How is the User-Agent generated?  iii. What does the program look for in the page it initially requests?  iv. What does the program do with the information it extracts from the page? | **20** |
| B. | Analyze the malware found in the file Lab12-02.exe. i.  What is the purpose of this program?  ii. How does the launcher program hide execution?  iii. Where is the malicious payload stored? iv. How is the  malicious payload protected? v. How are strings protected? | **20** |
| C. | Journal | **5** |
| D. | Viva | **5** |