**SRM Institute of Science and Technology**

SET A

**College of Engineering and Technology**

**School of Computing**

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamil Nādu

**Academic Year: 2022-23 (EVEN)**

**Test: CLA-T3** **Date: 09.04.2023**

**Course Code & Title:** 18CSE412J – Offensive security **Duration:** 2 periods

**Year & Sem: IIIYear / VI Sem** **Max. Marks:** 50 marks

**Program Learning Outcomes (PLO)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Engineering Knowledge | Problem Analysis | Design & Development | Analysis, Design, Research | Modern Tool Usage | Society & Culture | Environment & Sustainability | Ethics | Individual & Team Work | Communication | Project Mgt. & Finance | Life Long Learning | PSO - 1 | PSO - 2 | PSO – 3 |
|
|
|
|
|
| *3* | *-* | *-* | *-* | *2* | *-* | *-* | *1* | *-* | *-* | *-* | *3* | *-* | *-* | *-* |
| *3* | *-* | *-* | *-* | *2* | *-* | *-* | *1* | *-* | *-* | *-* | *3* | *-* | *-* | *-* |
| *3* | *-* | *-* | *-* | *2* | *-* | *-* | *1* | *-* | *-* | *-* | *3* | *-* | *-* | *-* |
| *3* | *-* | *-* | *-* | *2* | *-* | *-* | *1* | *-* | *-* | *-* | *3* | *-* | *-* | *-* |
| *3* | *-* | *-* | *-* | *2* | *-* | *-* | *1* | *-* | *-* | *-* | *3* | *-* | *-* | *-* |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PART B – (5\*10=50 Marks)** | | | | | |
| **Question** | **Mark** | **BL** | **CO** | **PO** | **PI code** |
| Discuss the techniques used in DLL injection attack. | 10 | 3 | 4 | 5 | 5.7.1 |
| Explain the significance of keeping databases up to date and the potential outcomes of failing to update the database. | 10 | 2 | 4 | 5 | 5.7.1 |
| Explain what is living off-the-land binaries (LOL Bins) are in offensive security testing and give an example of how they can be utilized. | 10 | 3 | 5 | 1 | 1.7.1 |
| How is open-source Intelligence used? Find the difference between passive versus active OSINT. | 10 | 3 | 5 | 1 | 1.7.1 |
| Explain how to find the antivirus signature of a detected file and use it to add the file to a white list? | 10 | 4 | 5 | 1 | 1.7.1 |

**SRM Institute of Science and Technology**

SET B

**College of Engineering and Technology**

**School of Computing**

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamil Nādu

**Academic Year: 2022-23 (EVEN)**

**Test: CLA-T3** **Date: 09.04.2023**

**Course Code & Title:** 18CSE412J – Offensive security **Duration:** 2 periods

**Year & Sem: IIIYear / VI Sem** **Max. Marks:** 50 marks

**Program Learning Outcomes (PLO)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Engineering Knowledge | Problem Analysis | Design & Development | Analysis, Design, Research | Modern Tool Usage | Society & Culture | Environment & Sustainability | Ethics | Individual & Team Work | Communication | Project Mgt. & Finance | Life Long Learning | PSO - 1 | PSO - 2 | PSO – 3 |
|
|
|
|
|
| *3* | *-* | *-* | *-* | *2* | *-* | *-* | *1* | *-* | *-* | *-* | *3* | *-* | *-* | *-* |
| *3* | *-* | *-* | *-* | *2* | *-* | *-* | *1* | *-* | *-* | *-* | *3* | *-* | *-* | *-* |
| *3* | *-* | *-* | *-* | *2* | *-* | *-* | *1* | *-* | *-* | *-* | *3* | *-* | *-* | *-* |
| *3* | *-* | *-* | *-* | *2* | *-* | *-* | *1* | *-* | *-* | *-* | *3* | *-* | *-* | *-* |
| *3* | *-* | *-* | *-* | *2* | *-* | *-* | *1* | *-* | *-* | *-* | *3* | *-* | *-* | *-* |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PART A – (5\*10=50 Marks)** | | | | | |
| **Question** | **Mark** | **BL** | **CO** | **PO** | **PI code** | |
| What is the difference between process hollowing and process injection? | 10 | 3 | 4 | 5 | 5.7.1 | |
| Explain the types of credential attacks with an example. | 10 | 2 | 4 | 1 | 1.7.1 | |
| Define Applocker and Techniques to bypass it | 10 | 2 | 5 | 1 | 1.7.1 | |
| Explain the distinction between encoders and encrypters when creating malware | 10 | 3 | 5 | 5 | 5.7.1 | |
| Explain the method employed in antivirus evasion using Metasploit and its effectiveness in bypassing antivirus detection. | 10 | 4 | 5 | 1 | 1.7.1 | |