**REM ASSIGNMENT MARKING RUBRICS**

|  |  |
| --- | --- |
| **Lab Setup (5 marks) Team** | **Marks** |
| Description of VM used | 2 |
| Network Diagram & Configuration | 3 |
|  |  |
| **Passive Information gathering (30 marks) Individual** |  |
| Description of important API calls | 20 |
| URL to access | 10 |
|  |  |
| **Code Analysis (30 marks) Individual** |  |
| Purpose of Subroutines with explanation | 20 |
| Calling Structure | 10 |
|  |  |
| **Patching (60 marks) Individual** |  |
| Malicious code identification and relating the code to IDA Pro | 20 |
| Code execution (relevant breakpoints and register/parameters values) | 20 |
| Patching (NOP should be used sparingly) | 20 |
|  |  |
| **General Analysis (15 marks) Team** |  |
| What type of malware is it? | 2 |
| What are the functionalities of the malware? Indicate host-based and network-based indicators | 8 |
| Malware Interaction and removal (manual steps) | 5 |
|  |  |
| **Demo & Presentation (20 marks ) Individual** |  |
| Understanding | 14 |
| Clarity | 6 |

**Note: Report must contain relevant evidence with aid of screenshots**