Assessment Front Sheet

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Assessment Title | | VAPT of Web Application of General Trading | | |
| Qualification |  | | Module Code and title | |
| HND in Computer Science |  | | HR90 47  Ethical Hacking Fundamentals | |
| Student ID |  | | Assessor’s Name | |
|  |  | | Kanchana Senadheera | |
| Cohort | Date Issued | |  | Submitted on |
|  |  | |  |  |

|  |  |  |
| --- | --- | --- |
| No. | Learning Outcome | Task no |
|  | Perform target information gathering reconnaissance. |  |
|  | Perform system security vulnerability testing. |  |
|  | Perform system vulnerability exploit attacks. |  |
|  | Produce a security assessment report |  |

|  |
| --- |
| Learner Declaration |
| I certify that the work submitted for this Assessment is my own and research sources are fully acknowledged.    Student Signature: ………………………………… Date: ………………... |

|  |  |
| --- | --- |
| Module Code and Title | HR90 47 Ethical Hacking Fundamentals |
| Qualification | HND in Computer Science |
| Deadline |  |
| Assessor’s Name | Kanchana Senadheera |

|  |  |
| --- | --- |
| Assessment Title | VAPT of the Web Application of General Trading |
| **Overview**: You are required to read the information presented in the case study below and to assume the position of Information Security Systems Engineer/Tester. | |
| “General Trading” is a popular retailer of different types of items. They have an island-wide branch network which spans in 45 branches.  Due to the ongoing pandemic situation and subsequent lock-downs, their business has been impacted considerably. To overcome these challenges, after a discussion with the board of directors Mrs Shantha Mayadunne, Mr Nayana Thilakarathne and Mr Hemasiri Halpita, the owner and the Chief Executive Mr Sudath Mahadiwulwewa has decided to open the business in a web channel, with an eCommerce application.  Being well aware of the inherent risks associated with eCommerce platforms, the CEO wants to have the partially developed and deployed web application to undergo a thorough round of black-box VAPT.  You, being the Information Security Engineer hired for the task, have been given with access to the network. | |
| Task List  You are being given with the following, regarding the technical infrastructure.   * Vagrantfile that mocks the network architecture of the internal network of General Trading * Source code of the application (ecmate.zip). **Installation instructions of the application is provided in README.md inside the ZIP**.   Having been presented with the information above along with the network architecture and subject software, perform a complete VAPT on the web application and web server that houses the said application. Submission artefacts required and the relevant instructions are given below.   1. Rules of Engagement Document – Prepare a suitable Rules of Engagement document for the given scenario. When preparing that, pay attention to the following content. (a sample is included herewith for your reference) 2. Introduction 3. Scope 4. Risks and Limitations 5. Logistics    1. Key Personnel    2. Test Schedule    3. Testing Tools 6. Incident Handling and Response 7. Termination of the Test 8. Data Handling 9. Reporting 10. Limitation of Liability 11. Signatures 12. VAPT Report – The structure of the VAPT report is included herewith (HR9047\_vapt\_report\_template.docx)     * This report should be submitted in **PDF format**.     * Topics that the report should comprise of, and the content expected is given in the template.     * Proper formatting and presentation of the report is expected. **Make sure the formatting of the content is consistent throughout the report**. 13. Presentation Slides: A presentation with **no less than 10 slides and no more than 15 slides** to be included. This presentation should include explanations of the exploitable vulnerabilities you have found during your testing. You will present this to the assessor followed by a Q&A session. You should discuss about a **minimum of three (03) vulnerabilities** here, focussing on the following about each     * Brief introduction     * Steps to exploit     * Nature of the impact   General Instructions.   * Naming of the files: Please make sure you submit 3 separate files, each named as follows. **Strict adherence to these is required, which otherwise will result in submissions rejection.**   + RoE Document - **<<ANC\_REG\_NO>>\_ROE.pdf** (e.g., If your ANC registration number is 01000234, **01000234\_ROE.pdf** should be the file name)   + VAPT Report - **<<ANC\_REG\_NO>>\_VAPT\_REPORT.pdf** (e.g., If your ANC registration number is 01000234, **01000234\_VAPT\_REPORT.pdf** should be the file name)   + Presentation Slides - **<<ANC\_REG\_NO>>\_PRESENTATION.pdf** (e.g., If your ANC registration number is 01000234, **01000234\_PRESENTATION.pdf** should be the file name) * Tools Required:   + Vagrant   + VMWare Workstation (Pro V16.x is recommended)   + Once the Kali Linux VM is booted up, you are free to install any tool required for the task | |

|  |  |
| --- | --- |
| Student Number |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Evidence Checklist** | **Summary of the evidence required by students** | **Task** | **Evidence Checked** |
| Outcome 01 | * RoE document * VAPT Report | Task 01, 02 |  |
| Outcome 02 | * RoE document * VAPT Report * Presentation | Task 01, 02, 03 |  |
| Outcome 03 | * VAPT Report * Presentation | Task 02, 03 |  |
| Outcome 04 | * VAPT Report | Task 02 |  |

Evidence checked by : ………………………………………………………………………………………………………

Signature & Date : ………………………………………………………………………………………………………