**BHI & CAE ASSESSMENT COVER SHEET**

This form must be attached to the front of all submitted hard copy assessments.

|  |  |  |  |
| --- | --- | --- | --- |
| **Student Details: Student to complete** | | | |
| **Student Name:** | Insert your name here | | |
| **Student ID :** | Insert your Student ID here | | |
| **Student Declaration**:  By signing below, I declare that the work submitted here is my own work and it does not include work which is plagiarised, copied in whole or in part from another student or other source such as published books, internet or journals without due acknowledgement in the text. | | | |
| **Student Signature:**  Insert your Signature here | | | **Date:**  Insert the date you submitted this assessment |
| **Assessment Details: Teacher to complete** | | | |
| **Course National ID and Title** | | 22334VIC Certificate IV in Cyber Security | |
| **Unit/s National ID and Title** | | VU21991 - Implement Network Security Infrastructure for an Organization Instructor Guide | |
| **Assessment Task number and name** | | Assessment Task 2: Proxy & WLAN vulnerabilities | |
| **Date due:**  ***Sunday after session 12 class*** | | **Date submitted:** | |
| **Assessor Name:** | | TBA | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Assessment Result and Feedback** | | | | | | |
| Result | | Satisfactory  Not yet Satisfactory | Re-submit date if required: | | |  |
| Feedback: | | | | | | |
| Assessor’s signature: | |  | Date: | | |  |
| **Assessment Review**  If you believe that you have been assessed unfairly, you have the right to request an informal assessment review. When your assessment cover sheet is returned to you, you can request an informal review by filling in the section below and returning it to your assessor or the Operations Manager of your area. If you are not satisfied with the outcome, you can apply for a formal review of assessment on the application form located on the Box Hill Institute Website <https://goo.gl/Pb3Rtx>  VCE courses: VCAA rules and regulations replace the above assessment review. Please see your VCE Teacher or VCE Coordinator for further discussion. | | | | | | |
| I request a review of my assessment for the following reasons (not applicable to VCE courses): | | | | | | |
| Student Signature |  | | | Date |  | |

|  |  |  |
| --- | --- | --- |
| **Instructions to Student** | | |
| **Assessment task name** | Assessment Task 2: Proxy & WLAN vulnerabilities | |
| **Assessment task type** | Report/Questioning/Meeting | |
| **Time allowed** | Week 4 – 6 in class and at home as required | |
| **Where the assessment will take place** | In timetabled classroom | |
| **Personal protective equipment required** | N/A | |
| **Emergency procedures** | Report Issues to Teacher or coordinators as appropriate | |
| **Equipment provided** | PC on campus during class time | |
| **Individual or group work** | Individual & Group Work | |
| **Support equipment allowed i.e.: calculator, dictionary** | All tools as appropriate for the assessment | |
| **Context and conditions of assessment** | Assessment must be conducted in a safe environment where evidence gathered demonstrates consistent performance of typical activities experienced in the knowledge management – research field of work and include access to:   * workplace information systems, equipment and resources * workplace policies and procedures * Case studies and, where possible, real situations.   Assessors must satisfy NVR/AQTF assessor requirements. | |
| **What to submit** | The completed report is to be submitted to StudentWeb under the Assessment Task 2: Proxy & WLAN vulnerabilities | |
| **How to submit** | Submit the completed document (this document) to the Assessment Task 2: Proxy & WLAN vulnerabilities section on StudentWeb. | |
| **How to present your work** | Complete this word document and answer all questions in the spaces provided. The coversheet must be submitted when uploading to StudentWeb. | |
| **How many attempts at assessment are permitted** | Students will be given **2** attempts to resubmit an assessment; additional attempts must be organized with teacher and student prior to submission. | |
| **Naming protocol for electronic files** | ID\_AT1\_API.doc  E.g.: S10054440\_AT1\_ API.doc  All files that do not have this naming convention will be sent back to you as it resembles part of you assessment that the information is corrected handled and stored. | |
| **How will the assessment judgement be made** | Observation checklist | Exemplar |
| Performance checklist | Rubric |
| Answer guide | - |
| **Safety** | | |
| If at any time during the learning and assessment process, your Trainer/Assessor considers that the safety of any person is at risk they will abort the session. | | |
| **Reasonable Adjustment** | | |
| Students identifying as having a disability may access reasonable adjustment to enable them to participate in training and assessment on the same basis as other students. Students can learn more about this through the Learners with a disability policy and procedure on the Box Hill Institute website http://www.boxhill.edu.au/for-students/student-support or by calling Student Life on 9286 9891, by emailing the Disability liaison service on dls@boxhill.edu.au or by calling into the Student Life office at Elgar Campus in E3.G56, just near the cafeteria. | | |
| **Special Consideration** | | |
| Where a student anticipates that a result will be impacted by special circumstances such as ill health or bereavement, application can be made for special consideration. Forms can be accessed from the Student Life office at Elgar Campus in E3.G56 or downloaded at: <http://www.boxhill.edu.au/for-students/student-information/forms-and-downloads>.  VCE courses: Supplementary exam procedures apply. Please see your VCE Teacher or VCE Coordinator for further discussion. | | |

**VU21991 AT3 – Introduction to securing security devices**

The following criteria will be used for this assessment:

Configure secure administrative access to network devices

* Network security architectures is described, demonstrated and implemented
* Process of configuring secure administrative access to network devices is described and implemented
* Process of allocation user command privileges for network devices is described, demonstrated and implemented
* Secure management and network monitoring is implemented
* Features to enable security on Internet Operating System (IOS) based routers are implemented
* Purpose of Authentication, Authorization and Accounting (AAA) procedures to access to network devices are described
* AAA authentication from a local server is implemented

Implement firewall technologies

* Higher level packet inspection is performed
* Function and operation of a firewall to mitigate network attacks is described and implemented
* Zone based policy firewall is demonstrated and implemented
* Tools to implement packet filtering are demonstrated and implemented
* Operation of inspection rules are described and demonstrated

Investigate new firewall technologies

* Higher level packet inspection is performed
* Holistic approaches to traffic inspection are investigated
* Concept of dynamic updates for defending against new cyber-attacks are examined
* New firewall technology operation is demonstrated

Implement Intrusion prevention systems (IPS)

* Securing a network with network based Intrusion Prevention System (NIPS)is examined
* Detecting malicious traffic using signatures is demonstrated
* Intrusion Prevention System (IPS) using an Internetworking Operating System (IOS) is defined and implemented

Demonstrate the fundamental operation of Cryptographic systems

* Overview of cryptography is provided
* Process of working with symmetric & asymmetric algorithms is defined
* Function and operation of encryption, hashes and digital signatures to secure a network is summarized
* Data integrity and authentication utilizing encryption algorithms are defined
* Data confidentiality utilizing encryption algorithms are summarized
* Process of public key encryption to ensure data confidentiality is demonstrated
* Cryptography standards and protocols are summarized
* Common use of protocols that utilize cryptography are demonstrated

Define and demonstrate the fundamentals of Virtual Private Networks (VPN’s)

* Advantages and operation of Virtual Private Networks (VPN’s) are explained
* Operation of Internet Protocol Security (*IPSec)* VPN’s is summarized
* Operation of tunneling is described and demonstrated
* Site to site IPSec VPN with pre shared key authentication is demonstrated

**Background Information:**

This unit utilizes the preformed student groups identified in the VU21992 Cyber Security Unit for the ABC Widgets Franchise scenario. This is an individual assessment task but will take the form of a Case Study. It is acknowledged that you will require support from your team members and also from the instructor.

It is suggested that a demonstration to representatives at ABC Widget Franchise would be appropriate for some of their requirements.

ABC Widget Franchise has asked you to provide support for their staff in the following areas:

1. To help them improve their networking device security
2. To help them understand how to improve user network security access by implementing authentication to users in their login sequence
3. To provide information about different types of firewalls and firewall technologies
4. To explain how an IPS can increase their network security and how it is implemented
5. To provide an overview of cryptography and how it can improve network security
6. To provide support in implement site to site VPS’s utilizing IPsec

You have taken their brief and you have split their request into two sections:

**Section 1.**

Improve networking device security and implementing user authentication. To do this you propose to:

1. Implement secure administrative access to existing networking devices (Lab demonstration)
2. Implement user command privileges for their networking devices (Lab demonstration)
3. Implement security features in the IOS of their networking devices (Lab demonstration)
4. Implement AAA for their network devices (Lab demonstration)
5. Demonstrate both Standard and extended access lists to improve the security of ABC Widget Franchise’s network (Lab demonstration)
6. Provide a report on firewall technologies: (You will brief representatives of the ABC Widget Franchise on the report outcomes)
   1. Zone based firewalls
   2. Packet filtering
   3. Introduction to inspection rules
   4. Concepts of higher level packet inspection
   5. How dynamic address updates can be used against cyber attacks
   6. New firewall technologies
7. Demonstrate IPS principles using the features of a networking device IOS
8. Clarify how signatures are used to detect malicious traffic

**Section 2.**

Cryptography and how it can improve security and implementing a secure VPN. To do this you propose the following:

1. An overview of cryptography
2. Define the difference between symmetric and asymmetric algorithms
3. Define how encryption, hashes and digital signatures can increase the security of their network
4. The role and operation of public and private keys in improving network security
5. Provide an overview of cryptography standards and where they are used
6. The operation of VPN’s and how they can improve network security
7. The basic operation of IPSec (Lab demonstration)
8. The operation of tunneling across a network (Lab demonstration)
9. The function and operation of IPSec VPN (Lab demonstration)