**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)

Router>

Router>en

Router#conf t

Enter Configuration commands, one per line. End with CNTL/Z.

Router(config)#username admin password cisco

Router(config)#

1. Implement user command privileges for their networking devices (Lab demonstration)

Router>sh

Router>sh pri

Router>sh privilege

Current privilege level is 1

Router>

Router>enable 15

Router#sh pri

Router#sh privilege

Current privilege level is 15

Router#pti

Router#pri

Router#sh pri

Router#sh privilege

Current privilege level is 15

Router#?

Enter Commands:

<1-99>

auto

clear

clock

configure

connect

copy

debug

delete

disable

disconnect

enable

erase

exit

logout

mkdir

more

no

ping

reload

resume

rmdir

send

setup

show

ssh

telnet

terminal

traceroute

undebug

vlan

write

1. Implement security features in the IOS of their networking devices (Lab demonstration)`

line con 0

exec-timeout <minutes> [seconds]

line vty 0 4

exec-timeout <minutes> [seconds]

no service password-recovery

1. Implement AAA for their network devices (Lab demonstration)

aaa new-model

aaa authentication login default group tacacs+!

tacacs-server host <ip-address-of-tacacs-server>

tacacs-server key <key>

1. Demonstrate both Standard and extended access lists to improve the security of ABC Widget Franchise’s network (Lab demonstration)

TACACS+ authentication, or additional typically AAA authentication, provides the power to use individual user accounts for every network administrator. after you do not depend upon one shared secret, the protection of the network is improved, and your answerability is strong.

RADIUS may be a protocol similar in purpose to TACACS+; but it solely encrypts the watchword sent across the network. In distinction, TACACS+ encrypts the whole communications protocol payload, which incorporates each the username and watchword. For this reason, TACACS+ ought to be utilized in preference to RADIUS once TACACS+ is supported by the abdominal aortic aneurysm server.

router(config)#ip access-list standard {access-list-name}

router(config)#ip access-list extended {access-list-name}

standard access-list - you can permit the IP address but you cant control the destination. extended access list- you can permit/block the IP at the same time you can control the the destination of the source

1. Provide a report on firewall technologies: (You will brief representatives of the ABC Widget Franchise on the report outcomes)
   1. Zone based firewalls

A zone-based firewall is a type of stateful firewall that is more complex. A stateful database is kept in a stateful firewall, where the source IP address, destination IP address, source Port number, and destination Port number are all stored.

* 1. Packet filtering

Packet filtering may be a firewall technique wont to management network access by watching outgoing and incoming packets and permitting them to pass or halt supported the supply and destination net Protocol (IP) addresses, protocols and ports.

* 1. Introduction to inspection rules

A review is, most usually, associate degree organized examination or formal analysis exercise. In engineering activities review involves the measurements, tests, associate degreed gauges applied to sure characteristics in respect to an object or activity. The results square measure sometimes compared to such necessities and standards for determinative whether the item or activity is in line with these targets, typically with a customary review Procedure in situ to confirm consistent checking. Inspections square measure sometimes non-destructive.

* 1. Concepts of higher level packet inspection

Deep packet review (DPI) is a complicated methodology of examining and managing network traffic. it is a style of packet filtering that locates, identifies, classifies, reroutes, or blocks packets with specific knowledge or code payloads that typical packet filtering, that examines solely packet headers, cannot discover.

* 1. How dynamic address updates can be used against cyber attacks

Dynamic IP addresses are an efficient thanks to defeat IP-based defense systems: launch application-level attacks that originate from real—but dynamic—IP addresses.

* 1. New firewall technologies

A next-generation firewall (NGFW) will this, so rather more. additionally, to access management, NGFWs will block trendy threats like advanced malware and application-layer attacks. per Gartner's definition, a next-generation firewall should include: normal firewall capabilities like stateful scrutiny.

1. Demonstrate IPS principles using the features of a networking device IOS

Intrusion Prevention System Concepts

Intrusion prevention systems scan network traffic as it passes through the network; unlike intrusion detection systems, which are designed to react, intrusion prevention systems are designed to prevent malicious events from occurring by blocking attacks as they occur. An IPS can protect against a variety of attack types, including

Denial of Service

Distributed Denial of Service

Exploits (Various types)

Worms

Viruses

1. Clarify how signatures are used to detect malicious traffic

When a signature is downloaded from Cisco, it is given a specific action that will be taken if the event is identified. There are a total of five options for you to choose from:

produce-alert—Sends an alarm when a signature is detected

deny-packet-inline—Drops the packet which contained the signature that was detected, but does not reset the connection

reset-tcp-connection—Sends a TCP reset to both the attacker and the destination host

deny-attacker-inline—Denies traffic from the IP address of the offending traffic with a dynamic access list

deny-connection-inline—Denies traffic from the offending traffic session with a dynamic access list

On the IOS IPS device, any of these five functions can be coupled and personalised to specific signatures. In the past, these actions could be customized with Security Device Manager (SDM), however, with IOS version 12.4(11)T and later, the use of SDM has been depreciated and the use of Cisco Configuration Professional (CCP)(Single device), Cisco Security Manager (CSM)(Up to 5 devices) or direct IOS

**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

There is area unit 5 primary functions of cryptography: Privacy/confidentiality: guaranteeing that nobody will scan the message except the meant receiver. Authentication: the method of proving one's identity. Integrity: reassuring the receiver that the received message has not been altered in any manner from the first.

1. Define the difference between symmetric and asymmetric algorithms

The basic difference between symmetric and asymmetric key cryptography is that symmetric encryption requires the same key to be encrypted and decrypted. In the other hand, asymmetric encryption uses a key for encryption and uses another key for decryption. It is also known as public-key cryptography.

1. Define how encryption, hashes and digital signatures can increase the security of their network

Cryptography is that the follow and study of secure communication within the presence of third parties. within the past cryptography referred largely to secret writing. secret writing is that the method of changing plain text data to ciphertext. The reverse is that the cryptography. secret writing could be a mechanism to create the data confidential to anyone except the needed recipients. Cipher is that the combine of algorithms that makes secret writing and cryptography. Cipher operation depends on the formula and therefore the key. secret is the key that far-famed by communicants.

1. The role and operation of public and private keys in improving network security

The public key is accustomed inscribe and a personal secret is accustomed decipher the info. personal secret is accustomed each inscribe and decipher knowledge the info the information} and is shared between the sender and receiver of encrypted data. the public secret is solely accustomed inscribe knowledge and to decipher the info, the personal secret is used and is shared.

1. Provide an overview of cryptography standards and where they are used

Users of the former "Crypto Toolkit" can now find that content under this project. It includes cryptographic primitives, algorithms and schemes are described in some of NIST's Federal Information Processing Standards (FIPS), Special Publications (SPs) and NIST Internal/Interagency Reports (NISTIRs).

#### Crypto Standards and Guidelines Activities

* [Block Cipher Techniques](https://csrc.nist.gov/projects/block-cipher-techniques)
* [Digital Signatures](https://csrc.nist.gov/projects/digital-signatures)
* [Hash Functions](https://csrc.nist.gov/projects/hash-functions)
* [Key Management](https://csrc.nist.gov/projects/key-management)
* [Lightweight Cryptography](https://csrc.nist.gov/projects/lightweight-cryptography) (LWC)
* [Message Authentication Codes](https://csrc.nist.gov/projects/message-authentication-codes) (MACs)
* [Post-quantum Cryptography](https://csrc.nist.gov/projects/post-quantum-cryptography) (PQC)
* [Privacy-Enhancing Cryptography](https://csrc.nist.gov/projects/pec) (PEC)
* [Random Bit Generation](https://csrc.nist.gov/projects/random-bit-generation)
* [Threshold Cryptography](https://csrc.nist.gov/projects/threshold-cryptography) (TC)

1. The operation of VPN’s and how they can improve network security

A VPN connection establishes a secure connection between you and the internet. Via the VPN, all your data traffic is routed through an encrypted virtual tunnel. This disguises your IP address when you use the internet, making its location invisible to everyone. A VPN connection is also secure against external attacks.

1. The basic operation of IPSec (Lab demonstration)

Router(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

Router(config)# crypto isakmp policy 10

Router(config-isakmp)# encryption aes

Router(config-isakmp)# authentication pre-share

Router(config-isakmp)# group 2

Router(config-isakmp)# exit

Router(config)# crypto isakmp key cisco address 10.2.2.2

1. The operation of tunneling across a network (Lab demonstration)
2. The function and operation of IPSec VPN (Lab demonstration)

(8 & 9 Combined)

Router# show crypto ipsec sa

interface: Serial0/0/0

Crypto map tag: VPN-MAP, local addr 10.1.1.2

protected vrf: (none)

local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)

current\_peer 10.2.2.2 port 500

PERMIT, flags={origin\_is\_acl,}

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0

#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0

current outboun d spi: 0x0(0)

<output omitted>

Ping PC-C from PC-A

Router# show crypto ipsec sa

interface: Serial0/0/0

Crypto map tag: VPN-MAP, local addr 10.1.1.2

protected vrf: (none)

local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)

current\_peer 10.2.2.2 port 500

PERMIT, flags={origin\_is\_acl,}

#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0

#pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 1, #recv errors 0

local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0

current outbound spi: 0x0A496941(172583233)

<output omitted>

Ping PC-B from PC-A.

On R1, re-issue the show crypto ipsec sa command. Finally, notice that the number of packets has not changed verifying that uninteresting traffic is not encrypted