20BCE1707

VIT
Vellore Institute of Technology

Continuous Assessment Test- I (CAT-I) – January 2023

Programme	: **B.Tech**		Semester	:	**WS 2022-23**
			Code	:	**CSE3502**
Course Title	: **Information Security Management**		Slot	:	**G2**
Faculty	: **Dr.Anusha K, Dr.Nachiyappan S, Dr.Braveen M, Dr.Ayesha S K**		Class Nbr	:	**CH2022235000336, CH2022235000340, CH2022235000338, CH2022235000342**
Time	: **90 Minutes**		Max. Marks	:	**50**

Q.No.	Sub. Sec.	Question Description	Marks
1		Assume you are a network security corporate trainer; your role is to train the network administrator of the company for providing security to the company's devices and on the network segmentation process. i) Identify the possible threats which would occur in the company if security measures are not being taken. (2 Marks) ii) Enlighten the steps to be provided by the trainer to ensure the data security of the company against various data threats. (3 Marks) iii) Elaborate on the responsibilities of Security Information and Event Management (SIEM) in the design of Intrusion Detection and Prevention systems. (3 Marks) iv) Explain the steps for preventing the DDoS attack. (2 Marks)	10
2		Demonstrate the Configuration steps for the given network topology using static and dynamic Network Address Translation (NAT).	10
3		Design a network topology with 7 PC's, 3 servers, 3 laptops, 1 router and 1 switch for an event management company which is organizing 4 events. Events celebrated are Marriage, Farewell, School Annual Day, and Birthday. The Marriage event requires 2 PC's and one	10

server. The Farewell event requires one PC, one server, and one laptop. The School annual day event requires 2 PC's and 2 laptops. The birthday event requires 2 PC's and one server.

(i) Discuss the process in detail to access the given network devices within the event and no access outside event for the above scenario (5 Marks)

(ii) Justify whether it is possible to provide access to given network devices outside the event. (5 Marks)

4 A leading private bank plans to configure the IPSec tunnelling using the Application layer protocols for their network to enable an https server located in a branch office which needs to be securely accessed from remote locations. The bank approaches ABITs Solutions Pvt Ltd., which provides networking solutions. Assume yourself as a network security analyst working for ABITs Solutions Pvt Ltd., and you are being given a task to configure the IPSec tunnelling with the help of appropriate commands. Provide suitable topological representation for the same. 10

5 An organization 'X' have a network topology with four LANs and it is connected to WAN. For the given network scenario, with the help of topological representation, answer the following : (1 Mark for Diagram) 10

i) Identify the security device that can be used to connect LAN and WAN. (1 Mark)

ii)Elucidate the different types of attacks which would occur on LAN and WAN (2 Marks)

iii) Illustrate the ways through which the attack can occur. (2 Marks)

v) What security measures can be taken to prevent the attack? (1 Mark)

vi) The CEO of the organization doesn't want his identity to be known when he accesses the internet. Identify the system which he would require to hide his identity. Explain how it works. (3 Marks)

VIT®

Vellore Institute of Technology

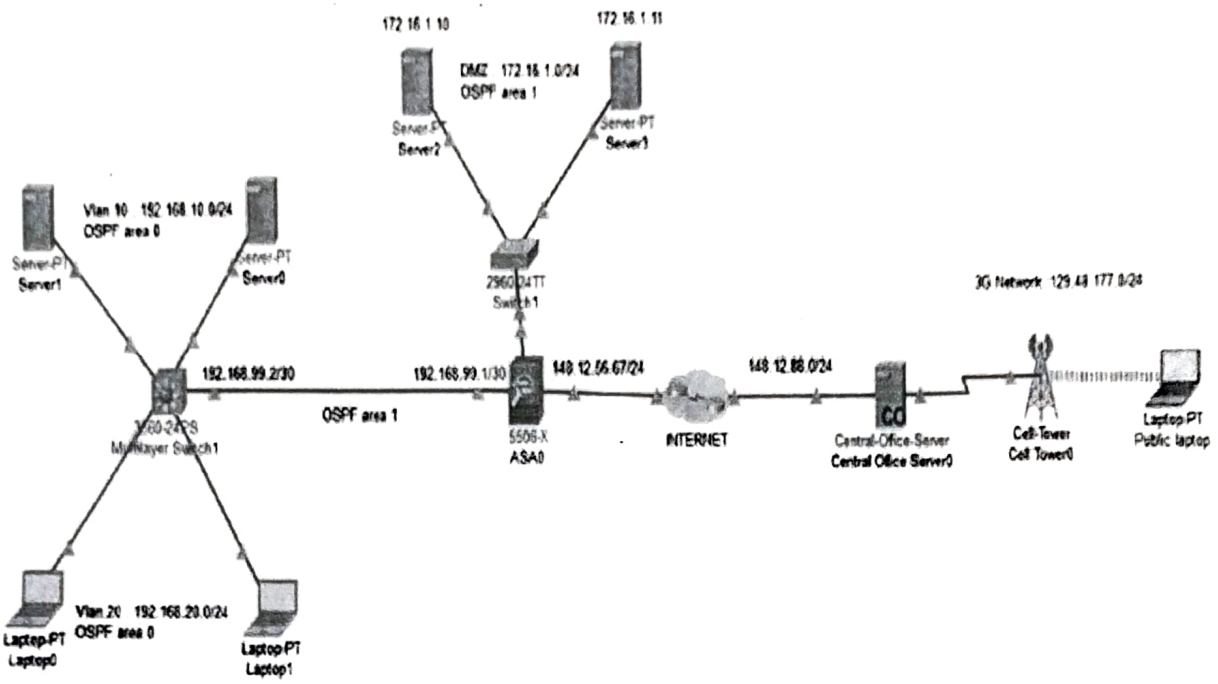
(Deemed to be University under section 3 of UGC Act, 1956)

Continuous Assessment Test- II (CAT-2) –March 2023

Programme	: **B. Tech.,**	Semester	:	**WS 2022-23**
Course Title	: **Information Security Management**	Code	:	**CSE3502**
		Slot	:	**G2**
Faculty	: **Dr. Anusha K, Dr.Nachiyappan S, Dr. Braveen M, Dr. Ayesha S K**	Class Nbr	:	**CH2022235000336, CH2022235000340, CH2022235000338, CH2022235000342**
Time	: **90 Minutes**	Max. Marks	:	**50**

Q.No.	Sub. Sec.	Question Description	Marks
1		Assume that, Mr. Bean is browsing the Internet with any of the known browsers. (a) Case 1: One of his friend Mr. Popeye is sending a malicious script in such a way that, Mr. Bean is believing that the script has come from a trusted source. (b) Case 2: Similarly, Mr. Popeye is forcing Mr. Bean to execute unwanted actions on a web application in which he is authenticated. To carry out the above action, Mr. Popeye is sending a link viz. email or chat. Now, identify the type of attack (both cases a and b) raised by Mr. Popeye towards Mr. Bean and explain it with neat diagrams. In addition to the above, both cases a and b, clearly state what are the impact of attacks and their limitations.	*10*
2		In recent times, many colleges and universities continue to find themselves as the targets of large-scale cyber-attacks. It is a known fact that these educational institutions always possess valuable information about their faculty members, students and hence attackers are actively working to steal that information. As a precautionary step, Vellore Institute of Technology (VIT) Chennai Campus is planning to install Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) to defend against these attacks. For the above scenario, identify and explain in detail about appropriate IDS and IPS methods to configure rules for port scanning and also to set the default action as DROP.	10

3



15

Consider the above topology in which all the routers and switch devices have been preconfigured. The topology is found to have multiple devices along with their connections. The diverse operations of the above devices require a special method to handle their connectivity with individual devices. Therefore, identify and apply appropriate CISCO Adaptive Security Appliance (ASA) to:

(*i*) Verify Connectivity and Explore the ASA. (7 Marks)

(ii) *Troubleshoot* the firewall. (8 Marks)

4 Mr. Alex is currently serving as an Inspector of Police in Chengalpattu area. As a policeman, he receives n number of messages threatening him that he will be killed. Despite taking it as a normal threat, the policemen again received a life threat message. The threat message was constructed with a combination of words, letters and images that are extracted from the magazine and glued to a piece of paper. Later, Mr. Alex received a dead cockroach taped to an index card with a straight pin through the body. The message written on the card was, "This could be you in near future". Now, by seeing the threats, how will you face the above situation? Explain the ways and steps involved in identifying the culprit behind this with solid evidence to oppose the threat messages raised by him. 5

5 PlipKart is an e-commerce company is holding more than 15 million customers. They have a festival offer week in the month of January, May and December. After one month of sales, below is the sequence of events that may occur: 10

- Suddenly a lot of customers reported that the website is not accessible.
- Month – 1 sale (Orders were high but revenue was low).
- Antivirus software alerts when it detects that a host is infected with malware
- A system administrator sees a filename with unusual characters
- An application logs multiple failed login attempts from an unfamiliar remote system
- A network administrator notices an unusual deviation from typical network traffic flows.
- A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server.

For the above scenario, as a security analyst, you are supposed to handle the security controls, policies, procedures, plans, cybersecurity challenges and risks towards your business growth and technological operations. Discuss in detail the need for auditing template framework, identify and fix the case study with required documentation.