PL Quiz 3

Due No due date	Points 57	Questions 30	Available Sep 12 at 3pm - Sep 12 at 3:20pm 20 minutes
Time Limit 20 Minute	es		

Instructions

Answer the quiz according to what is needed, this quiz is composed of multiple choice with multiple answers, fill in the blanks and Essay question. Take note that the quiz is time limited so make the most of your time, you cannot return to the previous questions, therefore make sure of your answers. If you cannot submit the quiz on time, the system will automatically submit your scores. Good luck!!!

This quiz was locked Sep 12 at 3:20pm.

Attempt History

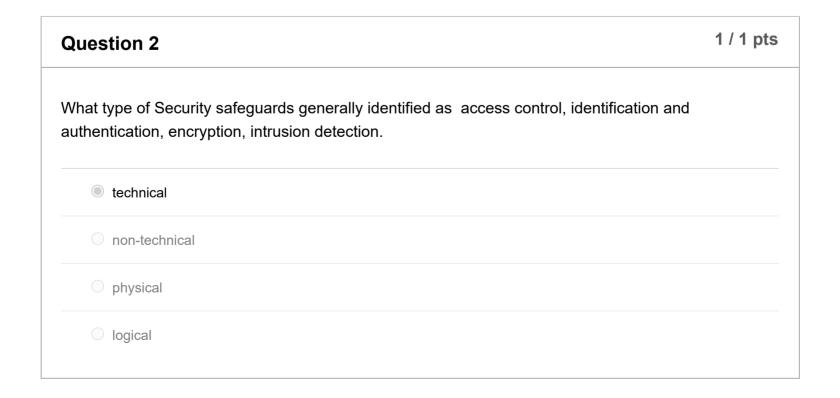
	Attempt	Time	Score
LATEST	Attempt 1	19 minutes	46 out of 57 *

^{*} Some questions not yet graded

! Correct answers are hidden.

Score for this quiz: **46** out of 57 * Submitted Sep 12 at 3:20pm This attempt took 19 minutes.

Question 1	2 / 2 pts
What are the two reasons why Business planning always involves a tradeoff between cost benefits.	and
Costs come in various forms.	
Potential for loss	
Business reputation	
Legislative and regulatory mandates	
Business is inherently profit-driven.	



Question 3	2 / 2 pts
What are the Functional Components of Information assurance? Choose all that apply.	
✓ protection	
impacts and losses to their opponents	
infrastructure systems	
cyber space protection	
capability restoration	
detection	
response	

Question 4	1 / 1 pts
An asset like devices, computers, people that have value so are worth protecting?	
non technical assets	
technical assets	
 systems assets 	
O logical assets	
physical assets	

Question 5	1 / 1 pts
A is a category of entities, or a circumstance, that poses a potential danger to a (through unauthorized access, destruction, disclosure, modification or denial of service). answer in lowercase only.	n asset
threat	

Question 6	1 / 1 pts
What federal law established in 1974, that pertains to the release of and access to educational records?	
answer in lowercase only.	

family educational rights and privacy act

Question 7	1 / 1 pts
What specific HIPAA Admin Security Safeguards that focuses on authorization and superviolearance termination procedures. answer in lowercase only.	rision,
workforce security	

Question 8	1 / 1 pts
A model of operation for computers handling classified information which all users are clear information on machine, no need for access control (MILS);	ared for all
system-high	
O multi-level	
dedicated	
○ compartmented	

Question 9	1 / 1 pts
A model of operation for computers handling classified information all users cleared, but representation of the need-to-know compartments (mandatory access control). System must handle requests a classifications.	
compartmented	
dedicated	
system-high	
O multi-level	

Question 10 1 / 1 pts

This act expressly prohibits the government from propagandizing the American public with information and psychological operations directed at foreign audiences.

answer in lower case only

smith-mundt act

Question 11	1 / 1 pts
A is a weakness or fault in a system that exposes information to attached answer in lowercase only vulnerability	ack.
Question 12	1 / 1 pts
A is one that does not pose a danger as there is no vulnerability to expethere, but can't do damage). answer in lowercase only dangling threat	oloit (threat is
Question 13	1 / 1 pts
A follow-on to Health Insurance Portability and Accountability Act that provides addition relating to financial reporting and disclosure.	nal protection
physical security	
Security Rule Privacy Rule	
technical security	
Patient's Omnibus Transaction on Mandatory Information Security	
Question 14	1 / 1 pts
At what categories of HIPAA safeguards does these belongs: Facility Access Controls, Workstation Use, Workstation Security, Device and Media Coanswer in lowercase only.	ntrols.

physical security

Question 15	1 / 1 pts
What HIPAA technical security safeguard categories which provides unique user ID, emeraces procedures, automatic logoff, encryption and decryption.	rgency
answer in lowercase only.	
access control	

Question 16	1 / 1 pts
An the term is a recognized action—specific, generalized or theoretical—that a (threat actor) might be expected to take in preparation for an attack.	n adversary
Object	
exposure	
indicator	
compromise	

Question 17	1 / 1 pts
is the possibility that a particular threat will adversely impact an information system exploiting a particular vulnerability. answer in lowercase only.	ı by
risk	

Question 18	1 / 1 pts
is a process for an organization to identify and address the potential threat in environment. answer in lowercase only	their
risk management	

Question 19 4 / 4 pts

What composes OODA? write your answer in lowercase

observe		
orient		
decide		
act		
Answer 1: observe		
Answer 2:		
orient		
Answer 3:		
decide		
Answer 4:		
act		

Question 20

It is the act or practice of obtaining secrets from individuals, competitors, rivals, groups, governments and enemies also for military, political, or economic advantage using illegal exploitation methods on internet, networks, software and or computers.

answer in lowercase only.

cyber espionage

Military activities that use computers and satellites for coordination are at risk from this type of attack.

Orders and communications can be intercepted or replaced, putting soldiers at risk.

Distributed Denial-of-Service Attacks

Gathering data

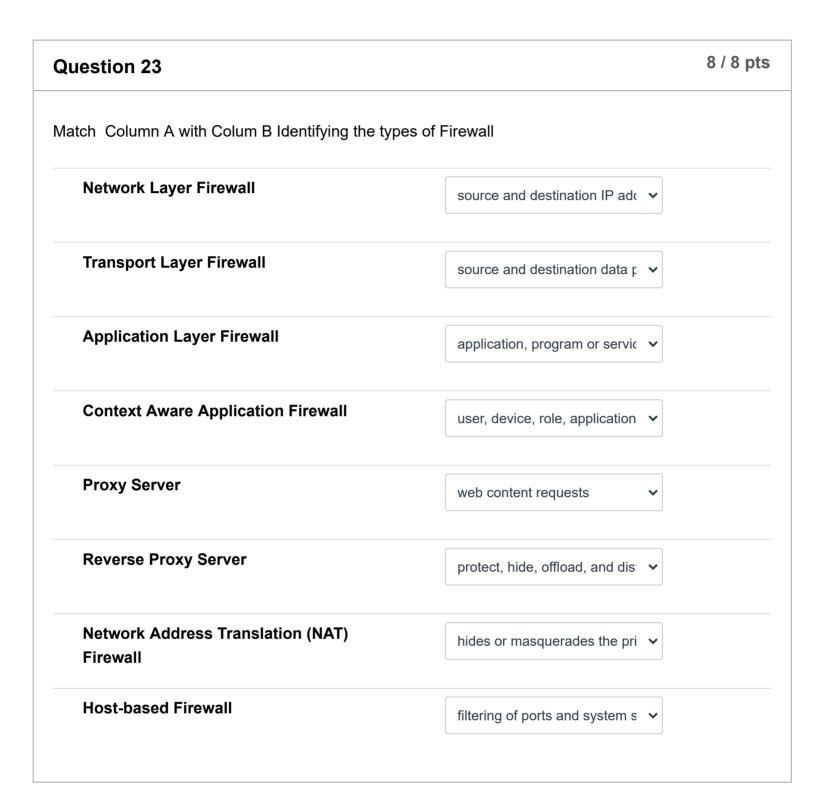
Propaganda

Equipment disruption

Web vandalism

Question 22 1 / 1 pts

Process o	of probing a computer, server or other network host for open ports
O Wil	reshark
○ Re	connaissance
O Po	rt Forwarding
Po	rt Scanning



Question 24	1 / 1 pts
A Type of security appliance that can have many firewall capabilities like traffic filtering, IPS encryption, and VPN.	S,
O IPS	
O VPN	
o routers	
○ firewall	

PL Quiz 3: Group 1 CS 3106 - INFORMATION ASSURANCE AND SECURITY	
Question 25	1 / 1 pts
These are next generation Cisco routers, firewalls, IPS devices, Web and Email Security and can also be installed as software in host computers.	Appliances
Routers	
O IPS	
O Firewall	
Advanced Malware Protection	
Question 26	0 / 1 pts

Incorrect

Question 26	0 / 1 pts
This is an attack that exploits a potentially serious software security weakness that the developer may be unaware of.	endor or
O ddos	
malware	
○ zero day attack	
Odos	

Question 27	1 / 1 pts
A cyber-attack in which the perpetrator seeks to make a machine or network resource unaits intended users by temporarily or indefinitely disrupting services of a host connected to the	
○ Worm	
Trojan	
ODOS	
DDos	

Question 28	1 / 1 pts
A number of Internet-connected devices, each of which is running one or more bots. T to perform Distributed Denial-of-Service (DDoS) attacks, steal data, send spam, and a to access the device and its connection.	
botnet	
O bot	
○ malware	

worm

Question 29	7 / 7 pts
Arrange the following stages o	of a Kill Chain in an information systems attack.
[Select]	Stage 1:
[Select]	Stage 2:
[Select]	Stage 3:
[Select]	Stage 4:
[Select]	Stage 5:
Command and Control - Ren 6:	note control from a command and control channel or server. Stage
[Select]	Stage 7:
Answer 1: Reconnaissance – Gathers in	formation
Answer 2:	
Weaponization - Creates targe	eted exploit and malicious payload
Answer 3:	
Delivery - Sends the exploit a	nd malicious payload to the target
Answer 4:	
Exploitation – Executes the ex	kploit
Answer 5:	
Installation - Installs malware	and backdoors
Answer 6:	
Command and Control - Rem	ote control from a command and control channel or server.
Answer 7:	
Action – Performs malicious a	actions or additional attacks on other devices

Question 30

Not yet graded / 10 pts

Differentiate the use of IPS and IDS? Define and give examples.

Your Answer:

IPS or Intrusion Prevention System provides the network with the feature of traffic blocking. It denies traffic based on a certain condition called a signature match while IDS, Intrusion Detection System,

does not prevent traffic. It simply detects such intrusions and creates a log.

An example of an IPS system is Sourcefire while and example of an IDS system is Snort.

Quiz Score: 46 out of 57