

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 Minutes

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 and benefits.

☒ Costs come in various forms.

☐ Potential for loss

☐ Business reputation

☐ Legislative and regulatory mandates

☒ Business is inherently profit-driven.

Question 2

1 / 1 pts

What type of Security safeguards generally identified as access control, identification and authentication, encryption, intrusion detection.

☒ technical

☐ non-technical

☐ physical

☐ logical

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

☐ logical assets

☒ physical assets

Question 5

1 / 1 pts

A _____ is a category of entities, or a circumstance, that poses a potential danger to an asset (through unauthorized access, destruction, disclosure, modification or denial of service).

answer in lowercase only.

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 supervision, clearance termination procedures.

answer in lowercase only.

workforce security

Question 8

1 / 1 pts

A model of operation for computers handling classified information which all users are cleared for all information on machine, no need for access control (MILS);

☐ system-high

☐ multi-level

☒ dedicated

☐ compartmented

Question 9

1 / 1 pts

A model of operation for computers handling classified information all users cleared, but must be need-to-know compartments (mandatory access control). System must handle requests across classifications.

☒ compartmented

☐ dedicated

☐ system-high

☐ 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 attack.

answer in lowercase only

vulnerability

Question 12

1 / 1 pts

A _____ is one that does not pose a danger as there is no vulnerability to exploit (threat is there, but can't do damage).

answer in lowercase only

dangling threat

Question 13

1 / 1 pts

A follow-on to Health Insurance Portability and Accountability Act that provides additional protection relating to financial reporting and disclosure.

- ☐ 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 Controls.

answer in lowercase only.

physical security

Question 15

1 / 1 pts

What HIPAA technical security safeguard categories which provides unique user ID, emergency access procedures, automatic logoff, encryption and decryption.

answer in lowercase only.

access control

Question 16

1 / 1 pts

An the term _____ is a recognized action—specific, generalized or theoretical—that an adversary (threat actor) might be expected to take in preparation for an attack.

☐ object

☐ exposure

☒ indicator

☐ compromise

Question 17

1 / 1 pts

_____ is the possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability.

answer in lowercase only.

risk

Question 18

1 / 1 pts

_____ is a process for an organization to identify and address the potential threat in their environment.

answer in lowercase only

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

1 / 1 pts

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

Question 21

1 / 1 pts

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 of probing a computer, server or other network host for open ports

- ☐ Wireshark
- ☐ Reconnaissance
- ☐ Port Forwarding
- ☒ Port Scanning

Question 238 / 8 pts

Match Column A with Column B Identifying the types of Firewall

Network Layer Firewall	source and destination IP address
Transport Layer Firewall	source and destination data port
Application Layer Firewall	application, program or service
Context Aware Application Firewall	user, device, role, application
Proxy Server	web content requests
Reverse Proxy Server	protect, hide, offload, and distribute
Network Address Translation (NAT) Firewall	hides or masquerades the private IP
Host-based Firewall	filtering of ports and system services

Question 241 / 1 pts

A Type of security appliance that can have many firewall capabilities like traffic filtering, IPS, encryption, and VPN.

- ☐ IPS
- ☐ VPN
- ☒ routers
- ☐ firewall

Question 25

1 / 1 pts

These are next generation Cisco routers, firewalls, IPS devices, Web and Email Security Appliances and can also be installed as software in host computers.

☐ Routers

☐ IPS

☐ Firewall

☒ Advanced Malware Protection

Incorrect

Question 26

0 / 1 pts

This is an **attack** that exploits a potentially serious software security weakness that the vendor or developer may be unaware of.

☐ ddos

☒ malware

☐ zero day attack

☐ dos

Question 27

1 / 1 pts

A cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

☐ Worm

☐ Trojan

☐ DOS

☒ DDos

Question 28

1 / 1 pts

A number of Internet-connected devices, each of which is running one or more bots. This can be used to perform Distributed Denial-of-Service (DDoS) attacks, steal data, send spam, and allow the attacker to access the device and its connection.

☒ botnet

☐ bot

☐ malware

☐ worm

Question 29

7 / 7 pts

Arrange the following stages 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 - Remote control from a command and control channel or server. Stage 6:

[Select] Stage 7 :

Answer 1:

Reconnaissance – Gathers information

Answer 2:

Weaponization - Creates targeted exploit and malicious payload

Answer 3:

Delivery - Sends the exploit and malicious payload to the target

Answer 4:

Exploitation – Executes the exploit

Answer 5:

Installation - Installs malware and backdoors

Answer 6:

Command and Control - Remote control from a command and control channel or server.

Answer 7:

Action – Performs malicious 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 an example of an IDS system is Snort.

Quiz Score: **46** out of 57