

MT Quiz 1

Due No due date **Points** 25 **Questions** 17
Available after Sep 26 at 3pm **Time Limit** 10 Minutes

Attempt History

| | Attempt | Time | Score |
|--------|---------------------------|------------|--------------|
| LATEST | Attempt 1 | 10 minutes | 12 out of 25 |

Score for this quiz: **12** out of 25

Submitted Sep 26 at 3:10pm

This attempt took 10 minutes.

Question 1

3 / 3 pts

These are the framework used to manage the activity of the user to a network that it wants to access.

authentication

authorization

accounting

Answer in order and in lowercase only.

Answer 1:

authentication

Answer 2:

authorization

Correct!

Correct!

Answer 3:**Correct!**

accounting

Question 2**0 / 1 pts**

It is the process of recognizing a user's identity and the mechanism of associating an incoming request with a set of identifying credentials.

answer in lowercase only.

You Answered

authorization

Correct Answers

authentication

Question 3**1 / 1 pts**

This command refers to the use of method lists by which AAA methods and sources can be grouped or organized.

☐ new-model aaa☐ aaa new model☐ new model aaa☒ aaa new-model**Correct!**

Question 4**1 / 1 pts**

It is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

Correct!

- ☐ radius
- ☒ firewall
- ☐ tacacs+
- ☐ aaa authenticaion

Question 5**1 / 1 pts**

A type of firewall that combines traditional firewall technology with additional functionality, such as encrypted traffic inspection, intrusion prevention systems, anti-virus, and more.

Correct!

- ☐ Proxy Firewall
- ☐ Network address translation
- ☒ Next-generation firewalls
- ☐ Stateful Multi-layer Inspection

Question 6**1 / 1 pts**

A type of firewall that filters packets at the network, transport, and application layers, comparing them against known trusted packets, it also examines the entire packet and only allows them to pass if they pass each layer individually.

Correct!

- ☒ Stateful multilayer inspection
- ☐ Cloud Firewalls
- ☐ Next-generation Firewalls
- ☐ Unified Threat Management

Question 7**1 / 1 pts**

This is a CISCO full-featured firewall MODEL for small business, branch, and enterprise teleworker environments. It delivers a high-performance firewall, SSL and IPsec VPN, and rich networking services in a modular, immediately operational appliance.

answer in lowercase, no shortcuts, no abbreviation, no acronyms, include the model #

Correct!

adaptive security appliance 5505

Correct Answers

adaptive security appliance 5506
adaptive security appliance 5505

Question 8**0 / 1 pts**

A command in the firewall that is used to customize the name an interface.

answer in lowercase, no shortcuts, no abbreviation, no acronyms,

You Answered**Correct Answers**

nameif

Question 9**1 / 1 pts**

This is the security level on the ASA and by default, it is assigned to the “outside” interface.

- ☐ security level 1
- ☐ security level 99
- ☐ security level 100
- ☒ security level 0

Correct!**Question 10****0 / 1 pts**

To create any other security levels that we want, for example, we can use the security level for DMZ, what would be the appropriate security level number?

You Answered

☒ 100

☐ 0

Correct Answer

☐ 50

☐ 1

Question 11

1 / 1 pts

Which of the following is the correct command to create a dhcp in ASA?

Correct!

☒ dhcp address 192.168.1.10-192.168.1.20 inside

☐ dhcp address range 192.168.1.10-20 inside

☐ ip dhcp address range 192.168.1.10-20

☐ ip dhcp address 192.168.1.10-192.168.1.20 inside

☐ ip dhcp address 192.168.1.10-192.168.1.20 inside

Question 12

1 / 1 pts

In the command dhcp option 3 IP 192.168.1.1, what does option 3 means?

answer in lowercase, no shortcuts, no abbreviation, no acronyms,

Correct!

default gateway

Correct Answers

gateway

default gateway

Question 13

0 / 1 pts

What command is used to enable the DHCP daemon within the ASA to listen for DHCP client requests on the enabled interface?

You Answered

dhcp enable outside

Correct Answers

dhcp enable inside

Question 14

0 / 1 pts

What command in R1 is used to implement the default static route in ASA?

R1 int S0 - 10.10.10.1

R1 int S1 - 10.10..10.2

You Answered

#ip route 0.0.0.0 0.0.0.0 10.0.0.2

Correct Answers

route outside 0.0.0.0 0.0.0.0 10.10.10.2

Question 15

1 / 3 pts

Which of the following are the commands used to implement NAT in Cisco ASA Firewall?

Answer should be in order.

You Answered

Step 1

service-policy global_ ▼

Correct Answer

object network
INSIDE-NET

You Answered

Step 2

nat (inside,outside)dy ▼

Correct Answer

subnet 192.168.1.0
255.255.255.0

Correct!

Step

nat (inside,outside)dyr ▼

Other Incorrect Match Options:

- nat (inside,outside)dynamic default
- route outside 0.0.0.0 0.0.0.0 10.1.1.2

- service-policy global_policy global
- match default-inspection-traffic
- subnet 0.0.0.0 0.0.0.0
- dhcp enable inside
- login authentication default

Question 16**0 / 3 pts**

Which of the following are the commands used to implement or create a global policy?

Answer should be in order.

You Answered

Step 1

inspect icmp

**Correct Answer**policy-map
global_policy

You Answered

Step 2

policy-map global_po

**Correct Answer**class
inspection_default

You Answered

Step 3

service-policy global_

**Correct Answer**

inspect icmp

Other Incorrect Match Options:

- route outside 0.0.0.0 0.0.0.0 10.1.1.2
- dhcp enable inside

- class-map
- service-policy global_policy global
- match default-inspection-traffic

Question 17**0 / 3 pts**

What commands to use If you want to add permission to the firewall?

Answer should be in order.

ou Answered

Step 1

dhcp enable inside

**Correct Answer**

policy-map
global_policy

ou Answered

Step 2

service-policy global_

**Correct Answer**

class
inspection_default

ou Answered

Step 3

class inspection_defa

**Correct Answer**

inspect HTTP

Other Incorrect Match Options:

- match default-inspection-traffic
- service-policy global_policy global
- route outside 0.0.0.0 0.0.0.0 10.1.1.2
- class-map
- dhcp enable inside

Quiz Score: **12** out of 25

MT Quiz 2

Due No due date **Points** 55 **Questions** 20
Available after Sep 28 at 3pm **Time Limit** 30 Minutes

Attempt History

| | Attempt | Time | Score |
|--------|---------------------------|------------|----------------|
| LATEST | Attempt 1 | 28 minutes | 19 out of 55 * |

* Some questions not yet graded

! Correct answers are hidden.

Score for this quiz: **19** out of 55 *

Submitted Sep 28 at 3:28pm

This attempt took 28 minutes.

Question 1

1 / 1 pts

A branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime.

answer in lowercase, no abbreviation, no acronyms

digital forensics

Partial

Question 2

1 / 5 pts

Identify the digital forensic process as required in order to present the digital evidence in the court of law

answer in lowercase, no abbreviation, no acronyms

Step 1 :

Step 2 :

Step 3 :

Step 4 :

Step 5 :

Answer 1:

identifying

Answer 2:

imaging

Answer 3:

analysis

Answer 4:

reporting

Answer 5:

court presentation

Question 3

2 / 2 pts

Identify the two sets of data in digital forensics by matching column A with Column B.

Persistent data

type of data found in :

Volatile Data

This data will be lost i :

Question 4

1 / 1 pts

A person who has a desire to follow the evidence and solve a crime virtually.

-
- ☐ crime scene investigator
-
- ☐ crime of the scene operatives
-
- ☒ digital forensics investigator
-
- ☐ first responder

Question 5

1 / 1 pts

These are information about a person on the system, such as the webpages they have visited, when they were active, and what device they were using.

answer in lowercase, no abbreviation, no acronyms

digital footprint

Question 6

1 / 1 pts

These are data that is recorded or preserved on any medium in or by a computer system or other similar device, that can be read or understood by a person or a computer system, or other similar devices which are valuable to an investigation that is stored on received, or transmitted by an electronic device.

answer in lowercase, no abbreviation, no acronyms

digital evidences

Question 7

3 / 3 pts

Which of the following is not digital evidence?

Choose all that apply

☐ Electronic game devices☒ SIM Card☐ iPods☒ digital printout☒ digital calculators☐ Wireless access points☐ Answering Machine**Question 8****1 / 1 pts**

The first person notified, and take action to the security incident.

☐ crime scene investigator☒ first responder☐ scene of the crime operatives☐ digital forensics investigator**Incorrect****Question 9****0 / 1 pts**

This step in the digital forensic process where data should be relevant to the incident or crime, sources should maintain data integrity. Timely execution of this process is crucial in order to maintain the confidentiality

and integrity of the data. Important evidence may be lost if not acted as required.

- ☐ presentation
- ☐ collection/acquisition
- ☒ indentification
- ☐ analysis

Incorrect

Question 10

0 / 1 pts

This is a technique to allow a system to automatically maintain multiple copies of data so that in the event of a disk hardware failure a system can continue to process or quickly recover data.

- ☐ partitioning
- ☐ mirroring
- ☒ backup image
- ☐ forensic duplication

Question 11

3 / 3 pts

Identify the different types of Imaging Process by matching column A and Column B

Disk to disk

imaging is used when 

Disk to file

cloning of the original ▼

Files to File

imaging is same thing ▼

Incorrect**Question 12****0 / 1 pts**

It is the process of verifying the integrity of data or information, if not compromised by internal or external factors.

☐ presentation☐ identification☒ analysis☐ preservation☐ authentication**Question 13****1 / 1 pts**

Hardware that ensures that the evidence does not change once it was acquired and can ensure that the examination machine did not manipulate the original media.

☒ write blockers☐ hashing

☐ write protect

☐ imaging

Question 14

1 / 1 pts

The practice of taking a string or input key, a variable created for storing narrative data, and representing it with a value, determined by an algorithm that ensures that the information isn't altered during the course of investigation since various tools and techniques are involved in data analysis and evidence collection that can affect the data's integrity.

answer in lowercase, no abbreviation, no acronyms

hashing

Question 15

1 / 1 pts

A cryptographic hash function that uses 'one-way' compression function that takes an input of random size and produces an output of a fixed size.

☐ SHA 128

☒ SHA 256

☐ MD5

☐ Cryptographic Hash Function

Question 16**1 / 1 pts**

A well-documented _____ is essential to maintain the integrity of the evidence.

answer in lowercase, no abbreviation, no acronyms

chain of custody

Question 17**Not yet graded / 3 pts**

Why should your evidence media write-protected?

answer in one sentence only.

Your Answer:

To prevent sensitive data on a particular device from being altered or deleted.

Question 18**1 / 1 pts**

A legal term used to provide a sworn statement of support of facts about evidence of a crime is submitted to a judge with the request for a search warrant before seizing evidence.

answer in lowercase, no abbreviation, no acronyms

affidavit

Question 19

Not yet graded / 20 pts

Explain the digital forensic process and give examples of each step.

Your Answer:

Identification- This is where pieces of evidence are presented, stored and how they are stored. Examples are electronic storage media such as PC and mobile phones.

Imaging - In this phase, the pieces of evidence are isolated, secured, and preserved. To prevent people from altering or deleting valuable data.

Analysis - In phase, the examiner will analyze why these data are important and how they could support a specific crime theory.

Reporting - In this phase, a record or documentation of all the valuable data must be created. It will help the court to recreate the crime scene.

Court Presentation - This is the last process where summarization and explanation of the conclusion are done.

Question 20

Not yet graded / 6 pts

Why is handling digital evidence sometimes harder than the handling of "traditional" evidence?

Your Answer:

Digital evidence is harder than the handling of traditional evidence since digital pieces of evidence are volatile and fragile so if the evidence is handled improperly, it can lead to the deletion or alteration of pieces of evidence. So there are protocols needed to be followed to ensure the security of the evidence.

Quiz Score: **19** out of 55

MTQuiz2: Test3

Due Sep 29 at 7:30am**Points** 37**Questions** 28**Time Limit** 45 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!!!

Attempt History

| | Attempt | Time | Score |
|--------|---------------------------|------------|--------------|
| LATEST | Attempt 1 | 15 minutes | 32 out of 37 |

⚠ Correct answers are hidden.

Score for this quiz: **32** out of 37

Submitted Sep 28 at 6:14pm

This attempt took 15 minutes.

Question 1

2 / 2 pts

What are the two pre-historic computers used by military in Information Assurance?

☒ ENIAC☒ Bombe☐ UNIVAC☐ Analytical Engine

☐ EDSAC**Question 2****2 / 2 pts**

What are the two reasons why Business planning always involves a tradeoff between cost and benefits.

- ☐ Potential for loss
- ☐ Legislative and regulatory mandates
- ☒ Business is inherently profit-driven.
- ☐ Business reputation
- ☒ Costs come in various forms.

Incorrect**Question 3****0 / 2 pts**

What are the benefits of Information assurance for commercial enterprises. Choose all that apply.

- ☒ Enabling safe operation of business services
- ☐ Competitive advantage
- ☒ Providing for recovery in case of disaster
- ☐ Potential for loss
- ☒ Legislative and regulatory mandates

- ☒ Assisting the organization in meeting regulatory requirements

Question 4**1 / 1 pts**

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

- ☒ technical
- ☐ non-technical
- ☐ logical
- ☐ physical

Question 5**2 / 2 pts**

What are the Functional Components of Information assurance?

Choose all that apply.

- ☒ protection
- ☒ capability restoration
- ☐ cyber space protection
- ☒ detection
- ☐ infrastructure systems

☐ impacts and losses to their opponents

☒ response

Question 6

1 / 1 pts

An asset like devices, computers, people that have value so are worth protecting?

☐ non technical assets

☐ logical assets

☐ systems assets

☐ technical assets

☒ physical assets

Question 7

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 8**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 9**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 10**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.

☐ multi-level

- ☐ dedicated
- ☐ system-high
- ☒ compartmented

Question 11**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 12**1 / 1 pts**

A _____ is a weakness or fault in a system that exposes information to attack.

answer in lowercase only

vulnerability

Question 13**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 14

1 / 1 pts

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

- ☐ Security Rule
- ☐ physical security
- ☒ Patient's Omnibus Transaction on Mandatory Information Security
- ☐ Privacy Rule
- ☐ technical security

Question 15

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.

- ☒ indicator

☐ compromise

☐ exposure

☐ object

Question 16

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 17

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 18

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 19

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 20

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.

- ☒ Equipment disruption
- ☐ Distributed Denial-of-Service Attacks
- ☐ Web vandalism
- ☐ Gathering data
- ☐ Propaganda

Question 21

1 / 1 pts

Rearrange the letters to fill in the blank.



Behavior-based analysis involves using baseline information to detect _____ that could indicate an attack.

answer in lower case only.

anomalies

Question 22

1 / 1 pts

Which protocol is used by the Cisco Cyberthreat Defense Solution to collect information about the traffic that is traversing the network?

- ☒ NetFlow
- ☐ NAT
- ☐ Telnet
- ☐ HTTPS

Question 23

1 / 1 pts

Which stage of the kill chain used by attackers focuses on the identification and selection of targets?

- ☐ weaponization
- ☐ exploitation
- ☒ reconnaissance

☐ delivery

Incorrect

Question 24

0 / 1 pts

During a cyberwarfare attack, which group is responsible for disabling the firewalls and IDS systems of the target?

- ☒ backdoor team
- ☐ offensive operations teams
- ☐ internal users
- ☐ defense suppression team

Question 25

1 / 1 pts

Which security threat method would be used to target a specific demographic such as government workers for a particular country?

- ☐ cyberwar
- ☐ money mules
- ☐ cloud computing
- ☒ search engine optimization (SEO) poisoning

Question 26**1 / 1 pts**

True or False?

Cyberwarfare can be launched by a small group of highly skilled attackers.

☐ True

☒ False

Question 27**1 / 1 pts**

Refer to the exhibit. Rearrange the letters to fill in the blank.



A recommended Enterprise Security Architecture consists of 5 layers; Security Drivers, Security Program Management, Security Governance, Security _____ and Security Technology Architecture.

answer in lowercase only.

operations

Partial**Question 28****1 / 3 pts**

What are the three strategic end goals of cybersecurity? (Choose three.)

- ☐ detecting anomalies in the organization
- ☐ deterring and disrupting hackers
- ☒ preventing strategic collapse
- ☒ stopping the creation of malware
- ☒ protecting information assets
- ☐ preventing people from becoming hackers

Quiz Score: **32** out of 37

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 | 44 out of 57 * |

* Some questions not yet graded

❗ Correct answers are hidden.

Score for this quiz: **44** 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.

☒ Business is inherently profit-driven.

☐ Legislative and regulatory mandates

- ☐ Potential for loss
- ☒ Costs come in various forms.
- ☐ Business reputation

Question 2**1 / 1 pts**

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

- ☐ logical
- ☐ non-technical
- ☒ technical
- ☐ physical

Question 3**2 / 2 pts**

What are the Functional Components of Information assurance?

Choose all that apply.

- ☒ detection
- ☒ capability restoration
- ☐ infrastructure systems

☐ impacts and losses to their opponents

☐ cyber space protection

☒ protection

☒ response

Question 4

1 / 1 pts

An asset like devices, computers, people that have value so are worth protecting?

☐ non technical assets

☒ physical assets

☐ logical assets

☐ technical assets

☐ systems 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.

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.

Question 7**1 / 1 pts**

What specific HIPAA Admin Security Safeguards that focuses on authorization and supervision, clearance termination procedures.

answer in lowercase only.

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);

- ☒ dedicated
- ☐ multi-level
- ☐ system-high
- ☐ 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.

- ☐ dedicated
- ☒ compartmented
- ☐ 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.

- ☒ Patient's Omnibus Transaction on Mandatory Information Security
- ☐ Privacy Rule
- ☐ technical security
- ☐ physical security
- ☐ Security Rule

Incorrect**Question 14****0 / 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 safeguard

Technical Safeguard

Incorrect**Question 15****0 / 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.

technical safeguard

physical safeguard

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.

- ☒ indicator
- ☐ object
- ☐ exposure
- ☐ 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.

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.

- ☒ Equipment disruption
- ☐ Gathering data
- ☐ Propaganda
- ☐ Distributed Denial-of-Service Attacks
- ☐ Web vandalism

Question 22**1 / 1 pts**

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

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

Question 23

8 / 8 pts

Match Column A with Column B Identifying the types of Firewall

Network Layer Firewall

source and destination IP ✓

Transport Layer Firewall

source and destination port ✓

Application Layer Firewall

application, program or protocol ✓

Context Aware Application Firewall

user, device, role, application ✓

Proxy Server

web content requests ✓

Reverse Proxy Server

protect, hide, offload, and cache ✓

**Network Address
Translation (NAT) Firewall**

hides or masquerades traffic ▼

Host-based Firewall

filtering of ports and systems ▼

Question 24

1 / 1 pts

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

☒ routers

☐ firewall

☐ VPN

☐ IPS

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.

☐ Firewall

☐ IPS

☐ Routers

☒ 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.

- ☒ malware
- ☐ dos
- ☐ zero day attack
- ☐ ddos

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.

- ☒ DDos
- ☐ Worm
- ☐ DOS
- ☐ Trojan

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

☐ malware

☐ bot

☐ worm

Question 29

7 / 7 pts

Arrange the following stages of a Kill Chain in an information systems attack.

Reconnaissance – Gathers information Stage 1:

[Select]



Stage 2:

Delivery - Sends the exploit and malicious payload to the target Stage 3:

Exploitation – Executes the exploit Stage 4:

Installation - Installs malware and backdoors Stage 5:

[Select]



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:

The difference between the two is that IPS blocks the attempted intrusion while IDS provides an alert of an upcoming incident. An example of this is when IDS alerts the administrator while the IPS in the firewall prevents the attack.

Quiz Score: 44 out of 57

1. These are raw facts with unknown coding schemes? **Noise**
2. These are accepted facts, principles, or rules of thumb that are useful for specific domains. This can be the result of inferences and implications produced from simple information facts:
Knowledge
3. It is an assurance that the sender is provided with proof of data delivery and the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.: **non-repudiation**
4. These are security measures to establish the validity of a transmission, message, or originator.:
Authentication
5. Enumerate the IA four security engineering domains: **physical security, personnel security, its security, operational security**
6. This refers to the protection of hardware, software, and data against physical threats to reduce or prevent disruptions to operations and services and loss of assets. **Physical Security**
7. What are three distinct levels protecting information that Information Assurance can be thought of? **Physical, perceptual, and information infrastructure**
8. What level of focus does information assurance covers information and data manipulation ability maintained in cyberspace, including data structures, processes, and programs, protocols, data content and databases? **information infrastructure**
9. According to studies, what is the biggest threat to computer security? **Malware**
10. What are the components of an information that makes it more significant compare from other type of data? Choose all that apply. **Perceptual, accurate, verifiable, comprehensive**
11. Which of the following statement best describe Hackers? **One who gains unauthorized access to or breaks into information systems for thrill, challenge, power or profit**
12. What category of security solution/policy is phrased in terms of entities that execute activities and request access to object? **Subjects**
13. Is a category of entities, or a circumstance, that poses a potential danger to an asset? **Threat**
14. What are the three categories of threat? Choose all that apply? **By impact, by intent, by kind of entity involve**
15. What term is used to describe a program written to take advantage of a known vulnerability?
Exploit
16. A Vulnerability in Cisco IOS that allows attackers to gain control of the routers, monitor network communication, and infect other network devices. **Synful knock**
17. It is the manipulation of an individual into performing actions or divulging confidential information: **social engineering**
18. A type of password cracking where the attacker tries several possible passwords in an attempt to guess the password. **brute-force attack**
19. An infiltration method where a malicious party sends a fraudulent email disguised as being from a legitimate, trusted source, tricking the recipient into installing malware on their device or sharing personal or financial information. **Phishing**
20. What algorithm calculates a string value from a file of a fixed size, that contains data, and transformed it into a short fixed key or value? **hashing**