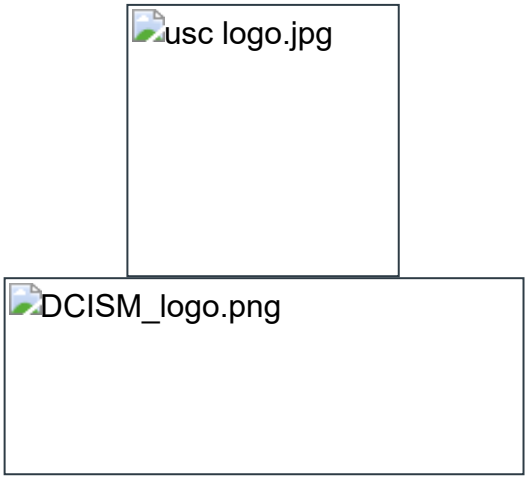
Midterm Exams: Test 1

Due No due date **Points** 148 **Questions** 92
Available Oct 17 at 3pm - Oct 17 at 4:30pm 1 hour and 30 minutes
Time Limit 90 Minutes

Instructions



University of San Carlos

Department of Computer and Information Sciences and Mathematics

Midterm Examination

ANY FORM OF COMPUTING DEVICE IS NOT ALLOWED DURING THE EXAMINATIONS!

OPENING OF BROWSER OR TABS OTHER THAN CANVAS IS STRICTLY PROHIBITED AND IS CONSIDERED CHEATING!!

A l w a y s f o l l o w i n s t r u c t i o n s !!!

This quiz was locked Oct 17 at 4:30pm.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	89 minutes	126.17 out of 148

Correct answers are hidden.

Score for this quiz: **126.17** out of 148
Submitted Oct 17 at 4:30pm
This attempt took 89 minutes.

Question 1

1 / 1 pts

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

- presentation
- authentication
- identification
- analysis
- preservation

Question 2

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

Incorrect

Question 3

0 / 1 pts

According to studies, What is the biggest threat to computer security?

Write your answer in lowercase only.

malware

Incorrect

Question 4

0 / 1 pts

Is a industry standards based implementation of carrying traffic for multiple VLANs on a single *trunking* interface between two Ethernet switches.

- VL
- Virtual Trunking Protocol (VTP)
- Dynamic Trunking Protocol (DTP)
- Vlan Trunking Protocol
- 802.1Q
- 802.1Q

Question 5

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 #

adaptive security appliance 5505

Question 6

1 / 1 pts

What category of security solution/policy is phrased in terms of operations, primitive or complex, that can operate on objects and must be controlled.

Write your answer in lowercase only.

actions

Question 7

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 8

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

Question 9

1 / 1 pts

A _____ is a category of entities, or a circumstance, that poses a potential danger to an asset.

Write your answer in lowercase only.

- threat

Incorrect

Question 10

0 / 1 pts

What would be the maximum number of bits that can be borrowed using the address 198.11.192.0/25?

7

Question 11

1 / 1 pts

This is a modular computer malware discovered in 2012 that attacks computers running the Microsoft Windows operating system.The program is being used for targeted cyber espionage in Middle Eastern countries.

- (●) sKyWIper
- ( ) Stuxnet
- ( ) Titan Rain
- ( ) Moonlight Maze

Question 12

1 / 1 pts

it is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution.

write your answer in lowercase only.

virtual local area network

Incorrect

Question 13

0 / 1 pts

What federal organization establishes federal policy directives on network security?

- [ ] NSA
- [x] CNSS
- [ ] NIST
- [ ] NBS

Question 14

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 15

1 / 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

route outside 0.0.0.0 0.0.0.0 10.10.10.2

Unanswered

Question 16

0 / 1 pts

A _____ is a type of defense against cyber attack when taking steps to prevent an attack or to mitigate the damage should an attack occur (access control, secure system design, security administration).

Question 17

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 18

1 / 1 pts

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

- dhcp address range 192.168.1.10-20 inside
- ip dhcp address 192.168.1.10-192.168.1.20 inside

- ip dhcp address range 192.168.1.10-20
- ip dhcp address 192.168.1.10-192.168.1.20 inside
- dhcp address 192.168.1.10-192.168.1.20 inside

Incorrect

Question 19

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.

workforce security

Question 20

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 21

1 / 1 pts

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

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

Question 22

1 / 1 pts

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

dhcp enable inside

Question 23

1 / 1 pts

_____ is a malicious computer worm, first identified in 2010, that targets industrial computer systems and was responsible for causing substantial damage to Iran's nuclear program. The software was designed to erase itself in 2012 thus limiting the scope of its effects. The worm is believed by many experts to be a jointly built American-Israeli cyber

weapon, although no organization or state has officially admitted responsibility.

stuxnet

Question 24

1 / 1 pts

Which of the following is not digital evidence?

Choose all that apply

- [ ] Wireless access points
- [x] digital calclulators
- [ ] Answering Machine
- [x] SIM Card
- [ ] Electronic game devices
- [ ] iPods
- [x] digital printout

Question 25

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 26

1 / 1 pts

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.

Write your answer in lowercase only.

physical security

Question 27

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 256
- ( ) MD5
- ( ) SHA 128
- ( ) Cryptographic Hash Function

Question 28

1 / 1 pts

_____ is a computer system for gathering and analyzing real time data, the systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation.

supervisory control and data acquisition

Question 29

1 / 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/acquisistion
- indentification
- analysis

Question 30

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 31

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 32

1 / 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,

nameif

Question 33

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.

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

Question 34

1 / 1 pts

Which of the following statement best describe Hackers?

- one who gains unauthorized access to or breaks into information systems for thrills, challenge, power, or profit.
- seek the military, diplomatic, and economic secrets of foreign governments, foreign corporations, and adversaries. May also target domestic adversaries.
- target information that may be of value to them: bank accounts, credit card information, intellectual property, etc.
- usually politically motivated and may seek to cause maximal damage to information infrastructure as well as endanger lives and property.

Question 35

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,

default gateway

Incorrect

Question 36

0 / 1 pts

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

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

Question 37

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.

- hashing
- write protect
- write blockers
- imaging

Question 38

1 / 1 pts

Write the command to set only one *secure* MAC addresses for the interface.

write your answer in lowercase.

- (●) switchporr port-security max 1

Question 39

1 / 1 pts

These are "individuals or organizations that have economic, political or social power and are able to influence at a national who employ violence in pursuit of their objectives.

- [ ] Verifiable Armed Sectors
- [ ] Vicious Non State Actors
- [x] Violent Non State Actors
- [ ] Arrmed Violent Sector

Question 40

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.

- firewall
- tacacs+
- aaa authenticaion
- radius

Question 41

1 / 1 pts

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

- aaa new model
- aaa new-model
- new-model aaa
- new model aaa

Question 42

1 / 1 pts

What are the four key attack attributes according to experts when determining whether a cyber attack is an act of cyber war?

- Instrument-based
- Strict liability
- Proportionality

- [x] Consequence
- [ ] Distinction
- [x] Source
- [x] Sophistication
- [ ] Necessity
- [ ] Effects-based
- [x] Motivation

Question 43

1 / 1 pts

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

- ( ) systems assets
- (•) physical assets
- ( ) technical assets
- ( ) logical assets
- ( ) non technical assets

Partial

Question 44

0.67 / 1 pts

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

Answer should be in order.

Step 1	object network INSDE-N
Step 2	subnet 192.168.1.0 255.
Step	nat (inside,outside)dynai

Question 45

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 46

1 / 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?

- 0

- 50
- 100
- 1

Question 47

1 / 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.

authentication

Incorrect

Question 48

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.

physical safeguard

Question 49

1 / 1 pts

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

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

Question 50

1 / 1 pts

It is an assurance that the sender is provided with proof of a data delivery and recipient is provided with proof of the sender's identity, so that neither can later deny having processed the data.

- integrity
- confidentiality
- availability
- non-repudiation

Question 51

1 / 1 pts

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

Your Answer:

Identification

the first step in the digital forensic process that identifies prospective sources of data and evidence (devices), as well as important data custodians and their locations. This stage is where we identify the evidence, the type of information available and how we should retrieve such information

Examples:

- email from an attacker regarding sextortion
- Identifying that a USB contains the digital evidence

Acquisition/Imaging

the second phase and requires forensically-sound procedures and validated tools. This is the stage where we can obtain a forensic image of the contents of a storage media. This is acquired by trained digital forensic examiner using validated hardware and software. This stage ensures that the crime scene should be left untampered.

Examples:

- Obtaining a USB drive that has a virus from the crime scene
- Leaving the computing device on to prevent any volatile data from getting lost.

Analysis

This stage, we examine all digital evidence acquired and authenticated. The process is determined by the examiner - certain software and hardware will be used to decrypt and encrypt files. The results of such analysis are system-generated files from certain software such as AccessData FTK Imager.

Examples:

- Using AccessData FTK Imager to process a disk.
- Using AccessData FTK Imager to decrypt a locked file and compare images and original evidence.

Reporting

This stage is creating a report based on tried and true methods from the examiner and assure that other examiners will be able to replicate the same findings using the evidence provided.

Examples:

- FTK txt file created from Imaging

- Software-generated report file

Court Presentation

Presenting evidence and a report to the court of law assuming that you have obtained evidence legally.

Examples:

- FTK text file created from Imaging
- Creating a written process report that appeals to the court of law

Question 52

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

Incorrect

Question 53

0 / 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
- system-high

- compartmented
- multi-level

Question 54

1 / 1 pts

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

Answer should be in order.

Step 1	policy-map global_policy
Step 2	class inspection_default
Step 3	inspect HTTP

Question 55

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

Incorrect

Question 56

0 / 1 pts

A malware which is a variety of software components that together provide services to the attackers. Currently this includes information stealing capabilities and in the background, kernel drivers and injection tools. Part of this malware is written in unknown high-level programming language.

- (●) sKyWIper
- ( ) Stuxnet
- ( ) flamer
- ( ) duqu

Question 57

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.

- ( ) Proxy Firewall
- ( ) Network address translation
- ( ) Stateful Multi-layer Inspection
- (●) Next-generation firewalls

Question 58

1 / 1 pts

Why should your evidence media write-protected?

answer in one sentence only.

Your Answer:

Evidence assurance is necessary to ensure that the original media is unchanged once it is acquired and must remain unchanged for validity of the entire investigation. No tampering shall occur on it.

Question 59

1 / 1 pts

What type of state that joins the political entity of a state to the cultural entity of a nation, from which it aims to derive its political legitimacy to rule and potentially its status as a sovereign state?

- None of the above
- Political State
- Nation State
- Academic State

Question 60

1 / 1 pts

These are security measures to establish the validity of a transmission, message, or originator.

- No answer text provided.

- No answer text provided.
- No answer text provided.
- (selected) authentication

Question 61

1 / 1 pts

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.

Write your answer in lowercase only.

information infrastructure

Question 62

1 / 1 pts

These are entities that participate or act in international relations.

- Neutral State Actions
- Natural Status Alienation
- (selected) Non-state actors
- Non-state Attributes

Question 63

1 / 1 pts

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

answer in lowercase only

vulnerability

Question 64

1 / 1 pts

What category of security solution/policy is phrased in terms of entities (users, processes, etc.) that execute activities and request access to objects.

Write your answer in lowercase only.

subjects

Question 65

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 understand 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 66

1 / 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.

- forensic duplication
- backup image
- mirroring
- partitioning

Question 67

1 / 1 pts

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.

- wisdom
- information
- raw facts or data
- knowledge

Question 68

1 / 1 pts

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

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

Question 69

1 / 1 pts

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

Answer should be in order.

Step 1	policy-map global_policy
Step 2	class inspection_default
Step 3	inspect icmp

Question 70

1 / 1 pts

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

Your Answer:

Due to its volatility, it is very difficult to handle digital evidence compared to traditional evidence. This volatility can lead to tampered evidence which then renders it unusable and invalid.

Question 71

1 / 1 pts

What type of state that joins the political entity of a state to the cultural entity of a nation, from which it aims to derive its political legitimacy to rule and potentially its status as a sovereign state?

- Academic State
- Nation State
- Political State
- None of the above

Question 72

1 / 1 pts

These are "individuals or organizations that have economic, political or social power and are able to influence at a national who employ violence in pursuit of their objectives.

- Violent Non State Actors

- Verifiable Armed Sectors
- Vicious Non State Actors
- Arrmed Violent Sector

Question 73

1 / 1 pts

_____ is a malicious computer worm, first identified in 2010, that targets industrial computer systems and was responsible for causing substantial damage to Iran's nuclear program. The software was designed to erase itself in 2012 thus limiting the scope of its effects. The worm is believed by many experts to be a jointly built American-Israeli cyber weapon, although no organization or state has officially admitted responsibility.

stuxnet

Incorrect

Question 74

0 / 1 pts

A _____ is a type of defense against cyber attack when taking steps to prevent an attack or to mitigate the damage should an attack occur (access control, secure system design, security administration).

virtual private network

Question 75

1 / 1 pts

It is an assurance that the sender is provided with proof of a data delivery and recipient is provided with proof of the sender's identity, so that neither can later deny having processed the data.

- (●) non-repudiation
- ( ) confidentiality
- ( ) integrity
- ( ) availability

Question 76

1 / 1 pts

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.

Write your answer in lowercase only.

information infrastructure

Question 77

1 / 1 pts

Which of the following statement best describe Hackers?

- [x] one who gains unauthorized access to or breaks into information systems for thrills, challenge, power, or profit.

target information that may be of value to them: bank accounts, credit card information, intellectual property, etc.

seek the military, diplomatic, and economic secrets of foreign governments, foreign corporations, and adversaries. May also target domestic adversaries.

usually politically motivated and may seek to cause maximal damage to information infrastructure as well as endanger lives and property.

Incorrect

Question 78

0 / 1 pts

What federal organization establishes federal policy directives on network security?

- NSA
- [x] CNSS
- NIST
- NBS

Question 79

1 / 1 pts

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

- [x] Business is inherently profit-driven.

- [x] Costs come in various forms.
- [ ] Potential for loss
- [ ] Business reputation
- [ ] Legislative and regulatory mandates

Question 80

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 81

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 82

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 83

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

Incorrect

Question 84

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.

technical safeguard

Question 85

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 86

1 / 1 pts

Is a industry standards based implementation of carrying traffic for multiple VLANs on a single *trunking* interface between two Ethernet switches.

- 802.1Q
- VL
- 802.1Q
- Virtual Trunking Protocol (VTP)
- Dynamic Trunking Protocol (DTP)
- Vlan Trunking Protocol

Question 87

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 understand 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 88

1 / 1 pts

Which of the following is not digital evidence?

Choose all that apply

- [x] digital printout
- [x] digital calclulators
- [x] SIM Card
- [ ] Answering Machine
- [ ] iPods
- [ ] Wireless access points
- [ ] Electronic game devices

Question 89

1 / 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.

- (●) collection/acquisistion
- ( ) indentification
- ( ) analysis
- ( ) presentation

Question 90

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 256
- ( ) MD5
- ( ) SHA 128
- ( ) Cryptographic Hash Function

Question 91

1 / 1 pts

Why should your evidence media write-protected?

answer in one sentence only.

Your Answer:

Evidence should be write-protected to avoid any tampering or manipulation. This then provides legitimacy to your evidence which then can be used in the court of law.

Question 92

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 93

1 / 1 pts

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

Your Answer:

1. Identification

Identifies sources of evidences and properly labels them and what type of information is available and how to retrieve such

Examples:

- email from attacker about sextortion
- identifying laptop that can be evidence if analyzed

2. Imaging

Makes a copy of the digital evidence to prevent tampering and to further legitimize the evidence using forensically-sound procedures and valid

tools. Obtaining the evidence

Examples:

- imaging the USB from the crime scene
- leaving computing devices on to prevent data loss

3. Analysis

examines all digital evidences to prove whether or not one is to be acquitted or convicted.

Examples:

- using FTK Imager to process a disk
- using Imager to compare the validity of the image and original media file.

4. Report

This is the result from the analysis. A system-generated file is created as a report for proof.

Examples:

- FTK Imager text file of the analysis report
- a generated report file from certain software

5. Presentation

Present the report that is acceptable by the court of law

- FTK Imager text file of the analysis report
- written report of the entire case with evidence

Question 94

1 / 1 pts

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

Your Answer:

digital evidence is harder than handling traditional evidence because digital evidence is quite volatile which means its difficult to maintain its integrity. This is also why we should image digital evidence for assurance.

Question 95

1 / 1 pts

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

- (●) security level 0
- ( ) security level 100
- ( ) security level 1
- ( ) security level 99

Question 96

1 / 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?

- (●) 50
- ( ) 0
- ( ) 100
- ( ) 1

Question 97

1 / 1 pts

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

- (●) dhcp address 192.168.1.10-192.168.1.20 inside
- ( ) ip dhcp address range 192.168.1.10-20
- ( ) dhcp address range 192.168.1.10-20 inside
- ( ) 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 98

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,

default gateway

Question 99

1 / 1 pts

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

Answer should be in order.

Step 1	object network INSDE-N
Step 2	subnet 192.168.1.0 255.
Step	nat (inside,outside)dynai

Question 100

1 / 1 pts

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

Answer should be in order.

Step 1	policy-map global_policy
Step 2	class inspection_default
Step 3	inspect HTTP

Question 101

1 / 1 pts

Which of the following describe a "State"? Choose 2.

the particular condition that someone or something is in at a specific time.

the condition of a person or thing, as with respect to circumstances or attributes

a nation or territory considered as an organized political community under one government.

is specifically a political and geopolitical entity, whilst a nation is a cultural and ethnic one.

Question 102

1 / 1 pts

Identify the network and broadcast of the given address:
150.188.200.209/22

Network Address: 150.188.200.0

Broadcast Address: 150.188.203.255

Answer 1:

150.188.200.0

Answer 2:

150.188.203.255

Incorrect

Question 103

0 / 1 pts

What are two types of defenses against cyber attacks?[

virtual private netwo

firewall

Answer 1:

virtual private network

Answer 2:

firewall

Question 104

1 / 1 pts

What are three different analytic frameworks have been proposed, various international conventions allow a self-defense or “anticipatory self-defense” response to an armed attack. and qualify a cyber attack “equivalent” to an armed attack.

instrument-based _____

effects-based _____

strict liability _____

Answer 1:

Instrument-based

Answer 2:

Effects-based

Answer 3:

Strict liability

Partial

Question 105

0.5 / 1 pts

What are the 3 port security violation mode on a port?

- [ ] restart
- [x] shutdown
- [ ] access
- [x] restrict
- [ ] disallow
- [x] protect

Question 106

2 / 2 pts

Enumerate the IA four security engineering domains. **write your answer in lowercase only.**

physical security _____

personnel security _____

IT security _____

operational security _____

Answer 1:

physical security

Answer 2:

personnel security

Answer 3:

it security

Answer 4:

operational security

Question 107

2 / 2 pts

What are three distinct levels protecting information that Information Assurance can be thought of?

- [ ] data
- [x] information infrastructure
- [ ] network
- [x] perceptual
- [ ] technology
- [ ] activities
- [x] physical

Question 108

1 / 1 pts

What are the three categories of threat? choose all that apply.

- [ ] by authenticity
- [x] by kind of entity involve
- [ ] by integrity
- [x] by impact
- [x] by intent
- [ ] by threat actor

Question 109

1 / 1 pts

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

- [ ] UNIVAC
- [x] ENIAC
- [x] Bombe
- [ ] Analytical Engine
- [ ] EDSAC

Incorrect

Question 110

0 / 1 pts

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

- [x] Assisting the organization in meeting regulatory requirements
- [ ] Competitive advantage
- [x] Legislative and regulatory mandates
- [x] Providing for recovery in case of disaster
- [ ] Potential for loss
- [x] Enabling safe operation of business services

Incorrect

Question 111

0 / 1 pts

What are the Functional Components of Information assurance?

Choose all that apply.

- [x] response
- [ ] cyber space protection
- [x] protection
- [ ] impacts and losses to their opponents
- [x] capability restoration
- [ ] infrastructure systems

detection

Incorrect

Question 112

0 / 3 pts

Given Class A address, creating 900 subnets,

255.255.252.0 What is the new subnet mask?

1-254 What is the Range or interval per network?

1022 How many number of host created?

Answer 1:

255.255.252.0

Answer 2:

1-254

Answer 3:

1022

Question 113

1 / 1 pts

How many useable host can be created if the subnet mask is 255.255.255.248?

6

Incorrect

Question 114

0 / 2 pts

In a Class A network,

8 . what is maximum bits to be borrowed?

16777214 . And how many useable host it can be created per subnet basing on the borrowed bits?

Answer 1:

8

Answer 2:

16777214

Partial

Question 115

1 / 4 pts

Using 198.13.128.0/22 determine the following:

255.255.252.0 what is correct subnet mask of /22?

17 how many bits to borrow if the requirement is 15?

255.255.128.0 What is the new subnet mask after borrowing the bits?

32766 how many useable host can be created per subnet?

Answer 1:

255.255.252.0

Answer 2:

17

Answer 3:

255.255.128.0

Answer 4:

32766

Partial

Question 116

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 identification :

Step 2 acquisition :

Step 3 analysis :

Step 4 report :

Step 5 presentation :

Answer 1:

identification

Answer 2:

acquisition

Answer 3:

analysis

Answer 4:

report

Answer 5:

presentation

Partial

Question 117

1 / 2 pts

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

type of data found in sto

This data will be lost if th

Persistent data type of data found in sto

Volatile Data This data will be lost if th

Question 118

3 / 3 pts

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

Disk to disk imaging is used when th

Disk to file cloning of the original st

Files to File imaging is same thing as

Question 119

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

Answer 3:

accounting

Partial

Question 120

2 / 4 pts

If a Class B network is subnetted with the subnet mask of 255.255.248.0,

0.1-7.254 What would be the interval of between subnets?

11 How many bits was borrowed from the host?

32 How many subnets?

2046 How many useable host was created?

Answer 1:

0.1-7.254

Answer 2:

11

Answer 3:

32

Answer 4:

2046

Question 121

2 / 2 pts

Identify the network and broadcast of the given address: 200.15.18.200/27

Network Address: 200.15.18.192

Broadcast Address: 200.15.18.223

Answer 1:

200.15.18.192

Answer 2:

200.15.18.223

Partial

Question 122

16 / 36 pts

Identify the following blank spaces in the given table

Address	# of required Host	Borrowed bits	# of subnetworks	Prefix
198.15.224.0/21	60	6	32	26
15.192.0.0/23	90	7	2	25
201.11.120.128/26	12	4	16	28
160.224.0.0/19	600	10	64	22

Answer 1:

6

Answer 2:

32

Answer 3:

26

Answer 4:

255.255.255.192

Answer 5:

198.15.224.1 - 192.15.224.62

Answer 6:

198.15.224.0

Answer 7:

198.15.224.192

Answer 8:

62

Answer 9:

2

Answer 10:

7

Answer 11:

2

Answer 12:

25

Answer 13:

255.255.255.128

Answer 14:

15.192.0.1-15.192.0.126

Answer 15:

15.192.0.0

Answer 16:

15.192.0.128

Answer 17:

126

Answer 18:

36

Answer 19:

4

Answer 20:

16

Answer 21:

28

Answer 22:

255.255.255.240

Answer 23:

201.11.120.129-201.11.120.142

Answer 24:

201.11.120.0

Answer 25:

201.11.120.240

Answer 26:

14

Answer 27:

2

Answer 28:

10

Answer 29:

64

Answer 30:

22

Answer 31:

255.255.252.0

Answer 32:

160.224.0.1-160.224.3.254

Answer 33:

160.224.0.0

Answer 34:

160.224.252.0

Answer 35:

1022

Answer 36:

422

Quiz Score: **126.17** out of 148