IBM-Cybersecurity-Analyst-Professional-Certificate-Assessment-Exam

Question 1

Select the answer the fills in the blanks in the correct order. A weakness in a system is a/an ____. The potential danger associated with this is a/an ____ that becomes a/an ____ when attacked by a bad actor. 1 point

risk, exploit, threat

vulnerability, threat, exploit

threat, exposure, risk

threat actor, vulnerability, exposure

Question 2

Putting locks on a door is an example of which type of control? 1 point

Preventative

Detective

Deterrent

Corrective

Question 3

The potential for an employee to accidently disclose confidential information is considered what? 1 point

A threat

A vulnerability

A risk

An exposure

Question 4

Implement a filter to remove flooded packets before they reach the host is a countermeasure to which form of attack? 1 point

A Trojan Horse attack

A Phishing attack

A Denial of Service (DoS) attack

An IP Spoofing attack

Question 5

Trudy intercepts a plain text message sent by Alice to Bob but in no way interferes with its delivery. Which aspect of the CIA Triad was violated? 1 point

Confidentiality

Integrity

Availability

All of the above.

Question 6

A company wants to prevent employees from wasting time on social media sites. To accomplish this, a document forbidding use of these sites while at work is written and circulated and then the firewalls are updated to block access to Facebook, Twitter and other popular sites. Which two (2) types of security controls has the company just implemented? (Select 2) 1 point

Physical

Operational

Administrative

Technical

Question 7

A penetration tester that gains access to a system without permission and then exploits it for personal gain is said to wear what color hat? 1 point

White

Gray

Black

Green

Question 8

Trying to break an encryption key by trying every possible combination of characters is called what? 1 point

A social engineering attack

A known cyphertext attack

A rainbow table attack

A brute force attack

Question 9

Which three (3) of the following are key ITIL processes? (Select 3) 1 point

Change Management

Time Management

Process Management

Problem Management

Project Management

Incident Management

Question 10

Which three (3) roles are typically found in an Information Security organization? (Select 3) 1 point

Security Guard

Vulnerability Assessor

Finance

Penetration Tester

Chief Information Security Officer (CISO)

Question 11

Which three (3) are considered best practices, baselines or frameworks? (Select 3) 1 point

ISO27000 series

HIPAA

ITIL

GDPR

COBIT

Question 12

Alice sends a message to Bob that is intercepted by Trudy. Which scenario describes a integrity violation? 1 point

Trudy deletes the message without forwarding it.

Trudy changes the message and then forwards it on.

Trudy reads the message.

Trudy cannot read it because it is encrypted but allows it to be delivered to Bob in its original form.

Question 13

In cybersecurity, Accountability is defined as what? 1 point

Being able to map an action to an identity.

Being able to apply financial management to a process.

The property of being genuine and verifiable.

The first or original copy of a document or message.

Question 14

Your bank just implemented 2-factor authentication. Before you can access your account. Which two (2) pairs of factors would satisfy the "2-factor" criteria? (Select 2) 1 point

Voice recognition and face scan.

Your fingerprint scan and face scan.

Your password and PIN number.

Your password and fingerprint scan.

Your bank's ATM card and a PIN number.

Question 15

Which three (3) of the following are Physical Access Controls? (Select 3) 1 point

Firewalls

Door locks

HoneyPots

Security guards

Fences

Question 16

Windows 10 stores 64-bit applications in which directory? 1 point

\Program Files

\System32

\System

\Program Files (x86)

Question 17

Which three (3) permissions can be set on a file in Linux? (Select 3) 1 point

execute

modify

view

write

run

read

Question 18

Which form of Cloud computing combines both public and private clouds? 1 point

Mixed cloud

Hybrid cloud

Universal cloud

Open cloud

Binary cloud

Question 19

Which security concerns follow your workload even after it is successfully moved to the cloud? 1 point

Data security

Disaster Recovery/Business Continuity Planning

Identity and Access Management

Compliance

All of the above.

Question 20

Which of these is a privacy regulation that went into effect in 2018 covering all residents of the European Union and all companies worldwide who do business with residents of the EU? 1 point

HIPAA

ISO27000 series

PCI-DSS

GDPR

NIST 800-53A

Question 21

Which two (2) of the following attack types target endpoints? 1 point

Denial of Service (DoS)

Ad Network

Spear Phishing

SQL Injection

Question 22

What is the most common patch remediation frequency for most organizations? 1 point

As soon as they are released.

Weekly

Monthly

Annually

Question 23

In Windows kernel mode, what stops a misbehaving driver from impacting other processes? 1 point

Each process runs in its own dedicated virtual address space.

The Windows Virtual Address Manager.

Nothing.

The Windows Process Director.

Question 24

In Linux, Bash, tcsh and sh are what? 1 point

Shells

Directories

Distros

Commands

Question 25

Public key encryption ensures which of the following? 1 point

Confidentiality and Availability.

Confidentiality and Integrity.

Confidentiality only.

Confidentiality, Integrity and Availability.

Question 26

Which of the following practices helps assure the best results when implementing encryption? 1 point

Choose a reliable and proven published algorithm.

Develop a unique cryptographic algorithm for your organization and keep them secret.

Change the cryptographic algorithm used monthly.

Hard-code encryption keys into your applications to assure consistent use.

Question 27

Which of the following statements about hashing is True? 1 point

If you have two hashes that differ only by a single character, you can infer that the original messages also differed very little.

Hashing uses algorithms that are known as “one-way” functions.

The original message can be retrieved from the hash if you have the encryption key.

A weakness of hashing is that the hash is proportional in length to the original message.

Question 28

Which of the following practices will help assure the confidentiality of data in transit? 1 point

Accept self-signed certificates.

Always compress files before sending if you are using TLS.

Implement HTTP Strict Transport Protocol (HSTS).

Disable certificate pinning.

Question 29

For added security you decide to protect your network by conducting both a stateless and stateful inspection of incoming packets. How can this be done? 1 point

You must install the stateful and stateless firewalls in parallel with an intelligent switch in front of them to direct the packets to one or the other as appropriate.

Install a single firewall that is capable of conducting both stateless and stateful inspections.

You must install 2 firewalls in series, so all packets pass through the stateless firewall first and then the stateless firewall.

Install a stateful firewall only. These advanced devices inspect everything a stateless firewall inspects in addition to state related factors.

Question 30

Which statement best describes configuring a NAT router to use overload mapping? 1 point

The organization will need as many registered IP addresses as it has computers that need Internet access.

The NAT router uses each computer's IP address for both internal and external communication.

Many unregistered IP addresses are mapped to a single registered IP address using different port numbers.

Unregistered IP addresses are mapped to registered IP addresses as they are needed.

Question 31

If a computer needs to send a message to a system that is not part of the local network, where does it send the message? 1 point

The network's DNS server address.

The computer's domain name.

The computer's IP address.

The computer's MAC address.

The network's default gateway address.

The network's DHCP server address.

Question 32

In IPv4, how many of the 4 octets are used to define the network portion of the address in a Class B network? 1 point

1

2

3

4

Question 33

Which three (3) of these statements comparing UDP and TCP are True? (Select 3) 1 point

TCP is connectionless.

UDP is connectionless.

TCP is more reliable than UDP.

TCP is faster than UDP.

UDP is more reliable than TCP.

UDP is faster than TCP.

Question 34

What is one difference between a Stateful Firewall and a Next Generation Firewall? 1 point

A NGFW understand which application sent a given packet.

A Stateful Firewall understands which application sent a given packet.

There is no real difference. These are two names for the same device.

A NGFW does not understand session information.

Question 35

You are concerned that your organization is really not very experienced with securing data sources. Which hosting model would require you to secure the fewest data sources? 1 point

PaaS

On premise

SaaS

IaaS

Question 36

A Vulnerability Assessment should be conducted during which phase of the Discover - Harden - Monitor & Protect - Repeat cycle? 1 point

Identification & Baseline.

Raise the Bar.

Real-Time Monitor & Protection.

Repeat.

Question 37

Which three (3) of the following are considered safe coding practices? (Select 3) 1 point

Avoid using OS commands whenever possible.

Use library functions in place of OS commands.

Avoid running commands through a shell interpreter.

Use blacklists but avoid whitelists when processing input data.

Question 38

An employee calls the IT Helpdesk and admits that maybe, just possibly, the links in the email he clicked on this morning were not from the real Lottery Commission. What is the first thing you should tell the employee to do? 1 point

Run a Port scan.

Start searching his hard drive for unusual files or folders.

Run an antivirus scan.

Run a vulnerability scan.

Question 39

If a penetration test calls for you to create a diagram of the target network including the identity of hosts and servers as well as a list of open ports and published services, which tool would be the best fit for this task? 1 point

John the Ripper

Wireshark

Nmap

Metasploit

Question 40

Spare workstations and servers, blank removable media, packet sniffers and protocol analyzers, all belong to which Incident Response resource category? 1 point

Incident Analysis Resources.

Incident Analysis Hardware and Software.

Incident Post-Analysis Resources.

Incident Handler Communications and Facilities.

Question 41

NIST recommends considering a number of items, including a high level of testing and monitoring, during which stage of a comprehensive Containment, Eradication & Recovery strategy? 1 point

Containment

Eradication

Recovery

None of these.

Question 42

True or False. Digital forensics is effective in solving cyber crimes but is not considered effective in solving violent crimes such as rape and murder. 1 point

True

False

Question 43

Which of these devices collects the most information on network activity? 1 point

Intrusion detection systems.

Firewalls.

System Event Management systems.

Packet sniffers.

Question 44

What scripting concept is widely used across different languages that checks if a condition is true, and if so, takes action, and if false, a different action? 1 point

Variables

if-then

Loops

Arguments

Question 45

Which three (3) statements about variables are true? (Select 3) 1 point

Variables must be declared at the top of the program.

Variables do not have to be declared in advance of their use.

Variable names are not case sensitive, i.e. the variable "TotalSales" and "totalsales" would refer to the same block of memory.

Variables can change type after they have been set.

A variable name must start with a letter or the underscore "_" character.

Question 46

What is the largest number that will be printed during the execution of this Python while loop?

1 point

1

10

9

0

Question 47

Which two (2) of these Python libraries provides useful statistical functions? (Select 2) 1 point

Seaborn

StatsModels

Pandas

NumPy

Matplotlib

Scikit-learn

Question 48

According to the Crowdstrike model, CISOs, CTOs and executive boards belong in which intelligence area? 1 point

Strategic

Control

Tactical

Operational

Question 49

According to the FireEye Mandiant's Security Effectiveness Report 2020, what fraction of security tools are deployed with default settings and thus underperform expectations? 1 point

50%

80%

25%

10%

Question 50

Which is the data protection process that prevents a suspicious data request from being completed? 1 point

Blocking, masking and quarantining

Data discovery

Data classification

Data risk analysis

Question 51

There are many good reasons for maintaining comprehensive backups of critical data. Which aspect of the CIA Triad is most impacted by an organization's backup practices? 1 point

Confidentiality

Authorization

Availability

Integrity

Question 52

C-level executives face 4 challenges when assuring their organizations maintain a comprehensive, workable data security solution. An organization creating a new Chief Information Security Officer (CISO) is an attempt to address which of one these? 1 point

New privacy regulations.

A cybersecurity skills shortage.

Operational complexity.

Explosive data growth.

Question 53

Which type of scan completes a TCP connection and is both slower and easier to detect than a SYN scan? 1 point

Stealth scan

Ping (ICMP Echo Request)

TCP Connect

UDP port scan

TCP/Half Open Scan (aka a SYN scan)

Question 54

Port numbers 1024 through 49151 are known as what? 1 point

Well known ports

Dynamic and Private Ports

Registered Ports

Virtual Ports

Question 55

The Decommission step in the DevSecOps Release, Deploy & Decommission phase contains which of these activities? 1 point

Creation of Immutable images.

Versioning of infrastructure.

Centralized Key-Value & Secret stores.

IAM controls to regulate authorization.

Question 56

Which type of application attack would include network eavesdropping, dictionary attacks and cookie replays? 1 point

Authorization

Exception management

Configuration management

Authentication

Question 57

Which of these is an aspect of a Solution Architecture? 1 point

Considers the needs of the entire organization.

Maps the main components of a problem space and solution at a very high level.

Gives the technology perspectives in detail.

Does not describe the internals of the main components or how they will be implemented.

Question 58

Which type of Building Blocks are Data Security and Application Security? 1 point

Solution Building Block (SBB)

Component Building Block (CBB)

General Building Block

Architecture Building Block (ABB)

Question 59

Which of these describes the process of data normalization in a SIEM? 1 point

Allows for predictable and consistent storage for all records.

Removes duplicate records from incoming data.

Compresses incoming.

Encrypts incoming data.

Question 60

The partnership between security analysts and technology can be said to be grouped into 3 domains, human expertise, security analytics and artificial intelligence. The human expertise domain would contain which three (3) of these topics? 1 point

Machine learning

Natural language

Abstraction

Anomaly detection

Pattern identification

Bias elimination

Question 61

True or False. If you have no better place to start hunting threats, start with a view of the global threat landscape and then drill down to a regional view, industry view and finally a view of the threats specific to your own organization. 1 point

True

False

Question 62

The cyber hunting team and the SOC analysts are informally referred to as the ____ and ____ teams, respectively. 1 point

Attack, Defense

Visitors, Home

Red, Blue

Blue. Red

Question 63

Which incident response team model assures consistency in the incident response policies and implementation across all IR teams in a global enterprise? 1 point

Coordinating incident response team.

Distributed incident response team.

Central incident response team.

Hybrid incident response team.

Question 64

According to the IRIS Framework, during which stage of an attack would the attacker attempt to escalate their privileges, move laterally and conduct internal reconnaissance? 1 point

Continuous phases occur.

Continue the attack, expand network access.

Attack beginnings.

Launch and execute the attack.

Attack objective execution.

Question 65

You are the CEO of a large tech company and have just received an angry email that looks like it came from one of your biggest customers. The email says your company is overbilling the customer and asks that you examine the attached invoice. You do but find it blank, so you reply politely to the sender asking for more details. You never hear back, but a week later your security team tells you that your credentials have been used to access and exfiltrate large amounts of company financial data. What kind of attack did you fall victim to? 1 point

As a phishing attack.

A shark attack.

As a whale attack.

As a spear phishing attack.

Question 66

Which three (3) of these control processes are included in the PCI-DSS standard? (Select 3) 1 point

Implement strong access control measures.

Require a photo ID for all credit card transactions.

Maintain an information security policy.

Regularly monitor and test networks.

Question 67

Stolen credit card numbers are sold to brokers who resell them to carders who use them to buy prepaid credit cards that are then used to buy gift cards that will be used to buy merchandise that is shipped to a reshipper who sends it on to its final destination before it is sold for profit. Why is such a complex process used instead of simply using the stolen numbers to buy the products that are desired? 1 point

If done quickly, there is a multiplying effect in play. The stolen credit card can be used to buy 3 or 4 prepaid cards each valued at the credit limit of the original card. The same is true for using each prepaid card to buy multiple gift cards and each gift card to buy more merchandise than its face value.

Because stolen cards can rarely be used directly to purchase merchandise.

To make the end-to-end transaction very difficult to follow.

It is easier to get approval to use a credit card to purchase a prepaid credit card than to it is to purchase merchandise.

Question 68

According to a 2018 Ponemon study third party risk management, which three (3) of these were identified as best practices? (Select 3) 1 point

Frequent review of third-party management policies and programs.

Requirement that all third-parties are bonded against data loss in the event of a breach.

Evaluation of the security and privacy practices of all third parties.

An inventory of all third parties with whom you share information.

Question 69

You get a phone call from a technician at the "Windows company" who tells you that they have detected a problem with your system and would like to help you resolve it. In order to help, they need you to go to a web site and download a simple utility that will allow them to fix the settings on your computer. Since you only own an Apple Mac, you are suspicious of this caller and hang up. What would the attack vector have been if you had downloaded the "simple utility" as asked? 1 point

Phishing

Software Vulnerabilities

Malicious Links

Remote Desktop Protocol (RDP)

Question 70

Very provocative articles that come up in news feeds or Google searches are sometimes called "click-bait". These articles often tempt you to link to other sites that can be infected with malware. What attack vector is used by these click-bait sites to get you to go to the really bad sites? 1 point

Malicious Links

Remote Desktop Protocol (RDP)

Phishing

Software Vulnerabilities

Answers

Of course, I can help you answer the questions. Here are the answers to the questions you provided:

Question 1

Answer: vulnerability, threat, exploit

Question 2

Answer: Preventative

Question 3

Answer: A vulnerability

Question 4

Answer: A Denial of Service (DoS) attack

Question 5

Answer: Confidentiality

Question 6

Answer: Administrative, Technical

Question 7

Answer: Black

Question 8

Answer: A brute force attack

Question 9

Answer: Change Management, Problem Management, Incident Management

Question 10

Answer: Vulnerability Assessor, Penetration Tester, Chief Information Security Officer (CISO)

Question 11

Answer: ISO27000 series, ITIL, GDPR

Question 12

Answer: Trudy changes the message and then forwards it on.

Question 13

Answer: Being able to map an action to an identity.

Question 14

Answer: Your fingerprint scan and face scan, Your bank's ATM card and a PIN number

Question 15

Answer: Door locks, Security guards, Fences

Question 16

Answer: \Program Files

Question 17

Answer: execute, modify, read

Question 18

Answer: Hybrid cloud

Question 19

Answer: All of the above.

Question 20

Answer: GDPR

Question 21

Answer: Ad Network, Spear Phishing

Question 22

Answer: Monthly

Question 23

Answer: Each process runs in its own dedicated virtual address space.

Question 24

Answer: Shells

Question 25

Answer: Confidentiality and Integrity.

Question 26

Answer: Choose a reliable and proven published algorithm.

Question 27

Answer: Hashing uses algorithms that are known as “one-way” functions.

Question 28

Answer: Implement HTTP Strict Transport Protocol (HSTS).

Question 29

Answer: Nmap

Question 30

Answer: Many unregistered IP addresses are mapped to a single registered IP address using different port numbers.

Question 31

Answer: The network's default gateway address.

Question 32

Answer: 2

Question 33

Answer: TCP is connectionless, UDP is connectionless, TCP is more reliable than UDP.

Question 34

Answer: A NGFW understand which application sent a given packet.

Question 35

Answer: SaaS

Question 36

Answer: Identification & Baseline.

Question 37

Answer: Avoid using OS commands whenever possible, Use library functions in place of OS commands, Avoid running commands through a shell interpreter.

Question 38

Answer: Run an antivirus scan.

Question 39

Answer: Nmap

Question 40

Answer: Incident Analysis Hardware and Software.

Question 41

Answer: Eradication

Question 42

Answer: False

Question 43

Answer: Packet sniffers.

Question 44

Answer: if-then

Question 45

Answer: Variables do not have to be declared in advance of their use, Variables can change type after they have been set, A variable name must start with a letter or the underscore "_" character.

Question 46

Answer: 10

Question 47

Answer: Pandas, NumPy

Question 48

Answer: Strategic

Question 49

Answer: 80%

Question 50

Answer: Blocking, masking and quarantining

Question 51

Answer: Availability

Question 52

Answer: A cybersecurity skills shortage.

Question 53

Answer: TCP/Half Open Scan (aka a SYN scan)

Question 54

Answer: Registered Ports

Question 55

Answer: Authorization, IAM controls to regulate authorization.

Question 56

Answer: Authentication

Question 57

Answer: Does not describe the internals of the main components or how they will be implemented.

Question 58

Answer: Solution Building Block (SBB)

Question 59

Answer: Allows for predictable and consistent storage for all records.

Question 60

Answer: Natural language, Abstraction, Pattern identification

Question 61

Answer: True

Question 62

Answer: Blue, Red

Question 63

Answer: Central incident response team.

Question 64

Answer: Continue the attack, expand network access.

Question 65

Answer: Spear Phishing

Question 66

Answer: Implement strong access control measures, Maintain an information security policy, Regularly monitor and test networks.

Question 67

Answer: To make the end-to-end transaction very difficult to follow.

Question 68

Answer: Frequent review of third-party management policies and programs, Evaluation of the security and privacy practices of all third parties, An inventory of all third parties with whom you share information.

Question 69

Answer: Phishing

Question 70

Answer: Malicious Links

Please note that these answers are based on the information provided in your questions. If you have any further inquiries or need more explanation, feel free to ask!