# Tests & Quizzes

## Quiz 1

Return to Assessment List

### Part 1 of 1 - / 5.0 Points

Question 1 of 20 0.25 Points

Explain the three tenets of cybersecurity (one sentence for each tenet).

It consists of CIA which are Confidentiality, Integrity and Availability. Confidentiality refers that only users who are authorized gain access to the content. Integrity refers to that only users who are authorizes gain access to changing the information stored. Availability refers to that the information stored are available while authorized users request them.

**Model Short Answer:**

**Confidentiality**: Only authorized users can view information.

**Integrity**: Only authorized users can change information to maintain valid, uncorrupted, and accurate information.

**Availability**: Information is accessible by authorized users whenever they request the information.

Question 2 of 20 0.25 Points

Explain in a few sentences the Colonial Pipeline attack (i.e., the type of attack and other details).

The Colonial Pipeline attack is an example of ransomware attack in 2021 which attacks Colonial Pipeline by Darkside. This group stole data from its IT Network System by intruding all devices, and the company paid with BitCoin to get the decryption key to regain control.

**Model Short Answer:**

Colonial pipeline was a **ransomware** attack launched by the Darkside group in May 2021. The attackers compromised the network of the Colonial Pipeline, locked the real-time data as well as stole around 100GB of raw data to demand a ransom. The Colonial Pipeline put the remaining systems offline for a few days to stop the operational systems as soon as possible. Colonial Pipeline confirmed that it paid US$4.4 million in cryptocurrency to DarkSide. However most of this money was recovered by the FBI.

Question 3 of 20 0.25 Points

Explain the concept of defense in depth and list 4 examples.

Defence in Depth refers to the defence techniques that can strengthen the system by setting up multiple layers in the devices and in cases of one layer failure, other layers can help defend against viruses or malware.

Examples: antivirus scanning, Network Monitoring and analyzing, multi-factor authentication, and VPN.

**Model Short Answer:**

Defense in depth provides multiple layers of security controls throughout the 7 domains of IT infrastructure. Some examples are firewalls, intrusion detection systems, access control, multifactor authentication, VPNs, encrypting files in storage, patching, anti-virus, segmentation,

Question 4 of 20 0.25 Points

Explain a man-in-the-middle attack in 1-2 sentences.

The man-in-the-middle attack is a type of attack that eavesdropping the information or communication sent between two parties or devices and in some cases changing the information or acquiring the information while also deceiving both parties or devices.

**Model Short Answer:**

The attacker is invisible between two communicating parties and can intercept all messages between them. The attacker can eavesdrop or alter communication.

Question 5 of 20 0.25 Points

List two access control authentication types and an example of each.

Access control authentication has five types:

Knowledge: account PIN

Ownership:  system token

Charasteristics: retina information

Location: users' physical location

Action: users actions such as keyboard typing.

**Model Short Answer:**

•**Knowledge (something you know):** A password, passphrase, or PIN.

•**Ownership (something you have):** A smart card, key, badge, or token.

•**Characteristics (something unique to you):** Fingerprints, retina, or signature. Any biometrics.

•**Location (somewhere you are):** Your physical location when you attempt to access a resource.

•**Action (something you do/how you do it):** The way you type on a keyboard.

Question 6 of 20 0.25 Points

Any action that could damage an asset is a:

- ✓ ○ A. Risk
- ✓ ○ B. Threat
- ✓ ○ C. Vulnerability
- ✓ ○ D. Exploit
- ✓ ○ E. All of the above

**Answer Key:** B

Question 7 of 20 0.25 Points

Weak passwords are an example of a:

- ✓ ○ A. Risk
- ✓ ○ B. Threat
- ✓ ○ C. Vulnerability
- ✓ ○ D. Exploit
- ✓ ○ E. Countermeasure

**Answer Key:** C

Question 8 of 20 0.25 Points

Which nmap command line option will enable OS detection, version detection, script scanning, and traceroute?

- ✓ ○ A. -A
- ✓ ○ B. -v
- ✓ ○ C. -O
- ✓ ○ D. -F
- ✓ ○ E. A and C

**Answer Key:** A

Question 9 of 20 0.25 Points

Where are Windows passwords stored?

- ✓ ○ A. SYSTEM
- ✓ ○ B. C:\windows\system\config
- ✓ ○ C. SAM
- ✓ ○ D. B and C
- ✓ ○ E. None of the above

**Answer Key:** C

Question 10 of 20 0.25 Points

Which component enforces access control in computer systems?

- ✓ ○ A. Reference monitor
- ✓ ○ B. Audit log
- ✓ ○ C. Object

- ✓ ○ D. Security kernel
- ✓ ○ E. Security resource

**Answer Key:** D

Question 11 of 20 0.25 Points

Eric Ormes discussed creating a simple content filtering alert to catch the red team testers that were testing his security.  He created an alert using what term?

- ✓ ○ A. Bluesnarfing
- ✓ ○ B. Kerberoasting
- ✓ ○ C. DirtyCOW
- ✓ ○ D. Shamoon
- ✗ ○ E. CodeRED

**Answer Key:** B

Question 12 of 20 0.25 Points

A pre-computed database of hashes used for password cracking is called a:

- ✓ ○ A. Wordlist
- ✓ ○ B. Salt table
- ✓ ○ C. Hasher
- ✓ ○ D. Rainbow table
- ✓ ○ E. None of the above

**Answer Key:** D

Question 13 of 20 0.25 Points

The IoT has many security problems.  Which of the following is NOT one of them:

- ✓ ○ A. Devices are not accessible from the Internet
- ✓ ○ B. Devices are installed and forgotten about
- ✓ ○ C. Devices have little or no security built in
- ✓ ○ D. Users often don’t change default settings
- ✓ ○ E. All of the above area IoT security problems

**Answer Key:** A

Question 14 of 20 0.25 Points

A tool to discover and explore unsecured IoT devices is:

- ✓ ○ A. Google
- ✓ ○ B. Wireshark
- ✓ ○ C. Shodan
- ✓ ○ D. Cyber range
- ✓ ○ E. All of the above

**Answer Key:** C

Question 15 of 20 0.25 Points

Wireshark is an example of a:

- ✓ ○ A. Sniffer
- ✓ ○ B. Protocol analyzer
- ✓ ○ C. Network scanner
- ✓ ○ D. A and B
- ✓ ○ E. All of the above

**Answer Key:** D

Question 16 of 20 0.25 Points

Eric Ormes recommended a good training website to use if you are interested in becoming part of a Red Team.  What is the site?

- ✖ ○ A. Hack the box
- ✔ ○ B. TryHackMe
- ✔ ○ C. Instruqt
- ✔ ○ D. HackerOne
- ✔ ○ E. KnowBe4

**Answer Key:** B

Question 17 of 20 0.25 Points

IP address spoofing is an example of:

- ✔ ○ A. Masquerading
- ✔ ○ B. Birthday attack
- ✔ ○ C. Phishing
- ✔ ○ D. Whaling
- ✔ ○ E. War driving

**Answer Key:** A

Question 18 of 20 0.25 Points

The difference between a virus and a worm is:

- ✔ ○ A. A worm doesn’t replicate
- ✔ ○ B. A worm requires a host program but a virus does not

- ✓ ○ C. A virus requires a host program but a worm does not
- ✓ ○ D. A worm is malware but a virus is not

**Answer Key:** C

Question 19 of 20 0.25 Points

War driving is physically driving around:

- ✓ ○ A. To packet sniff Bluetooth communications
- ✓ ○ B. Looking for open wireless access points
- ✓ ○ C. Creating rouge access points
- ✓ ○ D. Jamming the wireless communications
- ✓ ○ E. All of the above.

**Answer Key:** B

Question 20 of 20 0.25 Points

Malware countermeasures include:

- ✓ ○ A. Educating users
- ✓ ○ B. Anti-virus scanners
- ✓ ○ C. Testing programs on a quarantined computer
- ✓ ○ D. A and B
- ✓ ○ E. All of the above

**Answer Key:** E