Week 8 - Quiz

Due Sep 21 at 23:59 **Points** 15 **Questions** 15
Available Sep 20 at 0:00 - Sep 21 at 23:59 **Time Limit** None
Allowed Attempts 2

Instructions

This is the **eight** weekly quiz.

Keep in mind that the quizzes do not directly contribute to your marks (except through your participation mark). This is so that you can feel free to actually use them to self-assess your progress and see how you are doing. This, of course, doesn't mean that you should ignore them. Indeed, they are a very important way for you to obtain feedback on how you are doing.

This quiz was locked Sep 21 at 23:59.

Attempt History

	Attempt	Time	Score
KEPT	Attempt 1	84 minutes	6.35 out of 15
LATEST	Attempt 2	2,093 minutes	0 out of 15
	Attempt 1	84 minutes	6.35 out of 15

Score for this attempt: **0** out of 15
Submitted Sep 21 at 23:59
This attempt took 2,093 minutes.

Unanswered **Question 1** 0 / 1 pts

Match the following Cyber Security practices to their terms.

You Answered
Update software to close vulnerabilities and shut down bugs. [ ]

Install Patches

You Answered
Train employees to be vigilant. [ ]

Educate the Team

You Answered
Cultivate an environment that encourages honesty [ ]

with regards to cyber security problems.

Promote a Culture of Forgiveness

You Answered

Schedule deep scans and when in doubt, use quick scans.

Leverage Traditional and New Antivirus Software

You Answered

Have resources available for responding to breaches.

Keep Cyber Security Resources at Hand

Unanswered

Question 2

0 / 1 pts

The statement *"Individuals who work to exploit vulnerabilities in a computer system, sometimes for information gathering, protest or theft"* defines which one of the following threats?

- Employees
- Correct Answer — Hackers
- Hacktivists
- Activists
- Corporate Spies

Unanswered

Question 3

0 / 1 pts

The term Authentication is defined by which of the following statements?

- The ability to recover lost data.
- Method for ensuring data security.
- A means to enhance digital security.
- Correct Answer

The process of determining whether a computer system user is who he or she claims to be

Unanswered **Question 4** 0 / 1 pts

Match the following definitions to the correct cyber attack.

You Answered A type of application that can gain unauthorised access or cause damage to a computer or computer system. [ ]

Malware

You Answered Conversation monitoring, whether by listening in on a room, tapping into a landline or cell phone, or intercepting an email. [ ]

Eavesdropping

You Answered Exploiting vulnerabilities in a computer system, sometimes for information gathering, protest or theft. [ ]

Hacking

You Answered Intercepting the communication between two parties in an attempt to spy on the victims, steal credentials or personal information, [ ]

Man in the middle Attack

You Answered The act of pretending to be something or someone you are not in order to gain access to sensitive information. [ ]

Spoofing

You Answered A cyber-attack where an attacker tries to guess, or [ ]

crack a user's password.

Password Attack

You Answered

The act of modifying devices

Tampering

You Answered

Maliciously written codes that alter how a computer operates and can damage the computer and data stored on i

Virus

You Answered

A method that locks data systems or individual devices.

Ransomware

You Answered

An attacker essentially floods a target server with traffic in an attempt to disrupt, and perhaps even bring down the target.

Distributed Denial-of-Service Attack

You Answered

An attempt to acquire sensitive or valuable information by pretending to represent a legitimate organisation or person, often someone of authority.

Phishing

You Answered

A more sophisticated form of a phishing attack in which cybercriminals target only privileged users such as system administrators and C-suite executives

Spear Phishing

Unanswered **Question 5** 0 / 1 pts

Which of the following terms can be defined as *"a requirement of more than one method to validate an user"*

- Authorisation
- Correct Answer — Two-Factor Authentication
- Authentication

Unanswered **Question 6** 0 / 1 pts

"The process by which data is scrambled and encoded to make it unintelligible" is which of the following?

- Decryption
- Correct Answer — Encryption

Unanswered **Question 7** 0 / 1 pts

The following statement *"A password that works for only one network session or transaction"* defines which of the following terms.

- Authorisation.
- Authentication
- Security Token
- Correct Answer — One-Time Password

Unanswered **Question 8** 0 / 1 pts

A data security management plan includes which of the following? (Select all that are applicable).

- Correct Answer — Verifying and Updating the plan's components.
- Correct Answer — Implementing the plan
- The effective oversight of the organisation.
- Correct Answer — Developing a plan

Ensuring the data is not accessed by unauthorised users.

Unanswered

Question 9

0 / 1 pts

The *"cyber kill chain"* is a sequence of stages required for an attacker to successfully infiltrate a network and exfiltrate data from it.

Order the stages of a *"cyber kill chain"*.

You Answered

Stage 1

Reconnaissance & Probing

You Answered

Stage 2

Delivery & Attack

You Answered

Stage 3

Exploitation & Installation

You Answered

Stage 4

System Compromise

Unanswered

Question 10

0 / 1 pts

Which of the following best defines the security incident *"Improper Usage"*?

Correct Answer

Any incident resulting from violation of an organization's acceptable usage policies by an authorized user.

An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services

An attack executed via an email message or attachment (e.g. malware infection).

The loss or theft of a computing device or media used by the organization, such as a laptop or smartphone.

Unanswered

Question 11

0 / 1 pts

Match the following security incidents to the correct recommended action.

You Answered

Remediate any infections as quickly as possible before they progress.

Malware Infection

You Answered

Configure your critical systems to record all privileged escalation events and set alarms for unauthorized privilege escalation attempts.

Unauthorised Privilege Escalation

You Answered

Identify the privileged user accounts for all domains, servers, apps, and critical devices and ensure that monitoring is enabled for all systems

Insider Breach

You Answered

Detect, monitor and investigate unauthorized access attempts – with priority on those that are mission-critical and/or contain sensitive data.

Unauthorised Access

Unanswered **Question 12** 0 / 1 pts

Which of the following incident types aligns to the *"Exploitation and Installation"* Stage of the cyber kill chain? (Select all that are applicable).

- [ ] Malware Infection
- Correct Answer [ ] False Alarms
- [ ] Port Scanning Activity
- Correct Answer [ ] Unauthorized Privilege Escalation
- Correct Answer [ ] Distributed Denial Of Service Diversion
- Correct Answer [ ] Unauthorized Access
- Correct Answer [ ] Distributed Denial Of Service
- [ ] Destructive Attack
- [ ] Insider Breach

Unanswered **Question 13** 0 / 1 pts

Match the source of cyber security threats to the correct definition.

You Answered
Groups that use phishing, spam, spyware, and malware to conduct identity theft, online fraud, and system extortion to infiltrate systems or networks for financial gain. [ ]

Criminal Groups

You Answered
Groups that conduct cyber attacks to destroy, infiltrate, or exploit critical infrastructure to threaten national security, compromise military equipment, disrupt the economy, and cause mass casualties. [ ]

Terrorist Groups

You Answered
Groups or individuals that carry out cyberattacks in support of political causes rather than financial gain. [ ]

Hacktivists

You Answered

Employees, third-party vendors, contractors, or other business associates who have legitimate access to enterprise assets but misuse that accesses to steal or destroy information for financial or personal gain.

Malicious Insiders

You Answered

Individuals who conduct industrial or business espionage to either make a profit or disrupt a competitor's business by attacking critical infrastructure, stealing trade secrets, and gaining access.

Corporate Spies

Unanswered

Question 14

0 / 1 pts

Which of the following are some best practices to protect from cyber security? (Select all that are applicable).

Correct Answer ☐ Create an insider program.

☐ Only protect sensitive data.

Correct Answer ☐ Backup data

Correct Answer ☐ Update Systems and Software

Correct Answer ☐ Maintain Compliance

Correct Answer ☐ Train Employees

☐ Provide access to sensitive information to all employees.

Unanswered

Question 15

0 / 1 pts

Match the following common incidents to the correct response strategy.

You Answered

Quarantine the malicious email from all accounts on the system. Be sure no one can access the email from anywhere on your network until it is reviewed by an administrator.

Phishing

You Answered

Change passwords of all accounts and block email access from countries where employees won't be logging in.

Business Email Account Takeover

You Answered

Contain and eradicate. Disconnect the computer from the network, but don't power the device off. Work through the system and eradicate any malicious files or applications.

Malware

Other Incorrect Match Options:

- Spoofing
- Ransomware
- Virus

Quiz Score: **0** out of 15

◂ Previous Next ▸

Last Attempt Details:

Time:	2,093 minutes
Current Score:	0 out of 15
Kept Score:	6.35 out of 15

2 Attempts so far
View Previous Attempts
No More Attempts available