CYB0103: Cybersecurity Design Principles
Question Bank

Chapter 5
Prepared by: Rana Al Haj Fakeeh

Part I: multiple choice questions:

1) Firewalls and intrusion detection and prevention systems are examples of security measures at which layer:

A) Perimeter security.
B) Network security.
C) Endpoint security.
D) Data security / protection.

Answer: A

2) Virtual private networks (VPNs), secure socket layer (SSL) are examples of security measures at which layer:

A) Perimeter security.
B) Network security.
C) Endpoint security.
D) Data security / protection.

Answer: B

3) Antivirus, antimalware, and e-mail security solutions are examples of security measures at which layer:

A) Perimeter security.
B) Network security.
C) Endpoint security.
D) Data security / protection.

Answer: C

4) Encryption, hashing, and backups are examples of security measures at which layer:

A) Perimeter security.
B) Network security.
C) Endpoint security.
D) Data security / protection.

Answer: D

5) Virtual private networks (VPNs) are an example of security measures at TWO layers. Which are they:

A) Perimeter and Network.
B) Network and Access.
C) Perimeter and Access.
D) None of the above.

Answer: C

6) _____ controls include security measures that consist of policies or procedures directed at an organization's employees:

A) Physical controls.
B) Technical controls.
C) Administrative controls.
D) None of the above.

Answer: C

7) Layered Security includes which category of controls:

A) Physical controls.
B) Technical controls.
C) Administrative controls.
D) None of the above.

Answer: B

8) Which category of FLI threats refers to a system not to perform its intended function:

A) Failure (F).
B) Lies (L).
C) Infiltration (I).
D) None of the above.

Answer: A

9) Which category of FLI threats refers to a system being fed false information or deceptive commands:

A) Failure (F).
B) Lies (L).
C) Infiltration (I).
D) None of the above.

Answer: B

10) Which category of FLI threats refers to unauthorized access to a system:

A) Failure (F).
B) Lies (L).
C) Infiltration (I).
D) None of the above.

Answer: C

Part II: true / false questions:

#	Question	Answer
1	The layered security is about implementing the same defense multiple times. For example, having McAfee, Norton, and Avast antivirus tools installed on your Windows computer.	F
2	An organization sets up a firewall, runs an Intrusion Protection System with trained security operators, and deploys an antivirus program, is an example of implementing multi-layered security.	T
3	Access control creates virtual borders between systems.	F
4	Defense-in-Depth is considered part of Layered Security.	F
5	In comparison with Defense-in-Depth, multi-layered security uses the idea that various security measure will recover systems from threats after they happen.	F

Commented [R.1]: not about

Commented [R.2]: Network Segmentation

Commented [R.3]: Layered Security is considered part of Defense-in-Depth

Commented [R.4]: will protect systems against threats after they happen

Part III: essay questions:

1) List four examples on the importance of Multi-layer Defense approach.

- Protects against evolving threats and vulnerabilities.
- Create redundancy in security defenses, making it more difficult for an attacker to breach the system.
- By implementing security controls, organizations can better identify, prevent, and mitigate potential attacks.
- Ensures confidentiality, integrity, availability, and traceability of data and systems.
- Helps organizations comply with regulatory requirements.
- A multi-layered security strategy is an efficient and effective method of detecting and eliminating threats at multiple levels.
- Each layer of security you add will strengthen your defenses until you have created a nearly impenetrable wall of defense.

2) List the essential Layers of Defense in cybersecurity with one example each.

- **Perimeter security** – such as firewalls.
- **Network security** – such as virtual private networks (VPN).
- **Endpoint security** – such as antivirus.
- **Data security** – such as encryption.
- **Monitoring and prevention** – such as vulnerability scanners.
- **Access Measures** – such as biometrics.

3) Defense-in-Depth covers three levels/categories of security controls. List them with one example each.

- **Physical controls** – such as security guards or locked doors.
- **Technical controls** – such as a firewall or antivirus program.
- **Administrative controls** – such as policies on how employees should create and manage their passwords or training on incident response plans.