VU QUIZ REPORT

Generated by VU TALK Extension

Subject: CS205

Quiz Completed: 1/9/2026, 10:50:40 AM
Total Questions: 10

Question 1:

What type of machine should network administrators use for administrative tasks?

A. Isolated from organization’s primary network

B. Email and browsing facility available

C. Used for composing documents

D. Have internet access

Selected Answer: A

Question 2:

As per malware defense control why DNS query logging should be enabled?

A. analyze and block inbound email attachments with malicious behavior

B. To detect host-name lookup for known malicious domains

C. Continuously monitor and defend organization’s servers and workstations

D. To lower the chance of spoofed or modified emails from valid email addresses

Selected Answer: B

Question 3:

The dedicated machine used by administrators for administrative tasks should have following features.

A. Have internet access

B. Isolated from organization’s primary network

C. All routine operational functions can be performed on it

D. Email and browsing facility available

Selected Answer: B

Question 4:

In which format results of penetration testing should be documented?

A. XML format

B. PDF format

C. Machine readable standard

D. Excel format

Selected Answer: C

Question 5:

The 4-layer security transformation model.

A. Will be rejected by the it dept as it takes too much hard work

B. Is adapted to solve Pakistan’s security posture challenges while being practical not to waste time on security governance in the absence of solid underlying security controls

C. Is overkill

D. Takes too much time and effort to implement

Selected Answer: B

Question 6:

Why cis recommends to configure monitoring system in an organization’s network?

A. To record the network packets passing through the boundary

B. To detect compromise of systems at organization’s network boundaries

C. To block data loss through organization’s network boundaries

D. To block malicious traffic at organization’s network boundaries

Selected Answer: B

Question 7:

Security governance may be considered as.

A. A parallel function to it governance

B. A function lying above the it governance framework

C. An out-dated concept which is no longer practical

D. A sub-function of the it governance framework

Selected Answer: D

Question 8:

What should an organization do to control access to sensitive information on need-to-know basis?

A. Locate all sensitive information on separate vlans

B. Store all sensitive information on single server

C. Locate all sensitive information on single vlans

D. Store sensitive information on multiple servers

Selected Answer: C

Question 9:

If a system in an organization gets compromised, how can we prevent an attacker to compromise the neighboring systems?

A. Through network-based intrusion detection system(ips)

B. Through system firewall

C. Through network-based intrusion prevention system(ips)

D. Through antivirus

Selected Answer: C

Question 10:

How can an authorized wireless access point connected to a wired network can be detected?

A. Through host-based data loss prevention (dlp)

B. Through wireless intrusion detection system

C. Through network-based intrusion detection system

D. Through file integrity monitoring solution

Selected Answer: B