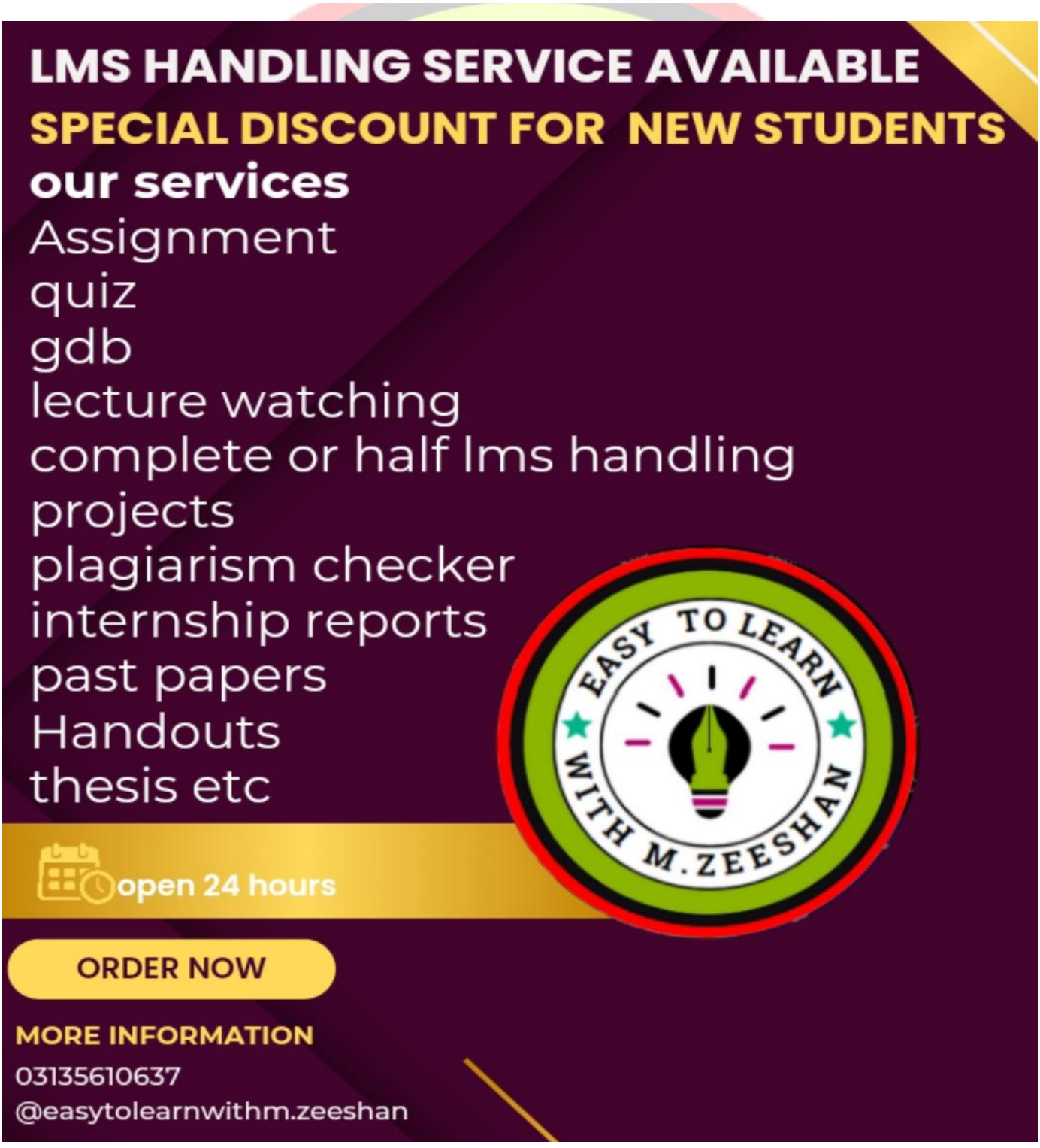
Easy to learn with M.Zeeshan

@easytolearnwithm.zeeshan · 10.8K subscribers · 494 videos

Assalam o alaikum ...more

whatsapp.com/channel/0029VakCijnBqbr6wqv0Bg3U and 2 more links

Subscribed



CS205 FINAL TERM QUIZ 4 2025

JON OUR WHASTAPP CHANNEL FOR CURRENT PAPERS AND MORE UPDATES

CLICK HERE TO JOIN

Which of the following system configuration management tool is used for Linux systems?
The correct answer is Puppet.
Explanation: Puppet is a widely used system configuration management tool that automates the deployment, configuration, and management of Linux (and other OS) systems. It uses a declarative language to define system states and ensures consistency across the infrastructure.

As per CIS Critical Security Framework, what is recommended for network boundaries of an organization?
The correct answer is Deny communication over unauthorized TCP or UDP ports.
Explanation: According to the CIS Critical Security Framework, it is recommended to block all unauthorized communication across network boundaries, including both TCP and UDP ports. This ensures that only explicitly allowed and necessary traffic is permitted, reducing the attack surface and enhancing network security.

As per CIS, which authentication protocols should be used by wireless networks?
The correct answer is Which require digital certificates for authentication.
Explanation: According to the CIS Critical Security Framework, wireless networks should use authentication protocols that leverage digital certificates, such as EAP-TLS (Extensible Authentication Protocol-Transport Layer Security). This ensures secure authentication and protects against unauthorized access to the network.

In which mode should vulnerability scanning be performed?
The correct answer is Authenticated mode.
Explanation: Vulnerability scanning should be performed in authenticated mode to provide deeper insights into potential vulnerabilities. This mode allows the scanner to access the system using valid credentials, enabling it to identify security flaws that unauthenticated scans might miss, such as misconfigurations or outdated software versions.

How can an authorized wireless access point connected to a wired network be detected and alerts generated?
The correct answer is Through network-based intrusion detection system.
Explanation: A network-based intrusion detection system (NIDS) monitors network traffic and can identify unauthorized wireless access points connected to a wired network. It generates alerts when unusual or unauthorized activities are detected, helping to maintain network security.

As per CIS framework, what is the best practice to store logs generated from a system?
The correct answer is Aggregate logs to a central management system.
Explanation: According to the CIS Framework, the best practice is to aggregate logs to a centralized management system. This approach enhances log integrity, facilitates monitoring and analysis, and allows for better incident detection and response by consolidating data from multiple systems in one place.

Wireless access control comes under which category of CIS Top 20 controls?
The correct answer is Foundational.
Explanation: Wireless access control falls under the "Foundational" category of CIS Top 20 Controls. Foundational controls are essential for securing network infrastructures, ensuring that only authorized devices and users can access wireless networks, thereby reducing vulnerabilities and risks.

Generally speaking, security implementation in Pakistan is:
The correct answer is One generation behind that of IT.
Explanation: Generally, security implementation in Pakistan is considered to lag behind modern IT advancements by about one generation. This is due to limited investment in advanced security technologies, a lack of skilled resources, and slower adoption of global security practices.

The main difference between security organization in a large-sized and medium-sized organization is that the following is absent in a medium-sized security organization:
The correct answer is Chief Risk Officer.
Explanation: In medium-sized organizations, the role of a Chief Risk Officer (CRO) is often absent due to limited resources and a smaller scope of operations. Larger organizations typically have a CRO to oversee enterprise-wide risk management, including security, whereas medium-sized organizations rely on other roles to handle such responsibilities.

Which of the following can be used to block malicious traffic on an organization's network boundaries?
The correct answer is Network-based intrusion prevention (IPS) system.
Explanation: A network-based intrusion prevention system (IPS) is designed to actively monitor and block malicious traffic at the organization's network boundaries. It not only detects potential threats but also takes action to prevent them from entering or leaving the network, making it more effective in blocking attacks than other options like IDS or host-based systems.