معهد المورد للتدريب
AL MAWRED TRAINING INSTITUTE

CompTIA Cybersecurity Analyst (CySA+) Certification

Course Outline

Network Analysis

Network Data Analysis
Network Data Correlation, Output, and Tools
Scanning a Host with NMAP
Network Segmentation and Honeypots
Group Policies, ACLs, Hardening, and NAC
Configuring a Host Firewall on Ubuntu using UFW

Security Practices

Pentesting — Part 1
Pentesting — Part 2
Reverse Engineering
Risk Evaluation
Analyzing Possible Malware
Threat Management

The Vulnerability Management Process

Vulnerability Scan Requirements and Frequency
Vulnerability Reports, Remediation, and Continuous Monitoring
Installing and Configuring OpenVAS

Common Symptoms

Network Related Symptoms
Host Related Symptoms
Netcat and Application Related Symptoms
Looking for Malware on Windows Systems
Looking for Malware on Linux Systems
Using Wireshark to Identify Malicious Network Activity

Determining Impact

Incident Response Process and Threat Classifications
Determining Impact Severity and Prioritization and Reviewing Data Classifications

Identity and Access Management (IAM)

Identities, Repositories, Federation, SSO, and Exploits
Working with Windows Accounts and Security Policies
Working with Linux Accounts and Password Policies