CYBERSECURITY FOR ENTERPRISE

OVERVIEW:

This course is mapped to the following certifications:

- **Cisco CyberOPs**
- **CompTIA Security+**
- **CompTIA Cybersecurity Analyst+**
- **Certified Ethical Hacking and Prevention v11**
- **License Pentesting**

This course is meant for those professionals who are looking for comprehensive and total knowledge in the network security domain.

This course is designed take you from novice to expert in cybersecurity This is the only course which teaches both hacking and counter measure techniques. This course is entirely hands on and real time oriented. And need we say the instructor is a network security and intrusion specialists with several years of experience.

Training Course Titles:

- **Understanding Cisco Cybersecurity Operations Fundamentals v1.0 (200-201 CBROPS)**
- **CompTIA Security+**
- **CompTIA Cybersecurity Analyst+**
- **EC-Council Certified Ethical Hacking**
- **EC-Council License Penetesting**

Estimated Time to Completion:

- 12 weeks (3 months)

Technology areas:

- Cybersecurity

Course Outline: Understanding Cisco Cybersecurity Operations Fundamentals v1.0 (200-201 CBROPS)

- Defining the Security Operations Center
- Understanding Network Infrastructure and Network Security Monitoring Tools
- Exploring Data Type Categories
- Understanding Basic Cryptography Concepts
- Understanding Common TCP/IP Attacks
- Understanding Endpoint Security Technologies
- Understanding Incident Analysis in a Threat-Centric SOC
- Identifying Resources for Hunting Cyber Threats
- Understanding Event Correlation and Normalization
- Identifying Common Attack Vectors
- Identifying Malicious Activity

Course Outline: CompTIA Security+

- **Attacks, Threats, and Vulnerabilities**
  - Compare and contrast different types of social engineering techniques.
  - Given a scenario, analyze potential indicators to determine the type of attack.
  - Given a scenario, analyze potential indicators associated with application attacks.
  - Given a scenario, analyze potential indicators associated with network attacks.
  - Explain different threat actors, vectors, and intelligence sources.
  - Explain the security concerns associated with various types of vulnerabilities.
  - Summarize the techniques used in security assessments.
  - Explain the techniques used in penetration testing.
- **Architecture and Design**
  - Explain the importance of security concepts in an enterprise environment.
  - Summarize virtualization and cloud computing concepts.
  - Summarize secure application development, deployment, and automation concepts.
  - Summarize authentication and authorization design concepts.
  - Given a scenario, implement cybersecurity resilience.
  - Explain the security implications of embedded and specialized systems.
  - Explain the importance of physical security controls.
  - Summarize the basics of cryptographic concepts.
- **Implementation**
  - Given a scenario, implement secure protocols.
  - Given a scenario, implement host or application security solutions.
  - Given a scenario, implement secure network designs.
  - Given a scenario, install and configure wireless security settings.
  - Given a scenario, implement secure mobile solutions.
  - Given a scenario, apply cybersecurity solutions to the cloud.
  - Given a scenario, implement identity and account management controls.
  - Given a scenario, implement authentication and authorization solutions.
  - Given a scenario, implement public key infrastructure.

- **Operations and Incident Response**
    - Given a scenario, use the appropriate tool to assess organizational security.
    - Summarize the importance of policies, processes, and procedures for incident response.
    - Given an incident, utilize appropriate data sources to support an investigation.
    - Given an incident, apply mitigation techniques or controls to secure an environment.
    - Explain the key aspects of digital forensics.
- **Governance, Risk, and Compliance**
    - Compare and contrast various types of controls.
    - Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.
    - Explain the importance of policies to organizational security.
    - Summarize risk management processes and concepts.
    - Explain privacy and sensitive data concepts in relation to security.

Course Outline: CompTIA Cybersecurity Analyst+

- **Threat Management**
    - Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes.
    - Given a scenario, analyze the results of a network reconnaissance.
    - Given a network-based threat, implement or recommend the appropriate response and countermeasure.
    - Explain the purpose of practices used to secure a corporate environment.
- **Vulnerability Management**
    - Given a scenario, implement an information security vulnerability management process.
    - Given a scenario, analyze the output resulting from a vulnerability scan.
    - Compare and contrast common vulnerabilities found in the following targets within an organization.
- **Cyber Incident Response**

- Given a scenario, distinguish threat data or behavior to determine the impact of an incident.
- Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation.
- Explain the importance of communication during the incident response process.
- Given a scenario, analyze common symptoms to select the best course of action to support incident response.
- Summarize the incident recovery and post-incident response process.

- **Security Architecture and Tool Sets**
  - Explain the relationship between frameworks, common policies, controls, and procedures.
  - Given a scenario, use data to recommend remediation of security issues related to identity and access management.
  - Given a scenario, review security architecture and make recommendations to implement compensating controls.
  - Given a scenario, use application security best practices while participating in the Software Development Life Cycle (SDLC).
  - Compare and contrast the general purpose and reasons for using various cybersecurity tools and technologies.

Course Outline: Certified Ethical Hacking and Pentesting

- **Module 01: Introduction to Ethical Hacking**
  - Cover the fundamentals of key issues in the information security world, including the basics of **ethical hacking**, information security controls, relevant laws, and standard procedures.
- **Module 02: Foot printing and Reconnaissance**
  - Learn how to use the latest techniques and tools to perform foot printing and **reconnaissance**, a critical pre-attack phase of the ethical hacking process.
- **Module 03: Scanning Networks**
  - Learn different **network scanning** techniques and countermeasures.
- **Module 04: Enumeration**
  - Learn various **enumeration** techniques, such as Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits, and associated countermeasures.

- **Module 05: Vulnerability Analysis**
    - Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems.
- **Module 06: System Hacking**
    - Learn about the various **system hacking** methodologies—including steganography, steganalysis attacks, and covering tracks—used to discover system and network vulnerabilities.
- **Module 07: Malware Threats**
    - Get an introduction to the different types of malware, such as Trojans, viruses, and worms, as well as system auditing for **malware attacks**, malware analysis, and countermeasures.
- **Module 08: Sniffing**
    - Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks.
- **Module 09: Social Engineering**
    - Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.
- **Module 10: Denial-of-Service**
    - Learn about different **Denial of Service (DoS)** and Distributed DoS (DDoS) attack techniques, as well as the tools used to audit a target and devise DoS and DDoS countermeasures and protections.
- **Module 11: Session Hijacking**
    - Understand the various **session hijacking** techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.
- **Module 12: Evading IDS, Firewalls, and Honeypots**
    - Get introduced to firewall, intrusion detection system, and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.
- **Module 13: Hacking Web Servers**
    - Learn about **web server attacks**, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.

- **Module 14: Hacking Web Applications**
    - Learn about web application attacks, including a comprehensive web application hacking methodology used to audit vulnerabilities in web applications and countermeasures.
- **Module 15: SQL Injection**
    - Learn about **SQL injection attack** techniques, injection detection tools, and countermeasures to detect and defend against SQL injection attempts.
- **Module 16: Hacking Wireless Networks**
    - Learn about wireless encryption, wireless hacking methodologies and tools, and Wi-Fi security tools.
- **Module 17: Hacking Mobile Platforms**
    - Learn about mobile platform attack vectors, Android vulnerability exploits, and mobile security guidelines and tools.
- **Module 18: IoT Hacking**
    - Learn how to secure and defend Internet of Things (IoT) and operational technology (OT) devices and possible threats to IoT and OT platforms.
- **Module 19: Cloud Computing**
    - Learn different cloud computing concepts, such as container technologies and server less computing, various cloud-based threats and attacks, and **cloud security** techniques and tools.
- **Module 20: Cryptography**
    - In the final module, learn about **cryptography** and ciphers, public-key infrastructure, cryptography attacks, and cryptanalysis tools.

About the Instructor:

ALIYU Azeez Omotayo

PRINCIPAL CONSULTANT|CEO (SEC-CONCEPTS NETWORKS LTD)

With over 18 years of experience in networking and security, including Cisco networks, Linux, and Windows Server environments, which includes the planning, designing, implementation, troubleshooting of large IP networks and vast experience on Routing, Switching, Security, Service provider, Wireless, Multicast and Quality of Service, VoIP (Voice over IP) / IPT (IP Telephony), Operating Systems and Protocols worldwide, including in Nigeria, South Africa, France and the United States. He holds degrees in Mathematics and Information Networks, and

System Security all from the USA. He is a member of Computer Society of Nigeria (CPN), and an Accredited Management Trainer (CMD). He currently holds more than 150 International IT certifications but not limited to: CCIE R&S, MCSE: Server Administration, CompTIA Network+ and Security+ etc.

He had trained over 15 CCIEs, many CCNPs and a lot students in both Networking and Security.