Zetlan Technologies

GIAC Defensible Security Architect Certification

Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Course Modules

1. **Cloud-based Security Architecture**

Understanding of the concepts involving cloud security, securing on-premise hypervisors, network segmentation, surface reduction, delivery models, and container security.

2. **Data Discovery, Governance, and Mobility Management**

Understanding of file classification, Data Loss Prevention (DLP), database governance, and Mobile Device Management (MDM).

3. **Data-Centric Security**

Understanding of the concepts involving data-centric security. Specifically, have an undrstandg of reverse proxies, web app firewalls, database firewalls, and database activity monitoring.

4. **Fundamental Layer 3 Defense**

o Undstndg of the concepts related to securg basic Layer 3 hardware, protocols & services & have an awareness of common attack vectors.

o In particular, demonstrate a knowledge of CIDR, Layer 3 routing attacks and mitigations, Layer 2/3 benchmark and auditing tools, securing SNMP and NTP protocols, and bogon filtering.

5. Fundamental Security Architecture Concepts

Understanding of the concepts of perimeter-focused deficiencies, presumption of compromise, Zero Trust Model, Intrusion Kill Chain, Diamond Model, software-defined networking, micro-segmentation, threat vector analysis and attack surface analysis.

6. IPv6

Understanding of the concepts of IPV6. Specifcally, have an udrstdg of addressing, dual stack systems, tunneling; & IPv6 router advrtismt attacks and mitigation.

7. Layer 1/Layer 2 Defense

Understanding of the concepts related to securing Layer 1 & Layer 2 services, applications and protocols and be aware of common vectors for these attacks. Specifically, have an understanding of the structure and deployment of VLANs, CDP, MAC spoofing, ARP cache poisoning, DHCP starvation, VLAN hopping, 802.1X, and NAC.

8. Network Defenses

Understanding of the concepts related to network defense. In particular, show a knwldg of NIDS, NIPS, network security monitorng, sandboxing, encryption, and DDOS protections.

9. Network Encryption and Remote Access

Understanding of secure remote access, dual factor for all remote access VPNs and Jump Boxes.

10. Network Proxies and Firewalls

Understanding of Web proxies, SMTP proxies, and next generation firewalls.

11. Zero Trust Endpoints

Understanding of the concepts of securing Zero Trust Endpoints. In particular, demonstrate an understndg of patching via automation, end-user privilege reduction, host hardening, host IDS/IPS; endpoint firewalls, and scaling endpoint log collection.

12. Zero Trust Fundamentals

Understanding of the concepts involving Zero Trust Architecture, credential rotation, & respndg to pivoting adversars & insider threats.

13. Zero Trust Networking

Understanding of the concepts of Zero Trust Networking. Specifically, demonstrate an understanding of authenticating and encrypting endpoint traffic, Domain Isolation, Single Packet Authentication, red herring defenses, & proactive defenses to change attacker behaviors.

Zetlan Technologies

LEARN REMOTELY!!

The efficiency of online learning in terms of time management, flexibility, and the ability to access resources anytime, anywhere can be compelling.

ZETLAN TECHNOLOGIES

www.zetlantech.com

For contact: +91 8680961847
+91 9600579474