Comprehensive Network Defense and Vulnerability Assessment Training Course

23 - 27 Nov 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #NO6483_128555

Course Introduction / Overview:

In today's hyper-connected digital landscape, the integrity of an organization's network is its most critical asset and its most significant vulnerability. This training course provides a comprehensive, in-depth exploration of both offensive and defensive cybersecurity strategies, equipping participants with the skills to protect digital infrastructures proactively. The curriculum moves beyond theoretical knowledge, focusing on the practical application of vulnerability assessment techniques and the implementation of robust network defense mechanisms. As discussed by renowned author William Stallings in his seminal work, "Cryptography and Network Security: Principles and Practice," a layered and intelligent approach to security is paramount. This course, offered by BIG BEN Training Center, embodies that principle by integrating threat intelligence, risk management, and incident response into a cohesive framework. Participants will learn to think like an attacker to identify weaknesses and build resilient defenses, ensuring they can safeguard their organization's data, reputation, and operational continuity against an ever-evolving array of cyber threats.

Target Audience / This training course is suitable for:

- Network Administrators and Engineers.
- Cybersecurity Analysts and Specialists.
- IT Security Managers and Team Leaders.
- Penetration Testers and Ethical Hackers.
- IT Auditors and Compliance Officers.
- Incident Responders.
- System Administrators.
- Information Security Consultants.
- IT professionals seeking to specialize in cybersecurity.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Medical Institutions.
- Information Technology and Telecommunications.
- Governmental and Public Sector Agencies.
- Retail and E-commerce.
- Energy and Critical Infrastructure.
- Consulting and Professional Services.

- Education and Research Institutions.

Target Organizations Departments:

- Information Technology (IT) Department.
- Information Security (InfoSec) Department.
- Risk Management and Compliance.
- Internal Audit and Governance.
- Network Operations Center (NOC).
- Security Operations Center (SOC).
- Technical Support and Help Desk.
- Research and Development.

Course Offerings:

By the end of this course, the participants will have able to:

- Develop a multi-layered network defense strategy based on security best practices.
- Conduct comprehensive vulnerability assessments using industry-standard tools and methodologies.
- Analyze and interpret the results of vulnerability scans to prioritize remediation efforts.
- Configure and manage core network security technologies like firewalls, IDS, and IPS.
- Understand the phases of the ethical hacking lifecycle to identify system weaknesses.
- Implement effective network monitoring and traffic analysis techniques.
- Develop a foundational incident response plan to manage security breaches.
- Integrate cyber threat intelligence into defensive operations.
- Evaluate and enhance an organization's overall security posture.
- Communicate security risks and mitigation strategies to technical and non-technical stakeholders.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive, ensuring that participants not only learn concepts but also master their application. This course employs a blended learning approach that combines expert-led instruction with hands-on lab exercises in a simulated network environment. Participants will engage in real-world case studies of security breaches and defense strategies, analyzing what went right and what went wrong. Collaborative group activities and workshops will encourage peer-to-peer learning and problem-solving, allowing attendees to tackle complex security challenges together. Our instructors facilitate dynamic discussions, encouraging participants to share their unique experiences and perspectives. Continuous feedback is a cornerstone of our approach, with regular knowledge checks and practical assessments to reinforce learning and address individual queries. This active learning model ensures that participants leave the course with tangible skills and the confidence to apply them directly in their professional roles, transforming theoretical knowledge into practical cybersecurity expertise.

Course Agenda (Course Units):

Unit One: Foundations of Network Security and Defense

- Introduction to Cybersecurity Principles (CIA Triad).
- Understanding TCP/IP and the OSI Model from a Security Perspective.
- Mapping the Modern Cyber Threat Landscape.
- Common Attack Vectors and Methodologies.
- Introduction to Security Policies, Standards, and Procedures.
- Legal, Ethical, and Compliance Considerations in Cybersecurity.
- Fundamentals of Cryptography and Its Role in Network Security.

Unit Two: Comprehensive Vulnerability Assessment

- The Vulnerability Management Lifecycle.
- Active vs. Passive Information Gathering and Reconnaissance.
- Introduction to Vulnerability Scanning Tools (e.g., Nessus, OpenVAS).
- Configuring and Running Authenticated and Unauthenticated Scans.
- Analyzing, Interpreting, and Validating Scan Results.
- Vulnerability Prioritization and Risk Rating (CVSS).
- Developing Effective Remediation and Patch Management Strategies.

Unit Three: Implementing Robust Network Defense Mechanisms

- Architecting a Defense-in-Depth Security Strategy.
- Firewall Technologies, Architectures, and Rule-Based Policies.
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).
- Configuring and Managing Virtual Private Networks (VPNs).
- Network Access Control (NAC) and Endpoint Security Solutions.
- Principles of Secure Network Design and Segmentation.
- Introduction to Security Information and Event Management (SIEM) systems.

Unit Four: Ethical Hacking and Penetration Testing Methodologies

- The Five Phases of Ethical Hacking.
- Advanced Scanning and Enumeration Techniques.
- System Hacking: Gaining and Escalating Privileges.
- Malware Threats: Viruses, Worms, Trojans, and Ransomware.
- Sniffing Network Traffic and Session Hijacking Techniques.
- Understanding and Defending Against Social Engineering Attacks.
- Web Application Vulnerabilities (e.g., SQL Injection, XSS).

Unit Five: Incident Response and Cyber Threat Intelligence

- Introduction to the Incident Response (IR) Lifecycle.
- Building an Effective Incident Response Team and Plan.

- Initial Containment, Eradication, and Recovery Strategies.
- Digital Forensics Fundamentals and Evidence Handling.
- The Role of Cyber Threat Intelligence (CTI) in Proactive Defense.
- Utilizing Threat Intelligence Platforms and Feeds.
- Post-Incident Analysis and Reporting for Continuous Improvement.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

How can an organization effectively measure the return on investment (ROI) of its network defense and vulnerability management programs beyond simply counting prevented incidents?

What unique qualities does this course offer compared to other courses?

This training course distinguishes itself by adopting a holistic, 360-degree view of cybersecurity, seamlessly integrating both offensive and defensive paradigms. Unlike programs that teach vulnerability assessment and network defense as separate disciplines, our curriculum is built on the premise that one cannot effectively defend a network without understanding how to attack it. We move beyond a tool-centric approach, focusing instead on the strategic mindset and analytical processes that underpin effective security operations. Participants learn not just how to run a vulnerability scanner, but how to interpret its output within the context of business risk and prioritize remediation based on impact. The course emphasizes practical application through realistic lab scenarios that mirror the complex challenges faced by modern organizations. Our methodology fosters critical thinking, enabling participants to develop bespoke security solutions rather than relying on one-size-fits-all answers. The curriculum is continuously updated to reflect the latest threat intelligence and attack vectors, ensuring the skills learned are not only relevant but also forward-looking, preparing professionals to counter emerging cyber threats.