หลักสูตร นักทดสอบการเจาะระบบ (Penetration Tester)

ในบริบทของสังคมดิจิทัลที่มีการขยายตัวอย่างรวดเร็ว ความต้องการบุคลากรที่มีความเชี่ยวชาญเฉพาะด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์มีแนวโน้มเพิ่มสูงขึ้นอย่างมีนัยสำคัญ อันเนื่องมาจากการเพิ่มขึ้นของภัยคุกคามไซเบอร์ที่มีความซับซ้อนและหลากหลายมากขึ้น การทดสอบเจาะระบบ (Penetration Testing) จัดเป็นวิธีการป้องกันภัยคุกคามทางไซเบอร์เชิงรุกที่มีประสิทธิภาพ เนื่องจากเป็นการค้นหาช่องโหว่ของระบบให้พบเสียก่อนที่จะเกิดการโจมตีจากผู้ไม่ประสงค์ดี ดังนั้นเพื่อเป็นการพัฒนากำลังคนให้สอดคล้องกับความต้องการในภาคอุตสาหกรรม จึงมีความจำเป็นในการพัฒนาหลักสูตรนักทดสอบการเจาะระบบ (Penetration Tester) โดยมุ่งเน้นการบูรณาการหลักการพื้นฐานทางด้านการเขียนโปรแกรม ความปลอดภัยของระบบเครือข่าย และการจัดการช่องโหว่ในระบบสารสนเทศ ตลอดจนการประยุกต์ใช้เครื่องมือด้านความมั่นคงปลอดภัยที่เป็นมาตรฐานสากลในอุตสาหกรรม หลักสูตรนี้จึงมีบทบาทสำคัญในการผลิตกำลังคนที่มีสมรรถนะเชิงเทคนิคและความสามารถในการปฏิบัติงานจริง เพื่อตอบสนองต่อความท้าทายดังกล่าว และสนับสนุนการเสริมสร้างภูมิคุ้มกันทางไซเบอร์ขององค์กรและประเทศชาติอย่างยั่งยืน

วัตถุประสงค์

1. เพื่อให้ผู้เข้าอบรมสามารถเขียนโปรแกรมเบื้องต้นได้
2. เพื่อให้ผู้เข้าอบรมสามารถจัดการระบบสารสนเทศให้มีมาตรฐานด้านความปลอดภัยทางไซเบอร์
3. เพื่อให้ผู้เข้าอบรมสามารถใช้เครื่องมือด้านความมั่นคงปลอดภัยทางไซเบอร์ได้
4. เพื่อให้ผู้เข้าอบรมสามารถทดสอบการเจาะระบบได้
5. เพื่อให้ผู้เข้าอบรมสามารถใช้งานระบบปฏิบัติการ Linux ได้

คุณสมบัติผู้เข้ารับการอบรม

1. มีพื้นฐานด้านคณิตศาสตร์และตรรกศาสตร์
2. มีพื้นฐานด้านระบบเครือข่าย
3. สามารถใช้งานคอมพิวเตอร์และอินเทอร์เน็ตได้

ระยะเวลา

10 วัน (60 ชั่วโมง)

ทักษะที่ได้รับ

- ☑ Programming/Coding
- ☑ Core Security Principles
- ☑ Network Security
- ☑ Security Tools
- ☑ Security Frameworks
- ☑ Linux Administration
- ☑ Threat Hunting
- ☑ Cloud Security
- ☑ Digital Forensics
- ☑ Incident Response
- ☑ Security Information and Event Management (SIEM)

☑ Vulnerability Assessment and Penetration Testing (VAPT)

เงื่อนไขการผ่านบทเรียน

- ต้องเข้าร่วมการเรียนไม่น้อยกว่า 80% ของระยะเวลาทั้งหมด
- ต้องผ่านการทดสอบหลังการอบรม โดยมีคะแนนไม่ต่ำกว่า 70%

สิ่งที่ผู้อบรมจะได้รับจากการอบรม

- สิทธิ์ในการสอบเพื่อรับ ประกาศนียบัตรมาตรฐานสากล IT Specialist: Cyber Security Certification

เนื้อหาการอบรม วันที่ 1

- Introduction to Programming
  - What is Programming?
  - Overview of Programming Languages & Their Uses (Python, JavaScript, Java, C, etc.)
  - Understanding Syntax, Variables, Data Types
  - Setting Up the Development Environment (IDE, Code Editors, Terminals)
  - Hands-on: Writing & Executing Your First Program
- Control Structures & Logic Building
  - Conditional Statements (if-else, switch-case)
  - Loops (for, while)
  - Logical & Comparison Operators
  - Hands-on: Building a Simple Decision-Making Program
- Functions & Code Reusability
  - What Are Functions & Why Are They Important?
  - Defining & Calling Functions
  - Function Parameters & Return Values
  - Hands-on: Creating Functions for Code Modularity
- Data Structures & Working with Collections
  - Lists, Arrays, Tuples, and Dictionaries
  - Basic Operations on Data Structures (Adding, Removing, Modifying)
  - Hands-on: Implementing a Simple Data Processing Program
- File Handling & Basic Debugging
  - Reading & Writing to Files
  - Handling Errors & Debugging Techniques
  - Hands-on: Creating a Simple File-Based Data Storage Program

- Mini Project & Course Wrap-Up
  - Mini Project: Build a Basic CLI Tool or Simple Web Script
  - Best Practices in Programming (Code Readability, Comments, DRY Principle)
  - Next Steps: Learning Paths in Web Development, Data Science, Automation

เนื้อหาการอบรม วันที่ 2

Introduction to Security Principles

- Understanding Cybersecurity & Its Importance
- The CIA Triad (Confidentiality, Integrity, Availability)
- Common Cyber Threats (Malware, Phishing, Ransomware, Insider Threats)
- Security Frameworks & Standards (NIST, ISO 27001, CIS Controls)

- Risk Management & Security Controls
  - Identifying & Assessing Security Risks
  - Security Control Types: Preventive, Detective, Corrective
  - Defense in Depth (Layered Security) & Zero Trust Model
- Identity & Access Management (IAM)
  - Authentication vs. Authorization
  - Role-Based Access Control (RBAC) & Least Privilege Principle
  - Multi-Factor Authentication (MFA) & Identity Federation
- Network & Endpoint Security
  - Secure Network Architecture (Firewalls, IDS/IPS, VPN)
  - Endpoint Security & Hardening (Antivirus, Patching, EDR)
  - Secure Configurations & Hardening Best Practices
- Security Awareness & Incident Response
  - Understanding Social Engineering Attacks (Phishing, Pretexting, Baiting)
  - Best Practices for Security Awareness Training
  - Incident Response Lifecycle (Detection, Containment, Eradication, Recovery)
- Security Best Practices
  - Implementing Security Policies & Governance
  - Cyber Hygiene & Secure Coding Practices

- The Future of Cybersecurity: AI & Cloud Security Trends

เนื้อหาการอบรม วันที่ 3

- Introduction to Network Security
  - Importance of Network Security
  - Threat Landscape & Common Attacks
  - Cybersecurity Frameworks & Best Practices
  - Role of Security Policies
- Network Security Fundamentals
  - OSI & TCP/IP Models – Security Considerations
  - Firewalls: Types & Configurations
  - IDS/IPS (Intrusion Detection & Prevention Systems)
  - VPNs & Secure Communication Channels
- Threats and Vulnerabilities
  - Common Network Attacks (DDoS, Man-in-the-Middle, Phishing, etc.)
  - Malware & Ransomware in Networks
  - Vulnerability Assessment vs. Penetration Testing
- Secure Network Design
  - Network Segmentation & VLANs
  - Zero Trust Security Model
  - Secure Network Architecture
  - Cloud Security Considerations

เนื้อหาการอบรม วันที่ 4

- Cryptography & Authentication
  - Symmetric vs. Asymmetric Encryption
  - SSL/TLS in Network Security
  - Authentication Protocols (LDAP, RADIUS, Kerberos)
  - Multi-Factor Authentication (MFA)
- Wireless & Cloud Security
  - Wireless Network Security (WPA3, WEP, WPA2)
  - Cloud Security Best Practices
  - Securing Hybrid Environments
  - Secure SD-WAN Implementation
- Security Operations & Incident Response
  - Security Operations Center (SOC) Overview

- Network Monitoring & Logging (SIEM, Syslog, NetFlow)
- Incident Response & Forensics
- Handling a Network Security Breach

- Hands-on & Final Assessment
  - Firewall & IDS/IPS Lab Exercise
  - Simulated Attack & Defense Scenarios
  - Security Best Practices Checklist

เนื้อหาการอบรม วันที่ 5

- Overview of Cybersecurity Tools
- Categories of Security Tools:
  - Network Security
  - Endpoint Security
  - Threat Detection & Monitoring
  - Forensics & Incident Response
- Network Security Tools
  - Firewalls: Configuration & Management (pfSense, Cisco ASA, iptables)
  - Intrusion Detection/Prevention Systems (IDS/IPS): Snort & Suricata
  - Wireshark: Packet Analysis & Network Traffic Monitoring
  - Demo: Capturing & Analyzing Network Traffic with Wireshark
- Vulnerability Assessment & Penetration Testing Tools
  - Nmap: Network Scanning & Discovery
  - Metasploit Framework: Exploitation Techniques
  - Nessus/OpenVAS: Vulnerability Scanning
  - Demo:Scanning & Identifying Vulnerabilities with Nmap & Nessus
- Web Security & Application Testing Tools
  - Burp Suite: Web Application Security Testing
  - OWASP ZAP: Web Security Scanning
  - SQLmap: Database Exploitation Testing
  - Demo: Identifying Web Security Vulnerabilities

เนื้อหาการอบรม วันที่ 6

- Threat Detection & SIEM Tools
  - Security Information & Event Management (SIEM): Overview
  - Splunk & ELK Stack: Log Analysis & Threat Hunting
  - Demo: Detecting Malicious Activities Using Splunk

- Digital Forensics & Incident Response Tools
  - Autopsy & FTK Imager: Digital Forensics & Data Recovery
  - Volatility: Memory Forensics for Incident Response
  - Demo: Conducting Basic Digital Forensics Investigation
- Endpoint Security & Malware Analysis
  - EDR Solutions (CrowdStrike, SentinelOne, Windows Defender ATP)
  - YARA & PEStudio: Malware Detection & Reverse Engineering
  - Demo: Analyzing Malware with YARA Rules
- Security Automation & Final Assessment
  - Automating Security Tasks with Python & PowerShell
  - SOAR (Security Orchestration, Automation, and Response) Overview
  - Demo: Simulating a Cyber Attack & Implementing Defense Mechanisms

เนื้อหาการอบรม วันที่ 7

- Introduction to Linux
  - History & Evolution of Linux
  - Linux Distributions (Ubuntu, CentOS, RHEL, Debian)
  - Linux File System Hierarchy
  - User & Group Management
- Linux Command Line & Shell Scripting
  - Basic Linux Commands (ls, cd, mv, cp, rm, cat, etc.)
  - File Permissions & Ownership (chmod, chown, chgrp)
  - Process Management (ps, top, kill, nice, nohup)
  - Introduction to Bash Scripting
  - Demo: Writing Basic Shell Scripts
- Package Management & Software Installation
  - Package Managers (APT, YUM, DNF, Zypper)
  - Installing & Removing Software
  - Managing Repositories & Dependencies
  - Demo: Installing & Configuring Applications
- User & Permission Management
  - Creating & Managing Users & Groups
  - Setting Password Policies
  - sudo & Privilege Escalation

- Demo: Configuring User Access & Permissions

เนื้อหาการอบรม วันที่ 8

- Introduction to Threat Hunting
  - What is Threat Hunting?
  - Proactive vs. Reactive Security
  - Threat Hunting vs. Threat Intelligence vs. Incident Response
  - The Cyber Kill Chain & MITRE ATT&CK Framework
- Understanding Adversary Tactics & Techniques
  - Common Attack Vectors (Phishing, Ransomware, Insider Threats)
  - Advanced Persistent Threats (APTs) & Their Methodologies
  - Understanding Indicators of Compromise (IoCs) & Indicators of Attack (IoAs)
  - Demo: Mapping Attacks to MITRE ATT&CK Framework
- Threat Hunting Methodologies & Techniques
  - Hypothesis-Driven vs. Data-Driven Threat Hunting
  - TTP-Based Hunting (Tactics, Techniques, and Procedures)
  - Threat Hunting with Logs & Network Data
  - Demo: Building a Threat Hunting Hypothesis
- Tools & Data Sources for Threat Hunting
  - SIEM Solutions (Splunk, ELK, Graylog)
  - EDR & XDR Platforms (CrowdStrike, SentinelOne, Microsoft Defender)
  - Network Traffic Analysis (Wireshark, Zeek, Suricata)
  - Demo: Collecting & Analyzing Threat Intelligence

เนื้อหาการอบรม วันที่ 9

- Introduction to Vulnerability Assessment (VA)
  - Overview of Cybersecurity & Threat Landscape
  - Difference Between Vulnerability Assessment (VA) and Penetration Testing (PT)
  - Importance of Regular Vulnerability Assessments
  - Common Types of Vulnerabilities (OWASP, CVEs, Misconfigurations)
  - Regulatory Compliance (PCI-DSS, NIST, ISO 27001, GDPR)
- Understanding Vulnerability Scanning Tools
  - Scanning Methodologies

        - Interpreting CVSS (Common Vulnerability Scoring System)
        - Types of vulnerability scanners
        - Setting Up a Lab Environment for Scanning
    - Vulnerability Scan (Hands-On)
        - Nmap
        - Nessus
        - OWASP ZAP
    - Reporting & Remediation Strategies
        - Best Practices for Documenting Vulnerabilities
        - Creating a Detailed VA Report (Executive vs. Technical Report)
        - Risk-Based Prioritization (Critical, High, Medium, Low)
        - Remediation Strategies:
        - Patching & Updates
        - Configuration Changes
        - Network Segmentation
        - Continuous Monitoring & Integrating VA into Security Framework

เนื้อหาการอบรม วันที่ 10

- Introduction to Penetration Testing
    - Understanding Cybersecurity Threats
    - Difference Between Penetration Testing & Vulnerability Assessment
    - Penetration Testing Methodologies (OWASP, PTES, NIST)
    - Ethical Hacking & Legal Considerations (Laws & Compliance)
    - Types of Penetration Tests
- Setting Up the Penetration Testing Environment
    - Introduction to Kali Linux & Other Pentesting Tools
    - Installing & Configuring Virtual Labs (Metasploitable, DVWA)
    - Understanding Attack Surfaces & Scoping a Test
    - Reconnaissance & Information Gathering
    - Passive vs. Active Reconnaissance
    - OSINT (Open-Source Intelligence)
    - Tools: Nmap, Shodan, Whois, Google Dorking
- Scanning & Enumeration (Hands-On)
    - Network Scanning Using Nmap
    - Identifying Open Ports & Services
    - Enumerating Users & Services

        - Banner Grabbing & Fingerprinting
        - Web Application Reconnaissance (Dirb, Nikto, Gobuster)
    - Exploitation & Gaining Access (Hands-On)
        - Exploiting Vulnerabilities with Metasploit Framework
        - Manual Exploitation Techniques
        - Brute Force Attacks & Credential Exploitation
        - Privilege Escalation Techniques
        - Web Application Attacks:
        - SQL Injection
        - Cross-Site Scripting (XSS)
        - File Inclusion Attacks
        - Post-Exploitation: Maintaining Access & Pivoting
        - sed Machine