Course Title: Information Security Assessment and Penetration Testing

Objectives of This Training:

Information Security Assessment and Penetration Testing course will prepare the participants for effective information systems security, risks assessment, and implementation, audit and VAPT activities. Performing assessment of Information security, Risks and VAPT provides management with key insight into the efficiency and effectiveness of their business processes, and this course looks specifically at the protection of the information assets of the organization. For organizations, information is the most valuable asset the organization possesses, and as Information Security, Risks, VAPT and Assurance professionals, we must be able to provide management with assurance that the information and information systems of the organization are being adequately protected. Throughout this course, participants will benefit from learning the techniques and skills necessary to conduct Security and Risks Assessment, VAPT of IT technologies and ensure that organization has made in IT security is effective. Major topics will cover include Security and Risk Assessment, Audit, Reporting, hardening systems and software of different business and technology area i.e: network, database, software, IOT, Cloud, Project management, risk management, VAPT, encryption, data loss prevention, physical security, Data Center, Information Systems Acquisition, development, management, Operations, resilience etc…

Topics Covered in this Course

Module 1: Information Security Concepts and Risk Management (3 hours)

- Risk Terminology
- Identifying Vulnerabilities
- Operational Risks
- The Risk Assessment Process
- Best Practices for Risk Assessments
- Policies, Procedures, and Incident Response
- A High-Level View of Documentation
- Documents and Controls Used for Sensitive Information
- Auditing Requirements and Frequency

Tabletop / Paper Base Exercise: Security and Risk Assessment of IT Infrastructure

Module 2: Secure Digital Business Channels (3 Hours)

- Digital Transformation and Digital banking
- Business Applications and Digital Channels
    - Obtain Bank Statement
    - Fund Transfer
    - Internet Banking
    - Mobile Banking
    - Bill Payments
    - Finance Management
    - Transaction Monitoring
    - Mobile Apps and Wallet
    - ATM / POS
    - Credit cards
    - Other Channels
- Enterprise Business Infrastructure Architecture

- Enterprise Application Software Implementation and Management Security (ERP)
- BCP and DRP

Module 3. The Technical Foundations of Hacking (1 Hour)

- Foundation Topics
- The Attacker’s Process
- The Ethical Hacker’s Process
- Security and the Stack

Module 4. Foot printing and scanning (6 Hours)

- Foundation Topics
- Overview of the Seven-Step Information-Gathering Process
- Information Gathering
- Determining the Network Range
- Identifying Active Machines
- Finding Open Ports and Access Points
- OS Fingerprinting
- Fingerprinting Services
- Mapping the Network Attack Surface

LAB:

Lab A1: Port Scanning
Lab A2: Hashing from the Command Line
Lab A3: Introduction to Hashing Using a GUI
Lab A4: Introduction to Windows Command-Line Forensic Tools
Lab A5: Cisco IOS Command-Line Basics
Lab A6: Configuring a VPN Client
Lab A7: Using the Windows Command-Line Interface (CLI)
Lab A8: Social Engineering

Module 5. Enumeration and Vulnerability Assessment (6 Hours)

- Foundation Topics
- Enumeration
- Vulnerability Assessment and **Security Research and Analysis**
- Apply Research Methods to Determine Industry Trends and Impact to the Enterprise
- Analyze Scenarios to Secure the Enterprise

Lab:

LAB: Lab Related with Enumeration

Module 6. Sniffing and Spoofing (2 Hours)

- Sniffing and spoofing network traffic
- Sniffing network traffic
- Basic sniffing with tcpdump
- More basic sniffing with WinDump (Windows tcpdump)
- Packet hunting with Wireshark
- Swimming with Wireshark

- Cryptographic Services
- Symmetric Encryption and Asymmetric Encryption
- Hybrid Encryption
- Hashing and Digital Signatures
- Public Key Infrastructure
- Implementation of Cryptographic Solutions
- Cryptographic Attacks

Lab:

Lab A9: Sniffing NETinVM Traffic with Wireshark

Module 7. System hacking and Penetration Testing (6 Hours)

- Network Systems Penetration Testing
- Operating Systems Penetration Testing
- Services Penetration Testing
- Privilege Escalation

Lab:

Lab A10: Cracking Encrypted Passwords
Lab A11: Threat Modeling
Lab A12: Introduction to the Metasploit Framework

Module 8. Web Server Hacking, Web Applications, and Database Attacks (6 Hours)

- Foundation Topics
- Web Server Security Testing
- Web Application Security Testing
- Database Ha
- cking
- Application Security Testing
- Specific Application Issues

LAB:

LAB A13: Security Testing for Web Applications (SQL Injection, Broken Authentication etc…)
Lab A14: Using Windows Remote Access
Lab A15: Performing a Wireless Site Survey
Lab A16: Introduction to a Protocol Analyzer
Lab 17: Perform VAPT Labs for Network, Operating Systems, Web Applications

Module 9: Securing Virtualized, Distributed, and Shared Computing (1 Hour)

- Enterprise Security
- Cloud Computing
- Virtualization
- Virtual LANs
- Virtual Networking and Security Components
- Enterprise Storage

LAB:

Lab A18: Shopping for Wi-Fi Antennas
Lab A19: Cloud Provisioning
Lab A20: Exploring Your Virtual Network

Module 10: Host Security (4 Hours)

- Firewalls and Network Access Control
- Host-Based Firewalls
- Trusted Operating Systems
- Endpoint Security Solutions
- Anti-malware
- Host Hardening
- Asset Management
- Data Exfiltration
- Intrusion Detection and Prevention
- Network Management, Monitoring, and Security Tools

LAB:

Lab A21: Verifying Systems Security Configuration Baseline

Module 11: Enterprise Security Integration (2 Hours)

- Integrate Enterprise Disciplines to Achieve Secure Solutions
- Integrate Hosts, Storage, Networks, and Applications into a Secure Enterprise Architecture

Reporting: Repot Preparation for VAPT and Security and Risk Assessment of IT Infrastructure

Certificate Awarding Criteria / Evaluation Criteria:

1. Participants Must Attend in MCQ Exam (15%)
2. Participants Must Attend in LAB Exam (25%)
3. Participants Must Submit LAB Assignment Report on VAPT (10%)
4. Participants Present the Report (10%)
5. Participants Must Pass Cyber Range Exam (40%)

Certification Mapping:

After Completing this course Participants will achieve the knowledge and skills in way so they can seat, interpret and demonstrate the knowledge, skills and can perform hands-on Practical work in their workplaces including mapping with different certifications which are recognized by NSDA, DOD, NIST, ANSI Certifications.

- ✔ Certification and Courses from NSDA
- ✔ Ethical Hacking Course and Exam
- ✔ Penetration Testing Course and Exam
- ✔ Defensive Architecture Exam
- ✔ Comptia Security+ CASP Course and Exam
- ✔ Etc….