

Ducara Info Solutions (P) Ltd.

CIETVA

Certified Enterprise Threat & Vulnerability Assessor

OverView

Manage Threats & Vulnerability at Enterprise Level!

Exploitation of information systems is rising rapidly today. More numerous, more capable and much more destructive attacks are encountered by many companies.

In this course, we'll help you better understand what is ETVA, how to mitigate information security risks affecting organizations across the globe, threat management, comprehensive vulnerability assessment and various approaches to ensure true value across the enterprise.

TarGeT AuDienCe

Ethical Hackers, Auditors & Managers

- ✓ Security Auditors
- ✓ Vulnerability Assessors
- ✓ System Administrators
- ✓ Vulnerability Program Managers

Compliance Officers & Consultants

- ✓ Technical Security Consultants
- ✓ Pen-testers
- ✓ IT Consultants
- ✓ Corporate Governance Specialists



Objective

Real Industry Standard Security Tools to Build Technical Skills

This course is the results of decades of experience performing vulnerability assessments, a combination of theory and practical exercises that are used for managing modern threats & vulnerabilities.

Various tools, techniques, methodologies and automation usage is included in this course to enhance your skills for implementing manageable strategies with consideration of different environments.

CouRse OuTline

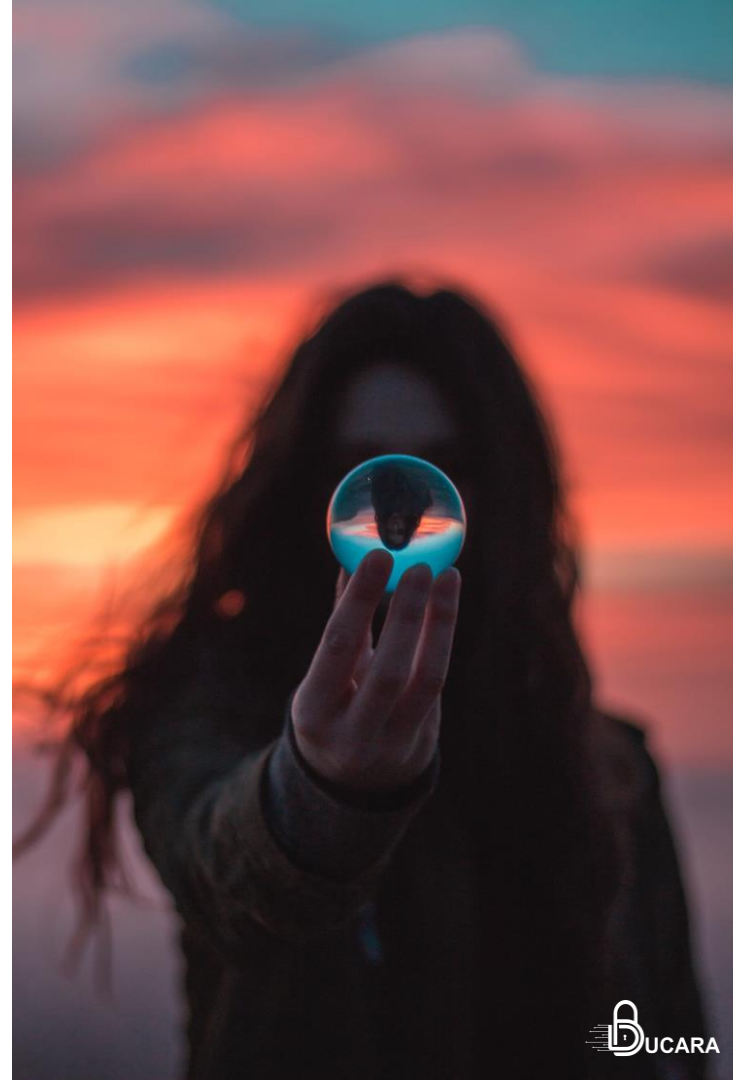
Course Duration: 40 Hrs

1. Methodology, Planning, and Threat Modeling
2. Open Source Intelligence Gathering
3. Network and Website Services Enumeration
4. Web Application Vulnerability Enumeration
5. Network Vulnerability Enumeration
6. Discovery of Vulnerabilities in WebApps & Websites
7. Discovery of Vulnerabilities in Networks
8. Vulnerability Validation & Data Management
9. Triage – Security Incidents
10. Remediation
11. Auditing & Reporting

MoDule 1

Methodology, Planning & Threat Modeling

1. Maximizing Value from Vulnerability Assessments & Programs
2. Enterprise Architecture and Strategy
3. Developing Transformational Vulnerability Assessment Strategies
4. Performing Enterprise Threat Modeling
5. Generating Compounding Interest from Threat Intelligence and Avoiding Information Overload
6. The Vulnerability Assessment Framework
7. Overview of Comprehensive Network Scanning
8. Compliance Standards and Information Security
9. Team Operations and Collaboration



MoDuIE 2

Open Source Intelligence Gathering

1. OSINT Cycle
2. Social Media & Geo-location
3. Network, Government & Business
4. Dark Web

MoDuIE 3

Network and Website Services Enumeration

1. Service Enumeration
2. Nmap Port Scanner
3. Masscan Enumeration
4. Web Frontend & Backend
5. Domain information Using Recon-ng
6. Web Crawling Using HTTrack



MoDuLE 4

Web Application Vulnerability Enumeration

1. Web Application Assessment
2. Acunetix Vulnerability Scanner
3. OWASP ZAP Proxy
4. Burp Suite Web Analyzer
5. Nikto
6. WPScan for WordPress Scanning

MoDuLE 5

Network Vulnerability Enumeration

1. Network Vulnerability Assessment
2. Nmap and Zenmap
3. Tripwire SeureCheq Scanner
4. Nessus Network Vulnerability Scanner

MoDuIE 6

Discovery of Vulnerabilities in WebApps & Websites

1. Web Application VM Lab Setup
2. SQL Injection Attack
3. Cross-Site Scripting Attack
4. Cross-Site Request Forgery Attack
5. Denial of Service Attack (DOS)
6. Buffer Overflow Attack
7. File Upload Attack
8. Insecure Cryptographic Storage
9. Sensitive Data Exposure
10. Local File Inclusion
11. Brute Force Attack

MoDuIE 7

Discovery of Vulnerabilities in Networks

1. Various Server Vulnerabilities
2. Protocol Password Attack
3. Sniffing/Spoofing
4. Wireless Attack
5. Flooding Attack
6. Various System Vulnerabilities
7. Phishing Attack
8. Windows Vulnerabilities
9. Malware Attack to Breach Security
10. Browser Vulnerabilities

MoDulE 8

Vulnerability Validation & Data Management

1. Recruiting Disparate Data Sources
 2. Manual Vulnerability Validation Targeting Enterprise Infrastructure
 3. Converting Disparate Datasets into a Central, Normalized, and Relational Knowledge Base
 4. Managing Large Repositories of Vulnerability Data
 5. Querying the Vulnerability Knowledge Base
 6. Evaluating Vulnerability Risk in Custom and Unique Systems, including Web Applications
-



MoDulE 9

Triage – Security Incidents

1. Security Triage Overview
2. Types of Security Incidents
3. External Media Attack (USB)
4. Drive by Download Attack
5. Attrition Attack
6. Email Attack
7. Assessing the Relative Importance of Vulnerabilities Against Strategic Risk

MoDuIE 10

Remediation

1. Seven Ways to Stop Attacks
2. Monitor Network Connections
3. Spoofing Attack Remediation
4. System Auditing Process
5. Identify Basic Threats
6. Deploy a Vulnerability Management System

MoDuIE 11

Auditing & Reporting

1. Domain Password Auditing
2. Creating and Navigating Vulnerability Prioritization Schemes in Acheron
3. Developing a Web of Network & Host Affiliations
4. Modeling Account Relationships on Active Directory Forests
5. Creating Effective Vulnerability Assessment Reports
6. Transforming Triage Listing into the Vulnerability Remediation Plan



Connect Us!

Ducara help harnessing latest security trends & enhancing skills to simplify IT security complexity efficiently.

✉ info@ducarainfo.com

🌐 www.ducarainfo.com