Course Outline

Cyber Security and Ethical Hacking

For Interactive Cares

Papan Saha
Cyber Security Analyst
Wipro Limited

Contents

Recorded course module:

Introduction to Cyber Security & Ethical Hacking

- What is Hacking? Who is a Hacker?
- Skills of a Hacker, Types of Hackers.
- Reasons for Hacking. Who are at the risk of Hacking attacks.
- Elements of Information Security.
- System Hacking concepts.
- Network Security concepts.
- The Security, Functionality & Usability Triangle.
- What is Ethical Hacking.
- Why Ethical Hacking is Necessary.
- Scope & Limitations of Ethical Hacking.
- What is Vulnerability Assessment.
- What is Penetration Testing.
- Audit and Compliances
- Overview of Cyber Security
- Importance of Cyber Security
- Types of Cyber Attacks
- Web Application Basics
- HTTP/HTTPS Protocol
- Web Application Architecture
- VPNs and Secure Communication
- Virtual Private Networks
- Secure Communication Protocols
- Security testing methodology
- Other security threats and concepts
- Ethics and Cyber security laws

Main course modules (Career Path):

Class# 1: Foot Printing and Enumeration

- What is Reconnaissance and Foot Printing
- Objectives of Foot Printing
- What is Enumeration
- SNMP Enumeration
- SMTP Enumeration
- DNS Enumeration
- Information gathering Tools and techniques
- Finding an organization's details / domain name / Internal & Public and Restricted URLs
- Finding an organization’s Server details
- Finding the details of domain registration

Class# 2: Operating System for Security testing (Kali Linux, BackBox, ParrotSec)

- Overview of security testing environment
- Selection and Installation
- Configuration Setup
- Introduction with tools and scope of usability

Class# 3: Introduction to Vulnerability Assessment and Scanning

- Types of Scanning
- What is a Vulnerability Assessment or scanning?
- Types of Vulnerability Scanner tools
- System scanning and overview of tools
- Web application scanning and overview of tools
- Network scanning and overview of tools

Class# 4: System Scanning techniques and reporting

- Installation of scanners
- Types of scanning
- Understanding scopes
- Configuration of scan
- Performing scan
- Generation of report
- Verification of report and customization

Class# 5: Network and Database/Compliance Scanning techniques and reporting

- Understanding scopes
- Configuration of scan
- Performing scan

- Generation of report
- Verification of report and customization

Class# 6: Web application scanning techniques and reporting

- Installation of scanners
- Types of scanning
- Understanding scopes
- Configuration of scan
- Performing scan
- Generation of report
- Verification of report and customization

Class# 7: Cryptography in security testing

- Basic cryptographic algorithms
- Hashing functions
- Different Types of Encoding Method
- Encryption-Decryption techniques
- Differences between hashing and salting

Class# 8: Penetration Testing Tools and methods

- Introduction with hacking/security tools
- Introduction to Burp-Suite
- Introduction to Metasploit Framework
- SQL map, John the Ripper, Fuzzing, Dirsearch

Class# 9: System Hacking/Exploitation techniques

- Exploitation using vulnerability scan report
- Understanding CVE, CVSS
- Understanding and finding open exploits and exploit database
- Understanding and techniques of DOS/DDOS attacks
- Understanding Buffer overflow

Class# 10: Exploitation of Metasploitable 2 using Metasploit Framework

- Understanding Metasploit Framework
- Basic Concept and Usability
- Using Metasploit framework to attack Windows machines
- Attacking System using vulnerable open ports.

Class# 11: Understanding Web application Penetration Testing

- Introduction to web application vulnerabilities
- Introduction to OWASP top 10 vulnerabilities
- Details about vulnerabilities

Class# 12: Broken access control/Broken authentication

- What is Broken Access Control/Broken Authentication
- Where and Why it Occurs
- How to Exploit
- What is the Impact of the Vulnerability
- Mitigation process

Class# 13: Cross-site scripting (XSS) and HTML Injection

- Differences between XSS and HTML injection
- Different types of XSS Attacks
- Root cause of these vulnerabilities
- Finding and Exploiting the Injection Points
- Impact of XSS and HTML Injection
- Mitigation process

Class# 14: Cross-site request forgery (CSRF) and Server-side request forgery (SSRF)

- Understanding CSRF and SSRF
- Why and Where these Occurs
- Exploitation of CSRF & SSRF
- Impact of CSRF & SSRF
- Mitigation process

Class# 15: SQL injection – Basic

- What is SQL Injection, Why Occurs
- Types of SQL Injection
- Impact of SQLi, How to Prevent
- Understanding SQL injection
- Identifying Vulnerable Sites
- Finding Suitable Injecting Point

Class# 16: SQL injection – Advanced

- Conduct Regular/ Union Based Injecting
- Xpath sql injection
- Firewall & Firewall Bypassing Techniques
- Disclosing Database, Tables and Columns

- Impact of SQL injection
- Mitigation process

Class# 17: Introduction to webshell, backdoor and shelling techniques

- What is Webshell
- What is Backdoor
- Different types of Shelling Techniques
- Persistence Backdooring

Class# 18: Remote code execution (RCE)

- What is Remote code execution (RCE)
- Why and Where this Occurs
- Finding and Execution Point
- Impact of Remote code execution
- Mitigation process

Class# 19: Insecure direct object reference (IDOR)

- What is Insecure Direct Object Reference (IDOR)
- Why and Where this Occurs
- Finding Exploitation Point
- Impacts of IDOR
- Mitigation process

Class# 20: Network penetration testing

- Introduction to Network Penetration Testing
- Scanning
- Network device testing
- Port Forwarding
- Packet capturing using Wireshark
- Network monitoring and understanding network protocols

Class# 21: Mobile Application Scanning and Penetration Testing

- Understanding Mobile Platform Attack Vector
- Overview of Mobile Penetration Testing
- Static and Dynamic analysis
- Environment setup for android application testing
- Genymotion setup for app testing
- Capturing and finding end points for testing
- API testing techniques
- SSL pinning bypass techniques

Class# 22: Python in Cyber Security

- Introduction to python
- Impact of python in Cyber Security
- Some tools in python
- Developing XSS scanning tools

Class# 23: Security audit, compliances and security hardening

- What is Regulatory Compliance
- Understanding Policy Enforcement
- Understanding Patch Management
- Configuration Management
- Understanding SELinux
- Security standards and guidelines

Class# 24: Ethics and Cyber Law of Bangladesh

- DIGITAL SECURITY ACT, 2018

Class# 25: Final Test