## B.SC. INFORMATION TECHNOLOGY WITH CYBER SECURITY

| Semester | Course Code | Course Category | Hours/ Week | Credits | Marks for Evaluation | | |
|---|---|---|---|---|---|---|---|
| | | | | | CIA | ESE | Total |
| III | 25UICVAC1 | Value Added Course – I | 30 | - | - | 100 | 100 |
| **Course Title** | **Reconnaissance for Web Application Security** | | | | | | |

| SYLLABUS | | |
|---|---|---|
| **Unit** | **Contents** | **Hours** |
| **I** | **Overview of Web Application Security:** Common vulnerabilities and attack vectors. Legal and Ethical Considerations: Responsible disclosure, scope limitations, and non-disclosure agreements. | 6 |
| **II** | **Setting up Tools and Environments:** Introduction to Burp Suite, OWASP ZAP, and Virtual Machines. Hands-on Exercises: Basic reconnaissance techniques, understanding common web vulnerabilities. | 6 |
| **III** | **Understanding the Importance of Reconnaissance:** Gathering information about the target. **Passive Reconnaissance Techniques:** OSINT (Open-Source Intelligence) gathering, footprinting. | 6 |
| **IV** | **Active Reconnaissance Techniques:** Port scanning, service identification, and fingerprinting. **Content Discovery:** Identifying hidden directories, files, and endpoints using tools like DirBuster, DirSearch, and Gobuster. | 6 |
| **V** | **Hands-on Labs:** Performing reconnaissance and content discovery on target web applications. | 6 |

**Text Book(s):**

Flaws Dafydd Stuttard and Marcus Pinto, “The Web Application Hacker’s Handbook: Finding and Exploiting Security”, Wiley Publishing, 2011

**Web Links**

1. https://www.geeksforgeeks.org/reconnaissance-penetration-testing/
2. https://nhattruong.blog/2024/08/12/web-application-reconnaissance-process/

**Course Outcomes**

Upon successful completion of this course, the student will be able to:

| CO No. | CO Statement |
|---|---|
| CO1 | Explain the underlying concepts of web application security |
| CO2 | Make use of the Burp Suite, OWASP ZAP |
| CO3 | Influence the knowledge on the Reconnaissance |
| CO4 | Analyze the various content discovery tools |
| CO5 | Develop a hands on sessions with real world scenarios |

**Course Coordinator:** Mr. P. Mohamed Thahir, Cyberheals Pvt. Ltd.

| Semester | Course Code | Course Category | Hours/ Week | Credits | Marks for Evaluation | | |
|---|---|---|---|---|---|---|---|
| | | | | | CIA | ESE | Total |
| V | 25UICVAC2 | Value Added Course – II | 30 | - | - | 100 | 100 |
| **Course Title** | **Endpoint Security Monitoring** | | | | | | |

| **SYLLABUS** | | |
|---|---|---|
| **Unit** | **Contents** | **Hours** |
| **I** | Endpoint Security Fundamentals - Endpoint Logging and Monitoring - Endpoint Log Analysis - Task Manager - System - System > smss.exe - csrss.exe - wininit.exe - wininit.exe > services.exe - wininit.exe > services.exe > svchost.exe - lsass.exe - winlogon.exe - explorer.exe | 6 |
| **II** | Install the Sysinternals Suite - Using Sysinternals Live - File and Disk Utilities - Networking Utilities - Process Utilities - Security Utilities - System Information - Miscellaneous | 6 |
| **III** | Event Viewer - wevtutil.exe - Get-WinEvent - XPath Queries - Event IDs - Sysmon Overview - Installing and Preparing Sysmon - Cutting out the Noise - Hunting Metasploit - Detecting Mimikatz - Hunting Malware - Hunting Persistence - Detecting Evasion Techniques - Practical Investigations | 6 |
| **IV** | Osquery: Interactive Mode - Schema Documentation - Creating SQL queries - Required: Deploy Wazuh Server - Wazuh Agents - Wazuh Vulnerability Assessment & Security Events - Wazuh Policy Auditing | 6 |
| **V** | Monitoring Logons with Wazuh - Collecting Windows Logs with Wazuh - Collecting Linux Logs with Wazuh - Auditing Commands on Linux with Wazuh - Wazuh API - Generating Reports with Wazuh - Loading Sample Data | 6 |

**Text Book(s):**

Gerardus Blokdyk , Endpoint security A Complete Guide , 2019

**Web Links:**

1. https://www.spiceworks.com/it-security/network-security/articles/what-is-endpoint-security/
2. https://www.trellix.com/security-awareness/endpoint/what-is-endpoint-security/

**Course Outcomes**

Upon successful completion of this course, the student will be able to:

| CO No. | CO Statement |
|---|---|
| CO1 | Explain the underlying concepts of Endpoint Security Fundamentals |
| CO2 | Make use of the Sysinternals Suite |
| CO3 | Influence the knowledge on the event viewer |
| CO4 | Analyze the classification of Osquery |
| CO5 | Develop a hands on session with Wazuh |

**Course Coordinator:** Mr. P. Mohamed Thahir, Cyberheals Pvt. Ltd.