



CODINGJUNCTION
CYBER SECURITY SOLUTIONS

CYBER SECURITY

Coding Junction is a leading Training and Consulting company, offering top-tier solutions in IT infrastructure, security implementation, security audits, vulnerability assessments, and penetration testing.

Coding Junction Focus on Delivering
Best **INDUSTRY CERTIFICATIONS**

EC-Council **CISCO** **CompTIA**

RedHat **python** **PECB**



CERTNEXUS

Beingcert
Learn | CERTIFY | Grow



@CodingJunctionOfficial



BASIC NETWORKING

LEVEL 1

Module 01

Introduction to Networking

Module 02

OSI Model

Module 03

TCP/IP Model

Module 04

Subnetting / Summarisation

Module 05

Packet Flow in Same & Different Network

Module 06

Information About Networking Device

Module 07

IP / ICMP

Module 08

APIPA

Module 09

Address Resolution Protocol

Module 10

Routing Protocols (Static & Dynamic)

Module 11

Static - Next Hop / Exit Interface

Module 12

Dynamic - RIP / EIGRP / OSPF & BGP

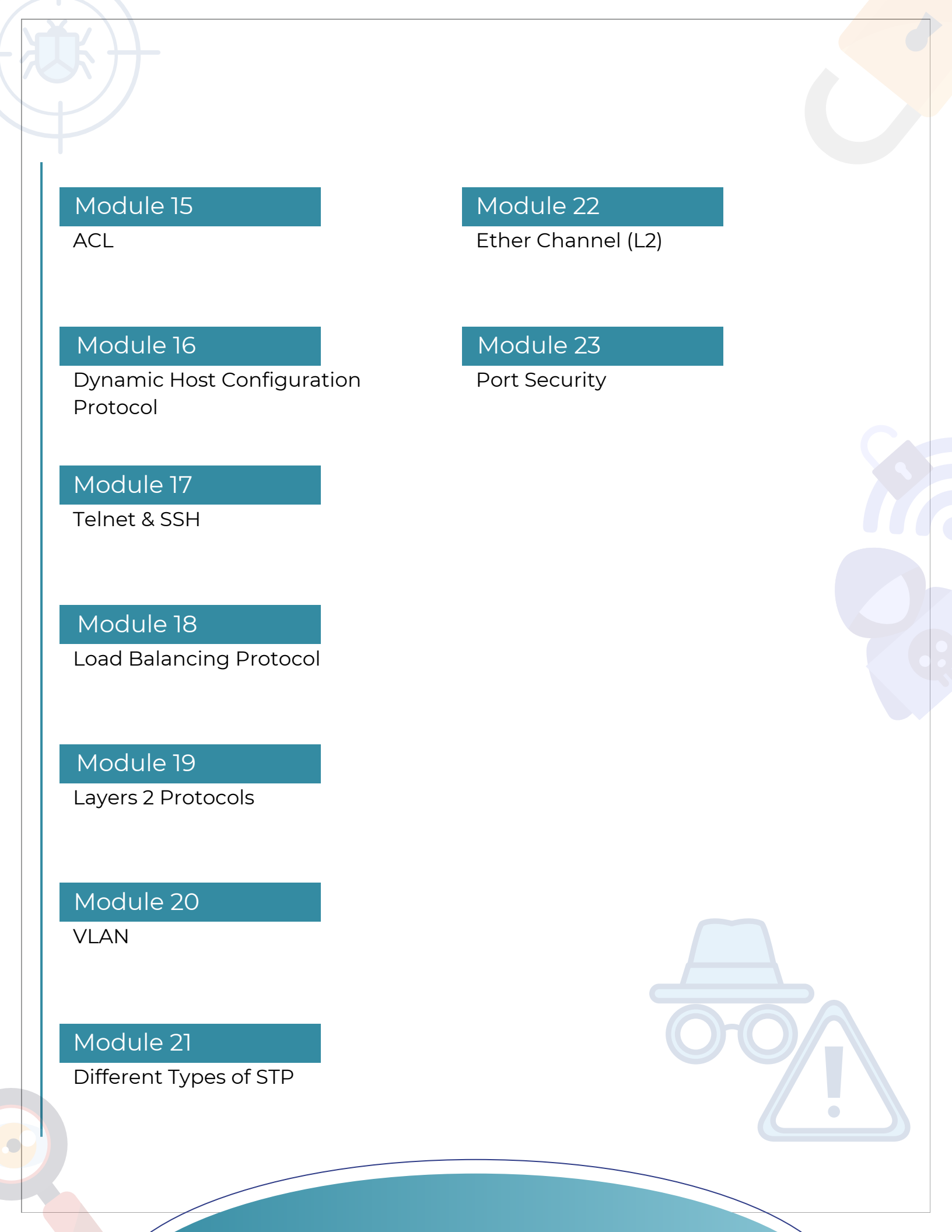
Module 13

Wan Technologies

Module 14

NAT





Module 15

ACL

Module 22

Ether Channel (L2)

Module 16

Dynamic Host Configuration
Protocol

Module 23

Port Security

Module 17

Telnet & SSH

Module 18

Load Balancing Protocol

Module 19

Layers 2 Protocols

Module 20

VLAN

Module 21

Different Types of STP



LINUX ESSENTIALS

LEVEL 2

Module 01

Getting Started with Red Hat Enterprise Linux

Module 02

Accessing the Command Line

Module 03

Managing Files from the command Line

Module 04

Getting Help in Red Hat Enterprise Linux

Module 05

Creating, Viewing & Editing Test Files

Module 06

Managing Local Users and Groups

Module 07

Controlling Access to Files

Module 08

Monitoring and Managing Linux Process

Module 09

Controlling Services and Daemons

Module 10

Configuring and Securing SSH

Module 11

Analyzing and Storing Logs

Module 12

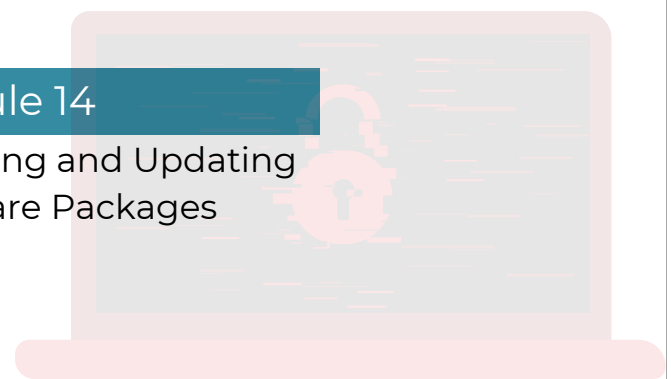
Managing Networking

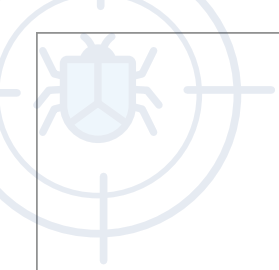
Module 13

Archiving and Transferring Files

Module 14

Installing and Updating Software Packages





Module 15

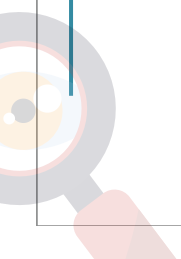
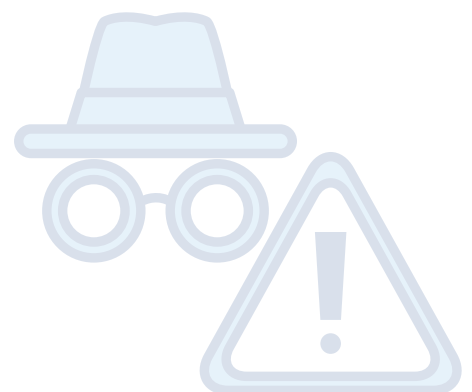
Accessing Linux File System

Module 16

Analyzing Servers and
Getting Support

Module 17

Improving Command-line
Productivity





Ethical Hacking

LEVEL 3

Module 01

Introduction to Basics of Ethical Hacking

Module 02

Foot Printing and Reconnaissance (Active)

Module 03

Foot Printing and Reconnaissance (Passive)

Module 04

In-depth Network Scanning

Module 05

Enumeration

Module 06

Vulnerabilities Assessment

Module 07

System Hacking Password Cracking & Bypassing

Module 08

Malware Threats (Viruses and Worms, Trojan and Back door)

Module 09

Sniffing (Man in the middle Attack)

Module 10

Social Engineering Toolkit Theoretical/Practical Based Approach

Module 11

Denial of Service DOS & DDOS Attacks

Module 12

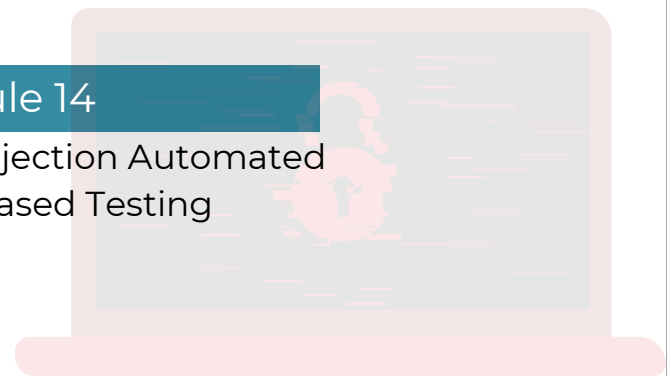
Web Session Hijacking

Module 13

SQL Injection Manual Testing

Module 14

SQL Injection Automated Tool Based Testing





Module 15

Evading IDS, Firewalls, and Honeypots

Module 16

Basics of Web App Security

Module 17

Hacking Web Servers

Module 18

Introduction to Anonymity

Module 19

Hacking Wireless Networks
Manual CLI Based (Wi-Fi)

Module 20

Hacking Mobile Platforms (Android Mobile Hacking)

Module 21

Buffer Overflow

Module 22

Cryptography

Module 23

Internet of Things (IOT)
Hacking

Module 24

Cloud Security and many more



ADVANCE PENETRATION TESTING

LEVEL 4

Module 01

Introduction

Module 02

In-Depth Scanning

Module 03

Exploitation

Module 04

Domain Domination

Module 05

Getting Comfortable with
Kali Linux

Module 06

Command Line Fun

Module 07

Practical Tools

Module 08

Bash Scripting

Module 09

Passive Information
Gathering

Module 10

Active Information Gathering

Module 11

Vulnerability Scanning

Module 12

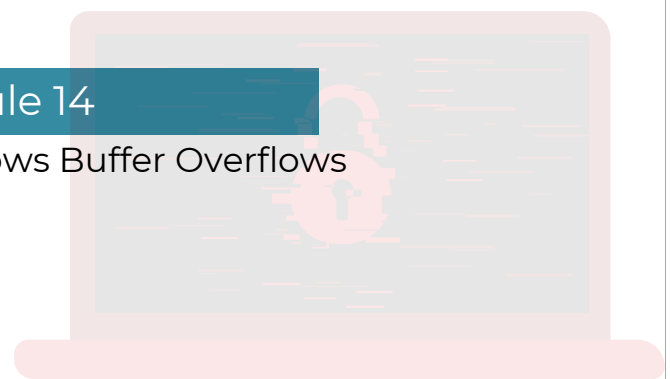
Web Application Attacks

Module 13

Introduction to Buffer
Overflows

Module 14

Windows Buffer Overflows





Module 15

Linux Buffer Overflows

Module 16

Client-Side Attacks

Module 17

Locating Public Exploits

Module 18

Fixing Exploits

Module 19

File Transfers

Module 20

Antivirus Evasion

Module 21

Privilege Escalation

Module 22

Password Attacks

Module 23

Port Redirection and
Tunneling

Module 24

Active Directory Attacks

Module 25

Power Shell Empire

Module 26

Penetration Test Breakdown

Module 27

Trying Harder: The Labs



WEB APPLICATION SECURITY

LEVEL 5 (OWASP TOP 10)

Module 01

Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Module 02

SQL Injection

Module 03

Code Injection

Module 04

Unrestricted Upload of File with Dangerous Type

Module 05

Download of Code Without Integrity Check

Module 06

Inclusion of Functionality from Untrusted Control Sphere

Module 07

Missing Authentication for Critical Function

Module 08

Improper Restriction of Excessive Authentication Attempts

Module 09

Use of Hard-coded Credentials

Module 10

Reliance on Untrusted Inputs in a Security Decision

Module 11

Missing Authorization

Module 12

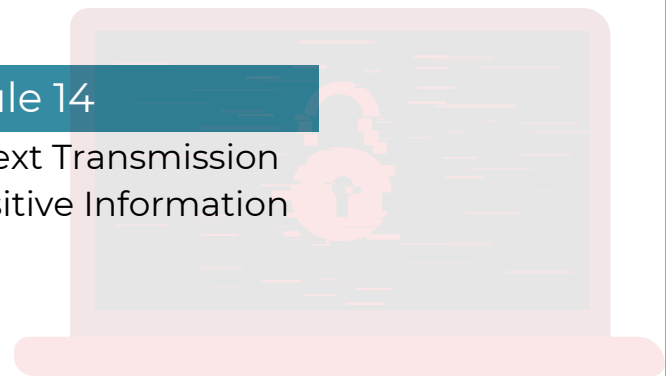
Incorrect Authorization

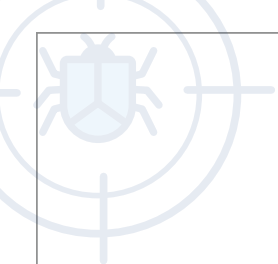
Module 13

Missing Encryption of Sensitive Data

Module 14

Cleartext Transmission of Sensitive Information





Module 15

XML External Entities

Module 16

External Control of File Name or Path

Module 17

Improper Authorization

Module 18

Execution with Unnecessary Privileges

Module 19

Use of Potentially Dangerous Function

Module 20

Incorrect Permission Assignment for Critical Resource

Module 21

Improper Neutralization of Input During web page Generation (Cross-Site Scripting)

Module 22

Use of Externally-Controlled Format String

Module 23

Integer Overflow or Wraparound

Module 24

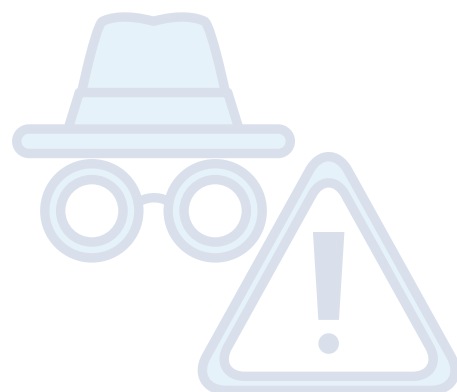
Use of a Broken or Risky Cryptographic Algorithm

Module 25

Use of a One-way Hash Without a Salt

Module 26

Insufficient Logging and Monitoring





END POINT SECURITY

LEVEL 6

Module 01

Implementing Internet
Security Anti Virus

Module 02

Two-Factor Authentication
Implementation

Module 03

Mobile Device Management
For Industry

Module 04

Data Loss Prevention
Overview & Implementation

Module 05

Security Information and
Event Management (SIEM)

Module 06

APT- Attack

Module 07

MITRE Framework

Module 08

EDR

Module 09

MDR

Module 10

Next Generation Firewall

Module 11

Unified Threat Management

Module 12

Physical Security

Module 13

ISO 27001 Lead Auditor
Guidelines





CODINGJUNCTION

CYBER SECURITY SOLUTIONS



Address: Near ICICI Bank ATM, 100 Ft. Crossing
Indrapuram Shamshabad Road, Agra (282001)



Contact Us For More Information :
+91 7078906702, 9761666702



www.codingjunction.in



info@CodingJunction.in



@CodingJunctionOfficial

