// CADRE 1

BLUEGUARDIA

Penetration Testing Training Syllabus

14-Week Practitioner Program · Theory + Hands-On Labs · Job-Ready Outcomes

SECTION 1 — FOUNDATION & THEORY | WEEKS 1 – 4

Week 1 · Basic Knowledge & Organizational Context

- Infrastructure of an organization and roles of different departments
- Role of cybersecurity in an organization
- Information security vs cybersecurity
- Market job trends for cybersecurity
- Security awareness for employees
- Basics of computer hardware & software
- Basics of the Internet (WWW, DNS, HTTP/HTTPS, client-server model)

Week 2 · Cybersecurity Fundamentals

- Different domains of cybersecurity
  - SOC (Security Operations Center)
  - DFIR (Digital Forensics & Incident Response)
  - Penetration Testing
  - GRC (Governance, Risk & Compliance)
- CIA Triad (Confidentiality, Integrity, Availability)
- AAA (Authentication, Authorization, Accounting)
- Types of attackers (insiders, outsiders, hacktivists, etc.)
- Common attacks (brute force, DoS/DDoS, MITM, ransomware, etc.)
- Malware types (virus, worm, trojan, spyware, ransomware)
- Phishing & spear phishing
- Social engineering
- Encryption fundamentals
- Hashing & integrity checks

Week 3 · Operating Systems Fundamentals and LAB Set UP

- Windows & Linux basics
- User accounts, permissions, authentication mechanisms
- Domains vs Workgroups
- File system basics
- Command-line basics (Windows CMD, Linux Shell)

Week 4 · Networking Fundamentals

- IP Addressing (IPv4 & IPv6 basics)
- MAC Address
- Routers & Switches
- VLANs
- Subnets & subnetting
- LAN vs WAN
- TCP/IP model
- OSI model
- Common ports & services
- Protocols (HTTP/S, FTP, DNS, SMTP, SSH, etc.)
- Firewalls
- Proxies
- IDS/IPS basics
- VPNs (concepts & usage)

SECTION 2 — Core Penetration Testing | WEEKS 5 – 12

Introduction to Penetration Testing & Core Concepts & Environment Setup

Penetration Testing Overview

- What is penetration testing?
- Types of penetration testing
- Importance of penetration testing

Career Path & Job Roles

- Junior Pentester – learning, tool-based
- Mid-level Pentester – independent tester
- Senior Pentester / Lead – leads engagements, reviews work
- Principal / Red Team Lead – advanced attacker, adversary simulation
- Manager / Consultant – strategy, leadership, client relations

Day-to-Day Terminologies

- Vulnerability, Exploit, Payload, Shell (reverse/bind)
- Pivoting & Lateral Movement
- Privilege Escalation
- Attack Surface & Zero-Day
- Proof of Concept (PoC), False Positive / False Negative
- Exploit Chain / Kill Chain
- Enumeration & Social Engineering
- Brute Force, DoS / DDoS
- Red Team vs Blue Team vs Purple Team
- Rules of Engagement (RoE) & Scope

Setting Up a Safe Practice Environment

- Installing VirtualBox
- Downloading and installing Kali Linux

Linux Command Line

- Navigating the file system: pwd, ls, cd, mkdir, rm
- Reading files: cat, less, head, tail
- Finding things: find, locate, grep
- Permissions: chmod, chown – who can read, write, or run a file
- Networking commands: ifconfig / ip a, ping, netstat, curl, wget

- Package management: apt update, apt install
- Running scripts and understanding file extensions (.sh, .py)

Lab Activity

- Install VirtualBox and set up Kali Linux VM

OWASP Top 10:2025 & Web Application Attack Theory

OWASP Top 10:2025

- A01:2025 – Broken Access Control
- A02:2025 – Security Misconfiguration
- A03:2025 – Software Supply Chain Failures
- A04:2025 – Cryptographic Failures
- A05:2025 – Injection
- A06:2025 – Insecure Design
- A07:2025 – Authentication Failures
- A08:2025 – Software or Data Integrity Failures
- A09:2025 – Security Logging & Alerting Failures
- A10:2025 – Mishandling of Exceptional Conditions

Web Application Attacks Overview

- Injection Attacks (SQL, Command, LDAP, NoSQL)
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- XML External Entity (XXE)
- Broken Authentication / Session Management
- Broken Access Control & IDOR
- Security Misconfiguration
- Data Exposure / Leaks
- Path Traversal / Directory Traversal
- Clickjacking, SSRF, HTTP Request Smuggling
- DoS / DDoS – including HTTP flood attacks

Penetration Testing Phases & Planning / Reconnaissance

Phases of a Penetration Test

- Phase 1 – Planning and Reconnaissance
- Phase 2 – Scanning and Enumeration
- Phase 3 – Gaining Access
- Phase 4 – Maintaining Access
- Phase 5 – Clearing Tracks
- Phase 6 – Reporting

Passive Reconnaissance

- Google Dorking
- WHOIS Lookup
- DNS Enumeration (dig, nslookup)

Active Reconnaissance

- Nmap Network Scanning
- WhatWeb Technology Fingerprinting
- Nikto Web Server Scanning
- Directory & File Enumeration (Dirb, Gobuster, ffuf)

Reconnaissance Tools

- Whois, Whois.net

- dig, nslookup
- Sublist3r, Amass
- Spider
- OWASP ZAP
- Gobuster, Dirb, Dirsearch, ffuf
- Wappalyzer, WhatWeb
- Nmap
- Google Dorking, Hunter.io
- Maltego,
- Nikto, OpenVAS

Lab Activities

- Identifying Domains, Subdomains & IPs
- Technology Stack Identification
- Web Application Mapping
- Attack Surface Enumeration
- Vulnerability Discovery Preparation

Vulnerability Assessment & Scanning

Scanning Tools

- Nessus
- OWASP ZAP
- Netsparker
- AppScan
- W3af
- Nikto
- WebInspect
- SQLMap
- RIPS

Lab Activities

- Open Port & Service Identification
- Banner Grabbing
- Operating System Detection
- Service Enumeration (SMB, FTP, SNMP, etc.)
- Vulnerability Identification
- Risk Analysis & Severity Assessment

Web Application Vulnerabilities & Exploitation Methods

- XSS (Cross-Site Scripting)
- Host Header Injections
- IDOR (Indirect Object Reference)
- Server-Side Request Forgery (SSRF)
- SQL Injection
- File Upload Vulnerabilities
- Command Injection
- Path Traversal

Web Application Exploitation Tools

- owasp zap

- beff
- tplmap
- jwt tool
- jwt editor
- hydra
- Medusa
- metasploit framework
- turbo intruder
- authorize
- param miner

Post-Exploitation / Maintaining Access

Lab Activities

- Privilege Escalation (Linux & Windows)
- Persistence Mechanisms
- Reverse Shells
- Credential Harvesting & Dumping
- Session Hijacking
- Pivoting to Internal Systems
- Monitoring & Lateral Movement

Reporting & Capstone Review

Reporting Activities

- Documentation of Findings
- Proof of Concept (PoC) Evidence
- Risk Rating & Business Impact Analysis
- Remediation Recommendations
- Executive & Technical Reporting

Capstone Review

- Full penetration test simulation on a lab environment
- Walkthrough of all phases: Recon → Scanning → Exploitation → Post-Exploitation → Report
- Peer review of findings and report quality
- Q&A and course wrap-up

SECTION 3 — JOB-READY PROFILE | WEEKS 13 – 14

Building Your Professional Presence

- Setting up LinkedIn Profile
- Dos and Don'ts
- Preparing a job-ready resume
- Preparation for interviews

BONUS ITEMS

- ★ Collection of questions asked during interviews
- ★ Meet with industry experts with extensive real-world experience
- ★ Live Q&A session with industry experts

TRAIN THE TALENT · BUILD THE FIRM · DEFEND THE INDUSTRY