Syntho Quest

# CERTIFIED PENETRATION TESTING PROFESSIONAL

# COURSE

Prepared By (CTO) SYNTHOQUEST

45 Days Duration

**Duration:** 45 days × 2 hrs/day = 90 hrs

**Goal:** Equip professionals to plan, execute, and report enterprise-level penetration tests across networks, applications, and systems.

**Core Domains**

1. **Penetration Testing Methodology (15%)**
   - PT life cycle: Recon → Scanning → Exploitation → Post-exploitation → Reporting
   - Legal, rules of engagement, and scope definition
   - Risk-based assessment and prioritization
2. **Reconnaissance & Information Gathering (15%)**
   - Passive recon: OSINT, footprinting, WHOIS, Shodan, public records
   - Active recon: ping, port scanning, enumeration
   - Subdomain discovery, DNS enumeration, service versioning
3. **Scanning & Vulnerability Assessment (15%)**
   - Nmap, Masscan, Nessus, OpenVAS, Nikto, Burp Suite
   - Identifying misconfigurations, open ports, outdated services
   - Vulnerability verification & prioritization
4. **Exploitation & Post-Exploitation (20%)**
   - Exploit frameworks: Metasploit, manual exploitation techniques
   - Privilege escalation (Linux & Windows)
   - Lateral movement, pivoting, maintaining access
   - Credential dumping, keylogging, password attacks
5. **Web & Application Penetration Testing (15%)**
   - OWASP Top 10 vulnerabilities
   - SQLi, XSS, CSRF, RCE, file upload flaws
   - Session management, authentication, and authorization bypasses
   - Manual testing & automated tools
6. **Network Penetration Testing (10%)**
   - LAN/WAN penetration techniques
   - Firewall bypass, VPN exploitation, ARP poisoning, MITM
   - Network sniffing and traffic analysis
7. **Reporting & Remediation (10%)**
   - Executive summary, PoC documentation, technical findings
   - Prioritization of vulnerabilities
   - Recommendations, remediation guidance, and retest planning

**Business Associate:** vivek
**Email:** contact@synthoquest.com
**Mobile:** +91-8333801638 (whats app)