Syntho Quest

NETWORK VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Prepared By (CTO) SYNTHOQUEST

45 Days Duration

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

Goal: Teach end-to-end network security testing: discovery → vulnerability scanning → exploitation → post-exploitation → lateral movement → persistence → reporting.

Core topics (focus areas)

- Recon & asset discovery (network mapping, host/port discovery)
- Vulnerability scanning & verification (Nessus, OpenVAS, scanners)
- Service & protocol testing (SMB, RDP, LDAP, DNS, SNMP, FTP, HTTP/S)
- Network exploitation (vuln-to-exploit workflow, Metasploit)
- Password attacks & credential harvesting (kerberoast, hashcat, pass-the-hash)
- Windows domain attacks & Active Directory exploitation (AD abuse, LLMNR/NBT-NS)
- Linux/Unix host exploitation & privilege escalation
- Lateral movement & pivoting (SSH tunneling, proxychains, SMB relay)
- Wireless & VPN testing (WPA2/3, WPA-Enterprise, VPN misconfig)
- Defensive evasion, persistence, cleanup & detection avoidance
- Reporting, remediation planning, and retest verification

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