Syntho Quest

INFRASTRUCTURE VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Prepared By (CTO) SYNTHOQUEST

45 Days Duration

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

Goal: Teach hands-on assessment of physical & virtual infrastructure: network devices, servers, hypervisors, storage, virtualization platforms, ICS/OT basics, cloud infra overlap, secure configuration, exploitation, persistence, and remediation.

Core focus areas

- Network perimeter, segmentation, and edge devices (firewalls, routers, load-balancers)
- Host security (Windows & Linux servers), patching, services, hardening
- Identity & access (AD/LDAP, local accounts, privileged access)
- Virtualization & hypervisor security (VM escape, misconfig, management planes)
- Storage & backup systems (NAS, SAN, backup servers)
- Remote access & VPN gateways, RDP, SSH hardening
- ICS/OT fundamentals and common weak points (if in scope)
- Logging, monitoring, detection, and incident response readiness
- Physical security considerations (where applicable)
- Secure baseline & configuration management (CIS, benchmarks)

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