Syntho Quest

ROUTER VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Prepared By (CTO) SYNTHOQUEST

45 Days Duration

Scope: Routers / home gateways / SOHO & enterprise edge devices (web admin UI, management services, wireless, firmware, routing features, remote management).

Core goal: Discover, exploit, and report vulnerabilities in router firmware, configuration and exposed services; provide prioritized fixes and re-test plan.

Top attack areas (must test)

- Default / weak credentials (admin:admin, telnet/ssh).
- Web admin UI flaws: CSRF, authentication bypass, XSS, command injection, insecure cookies.
- Firmware issues: outdated firmware, unsigned images, backdoors, hardcoded keys.
- Wireless attacks: weak WPA/WPA2 keys, WPS PIN, MIMO misuse, guest/SSID isolation bypass.
- Remote management: TR-069, UPnP, Telnet/SSH/HTTP(S) remote access.
- Services & protocols: SNMP (public/readonly), ftp/tftp, SMB, DNS/DHCP hijack, RCE via exposed services.
- Port forwarding / NAT abuse: open ports, exposed management ports, UPnP granted forwarding.
- Supply chain / 3rd-party modules: embedded SDKs, IoT chips, vendor cloud features.
- Logging & monitoring failures: no alerting for config changes, weak logging, sensitive data in logs.
- Physical & hardware: serial/JTAG access, debug interfaces, removable flash exploitation.

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