



Attack & Penetration Testing

Services Data Sheet

External Penetration Assessment

These assessments will check the possibility of someone (valid or invalid) (trusted or non-trusted) (privileged or unprivileged) situated anywhere on the external network who can gain access by any means (internet leased line, modem, RAS or public net points) to private and presumed secure areas of the < >network.

CyberQ will conduct a security analysis on the devices/ servers configured with public IP Addresses but not limited to the equipments listed

- o Servers
- o Routers
- o Firewall
- o Switches
- o Intrusion Detection Device
- o Intrusion Prevention device
- o Proxy Servers

CyberQ will utilize tools and equipment as deemed necessary to conduct the Penetration testing, which will cover the following areas

- o Port Scanning
- o Services scanning
- o Protocol analysis
- o Vulnerability identifications
- o Operating system loopholes
- o Password guessing & cracking
- o Denial of Service
- o SMTP encapsulation
- o WWW content bypassing
- o MSN & Other Chat services vulnerabilities
- o Buffer overflow

Internal Penetration Assessment

These assessments shall check the possibility of someone (valid or invalid) (trusted or non-trusted) (privileged or unprivileged) connected to the internal network who can gain access to private and presumed secure areas of the < >network.

CyberQ will conduct a security analysis of the following but not limited to the equipments listed

- o Servers
- o Routers
- o Firewall
- o Switches
- o Intrusion Detection Device
- o Intrusion Prevention device
- o Proxy Servers

CyberQ will utilize tools and equipment as deemed necessary to conduct the Penetration testing, which will cover the following areas

- o Port Scanning
- o Services scanning
- o Protocol analysis
- o Vulnerability identifications
- o Operating system vulnerability
- o Database vulnerability
- o Password guessing & cracking
- o Network Sniffing for system traffic vulnerability
- o Denial of Service
- o IP address Spoofing
- o Antivirus vulnerabilities
- o Buffer overflow

Review of Network Security Assessment / Architecture

- CyberQ will conduct a detailed analysis of all the network assets.
- Review of Network Architecture will cover the following :-
 - o Remote and external access methods
 - o Remote administration of critical devices
 - o Network Exposure to unauthorized access from Internet
 - o Confidentiality / Integrity of Incoming / Outgoing data to Intranet / Internet
 - o DOS(Denial of Services) attacks on network resources
- The review report will cover areas like
 - o Design of Secure Network Architecture outlining the perimeter defense, segregation of LAN, WAN, Remote Access Mechanism, NAS and SAN etc
 - o Requirement of appropriate perimeter security solutions like firewall, intrusion detection system, Intrusion Prevention system, antivirus solution etc
 - o Requirement of application security and solutions like Identity Management, Single Signon, Usage of Digital Signatures etc
 - o Recommended security configurations for the existing information systems like operation systems, firewall, applications, routers etc