Network Level Penetration Testing

The iBeta Penetration Testing program utilizes tools that are compatible with and updated from the National Vulnerability Database (NVD, http://nvd.nist.gov/) which in turn supports the identifiers of the Common Vulnerabilities and Exposures (CVE, http://cve.mitre.org/compatible/compatible.html). The tool has scripts to check for over 45,000 vulnerabilities.

Our Penetration Testing scans for such vulnerabilities as

- open ports that may not need to be open
- open ports using outdated and vulnerable protocols that need to be updated
- insecure SSL or TLS
- default passwords on internet facing routers and devices

Vulnerabilities observed are cataloged and reported with their CVSS Base Score and a severity of low, medium, high and critical. Low severity vulnerabilities are reported, vendors should consider fixing medium vulnerabilities based on their own risk analysis, high and critical vulnerabilities should probably be fixed at the earliest convenient time. The technical report containing a vulnerability provides links such as this one to possible solutions.

We provide both an Executive level summary report of our findings, as well as a detailed report that will aid the technologists in fixing any problems found.

iBeta can also provide regularly scheduled scans of your website(s). In those cases, we provide an additional difference report to show the differences found between the last scan and the current scan.