



Penetration Testing Services for a Leading Charity Organization in UK

Client Profile

The client is one of UK's leading charity organizations, working with physically challenged people, by not only helping them with information, support and advice, but also with imaginative and practical solutions to everyday challenges. It encourages patrons to help both in terms of donation as well as volunteering for help with the physically challenged.

Client Context

The client wanted to understand where it stood in terms of 'security' with regard to its IT infrastructure and identify the vulnerabilities that may exist, if any. The stakeholders wanted to ensure that its IT infrastructure had the highest levels of security since the patrons logged into its website to contribute money towards charity. The patrons were entering credit card details and other personal/financial information on its website, which made it imperative that high levels of security were achieved and maintained. Microland proposed a black box penetration testing of its internet facing IT infrastructure, to assess the existing security levels and identify any vulnerabilities.

Microland Approach

Microland conducted a black box penetration testing exercise for the internet facing infrastructure of the customer which includes firewall, IDS, routers, mail systems, customer portal, intranet, etc. Microland simulated hacker action in a controlled environment from its secure lab to check for security vulnerabilities across the entire IP blocks (20+ live IPs).

This exercise was done with Microland methodology which is derived from OSSTMM, NIST, OWASP, WASC and ISSAF. Microland's highly experienced security consultants used tested and safe commercial, open source and in-house tools. Salient features of the tests were:

- Tests were carried out only from Microland Penetration Test SDC with source IP address communicated to customer prior to the commencement of the process

- Tests were done only during the time slots specified by the client (Non-office hours)
- In the event of finding any high/critical level vulnerability, Microland informed the customer immediately

Key Deliverables

Executive report for the management which highlights number of vulnerabilities against each asset/IP address, and the strategic recommendation to remedy the same

Engineering Report including tactical/detail report for the security administrator containing:

- Information gathered about each asset
- Asset location and prioritizing found vulnerabilities
- Details of vulnerabilities exploited per asset
- Possible impacts due to these identified vulnerabilities
- Recommendations to mitigate the vulnerabilities

Benefits

- Better understanding of the IT infrastructure security environment for the customer as a result of identification of vulnerabilities
- Secure environment for the patrons to share financial information. This was due to remedial action suggested by Microland for the vulnerabilities identified during the penetration tests
- Increased control of risks owing to a highly secure IT infrastructure