

Case Study – Midlands Service Provider

Brief

Perform spot analysis of the Service Provider's Internet facing services.

Approach

All testing was done manually except for the use of a brute force tool where appropriate. We approached this network in a passive manner simply probing for vulnerabilities.

Outcome

Although the web site had no dynamic content it was found to have multiple vulnerabilities. These uncommon vulnerabilities were found in the way of inappropriate links to internal network services. From the web site we were able to locate the network gateway login and administration functions. Weak and similar passwords allowed us to brute force access to this service in less than 5 minutes. Having gained access to the server we would have been able to add ourselves to a VPN login and once completed gain access to all network services. Furthermore we were able, through analysis of email headers, to track IP paths directly back to the exchange server itself. Knowing that the respond to email would be the same as the log in for the exchange server we were one step away from brute forcing access to the OWA service.

Once the public gateway IP address was located it was quickly determined that the network was running only a software firewall which was set to allow nearly all traffic through all ports.

Solutions

Inappropriate links were removed from the site; SMTP banners were modified to hide paths to network services. External administration disabled on the gateway. IP Sec policy introduced to prevent access to network services from outside of the WAN. Ongoing security policy development consultancy and ICT staff training undertaken.

