

Days in the life of a pen-tester

by David Beesley Technical Services Director – Network Defence



Foreign hackers, weak passwords, backdoors and buffer overflows - just another day at the office for Network Defence's penetration testers. Here's a look at sample pages from the head tester's diary– and what companies can learn from the results.

Monday 2nd

We tested the website of a manufacturing company, and amazingly found the web server was installed on the company's internal network. Our tests revealed that the firewall rule was to permit ANY inbound traffic to connect to this server. Exposure of the Microsoft directory services ports to the Internet allowed us to connect to this server, from there a weak password gave us access to a domain administrator account. A couple of errors has led to the potential for a hacker to control the network.

The lesson here is to check your firewall rulesets carefully and regularly. One mistake could allow an attacker in.

Wednesday 11th

At a financial services company today. The company's website was hit by the widespread Sasser worm earlier in 2004, which causes buffer overruns and shuts down unpatched machines running Windows XP and 2000. It can also enable attackers to upload code, or modify data. Of course, Sasser was

widely known, so most companies have updated anti-virus software and have patched their systems – which is why we are doing a pen test.

We identified some points on the network that had not been patched. This is potentially serious for a financial services company, as vulnerabilities could be exploited to obtain user IDs, passwords and personal information. The moral is: keep your AV software up-to-date and keep abreast of the latest patches as they become available.

Thursday 19th

We moved onto a major chain of car dealers today. One of its IIS 5.0 servers had been hacked by a foreign spamming group, with the intention of using the server as a spam "proxy", concealing the original spammers. This demanded quick action – pulling the server from the Internet so the rogue code could be identified and removed, and new firewalling software loaded onto the machine.

Friday 27th

Testing the websites of a large property management company. This customer is one of our regulars, for which we conduct regular pen tests. On the sites tested regularly, we did not find anything apart from a couple of low-risk vulnerabilities that had appeared since the previous test.

However, this week we tested one of its newly-developed e-commerce websites and found it to be susceptible to multiple SQL insertion attacks which would have allowed us to take almost full control of their system. Yet again we were straight on to the telephone explaining the issue and giving guidance for remedial action.

Tuesday 7th

We're doing an external penetration test for a social housing company. We discover that the firewall permits remote administration, and that the administrator account was still using the default password.

This caused some red faces in the company's IT department - the default password had been left on by the firewall installer who had told the IT manager to change it; of course this had never happened. It also highlights just how frequently weak passwords crop up. We always recommend that passwords should include a mix of letters and numbers, upper and lower case and should be as random as possible. Also, firewall external administrator access should be switched off – security is more important than convenience in this case.

Tuesday 14th

Our test at a further education college revealed the mail server to be an open mail relay. This is an obvious target for spammers, who will use the relay to send thousands of email messages worldwide. As well as being a serious nuisance for the recipient, the college bandwidth would be compromised and the college would get its email domain blacklisted. It's easy to test mail setups for open relays – so do it before someone else does!

Thursday 23rd

A test of a company's web server revealed that the intervening firewall was well set up and the server was patched up-to-date. So far, so good. However we could gain access to the password-protected part of the site using a SQL injection trick; this allowed us to log in without knowing either username or password. The ASP code did not provide sufficient input validation on the forms.

You should always check your application coding, because even a well configured firewall and a patched server can still be compromised.