

Lessons learned from ethical hacking

By Robert McAdam,
founder of Pure Hacking

Many organisations have their digital networks attacked on a daily basis. Some of these attacks bring into question the viability of an organisation's information technology practices, if not the company's data security as a whole.

So what lessons can we learn from these attacks? Pure Hacking has been conducting penetration testing – or ethical hacking – on IT communications infrastructure since 2002 to locate system vulnerabilities and assess the best solution to fix the problem.

Over the past five years a number of themes have emerged. The most attacks were low risk with only a very small percentage with extreme vulnerability. The most common issue which caused the vulnerability was configuration.

Risks

We simulate what hackers would do when trying to take over a server or network. We detail the holes in the company's existing security measures and provide steps they can take to protect their data better.

Our tests concentrate on external and internal infrastructure, web applications, wireless, VoIP and various other systems that are necessary to an organisation's information technology structure.

During our tests we isolated these risk categories:

- Low – The information gleaned from the vulnerabilities will not allow an attacker to gain direct access to systems or data but may be used to escalate a separate vulnerability;



Robert McAdam

Problem solving

After assessing the risk we work out how to solve the problem through a number of options:

- Configuration – i.e. if you applied this parameter or took this parameter off the system would function effectively;
- Best Practice – i.e. backup system;
- Education – ensuring your population is aware of the risks so they don't fall for tricks;
- Software Update – i.e. apply patch updates;
- Tools – using a product to solve the problem, i.e. buying a valid SSL certificate.

Our findings

By analysing our data from the past five years of testing, we were able to get to the root of the problem and establish how these solu-

best practice and education were the best solution for one case each, configuration accounted for 11 and a software update fixed the problem three times. Tools were not used in these cases.

Looking at the 'High' vulnerability results, best practice solved one problem, education four and configuration was the best solution in 43 cases. Software updates and tools were not needed for these results.

Results

Our penetration test results can be interpreted a number of ways, with the following reasons:

- Pure Hacking is biased and looks for configuration issues;
- IT companies have developed solutions to solve these problems but clients don't know how to access them;

● **Low** – The information gleaned from the vulnerabilities will not allow an attacker to gain direct access to systems or data but may be used to escalate a separate vulnerability;

● **Medium** – A vulnerability that by itself will not allow unauthorised access to systems or data, however, two or more medium-rated vulnerabilities used in conjunction may allow an attacker unauthorised access;

● **High** – A medium to high level of technical knowledge is required for an attacker to gain unauthorised access to a system or data from a single vulnerability. The attacker or user can harm the professional image of a corporation;

● **Extreme** – Little or no technical knowledge is required for an attacker to gain unauthorised access to a system or data from a single vulnerability;

● **Unknown** – Software or system is vulnerable, but the team were unable to complete testing.

Our findings

By analysing our data from the past five years of testing, we were able to get to the root of the problem and establish how these solutions worked for different clients.

Best practice resolves the vulnerability in five per cent of cases; configuration accounts for 89 per cent, education three per cent, software updates work for one per cent of cases and tools are used to solve two per cent of the penetration issues we assess.

Our results also showed most of the penetration tests we carried out had a low vulnerability (52 per cent), followed by 35 per cent with medium vulnerability, high in 10 per cent of cases and extreme vulnerability for three per cent.

How do you fix these issues?

If we look closer at the more serious vulnerability results, we can see how the solutions measure up. In our 'Extreme' assessments,

● Pure Hacking is biased and looks for configuration issues;

● IT companies have developed solutions to solve these problems but clients don't know how to access them;

● Companies say they "didn't realise the significance of the problem";

● Clients know how to solve their vulnerability problems but don't have the resources (i.e. time or money).

From these reasons it is fair to ask the question, 'Is the penetration problem ignorance or time management when it can be solved with known business solutions?'

If I were going to secure my IT systems, I would start by looking at what the configuration should be. From there, I would find the gap and then action that gap. The results are self explanatory: if you're going to get a 9:1 ratio return by working on the configuration, that may be a good starting point, especially if you have limited resources. ■