



## Hacking by invitation (Mar 2007)

As the world becomes more accepting yet susceptible to digital networks, extraordinary steps must be taken to ensure confidence in systems that could be the backbone of international commerce.

That is why organizations pay Pure Hacking (<http://www.purehacking.com/>) to perform cyber sabotage on their infrastructure. Many know first hand that an act of sabotage can bring into question the viability of an organization's information technology practices, if not the company's data security as a whole.

Pure Hacking is contracted to fully scrutinize the sanctity of the IT communications infrastructure. They do what is known as ethical hacking or penetration testing where they simulate what hackers do when trying to take over a server or network.

The Pure Hacking team details the holes in the company's existing security measures and provide steps they can take to protect their data better. They work with companies both large and small, predominantly in data intensive industries including finance, business services, communications, education and health.

Pure Hacking CEO Robert McAdam believes that ensuring the security of the infrastructure from internal and external threats is vital to business continuity. Often IT security policies demand an independent penetration test as sound business practice.

"Pure Hacking is a dedicated penetration testing firm," says McAdam. "We will identify the risks to our client's business, establish the appropriate measures to minimize the exposure to hacking and continue to monitor the state of their security."

### The testing steps

In determining whether a network or server is vulnerable to attack, the hacking team would first "footprint" a target to acquire all pertinent information towards launching a surgical cyber strike. The next step would be to scan the various listening services on a network to seek out any promising vulnerabilities.

With this data in hand, the more intrusive probing begins, as the testers identify poorly protected resources and gain access into the system.

Once in, they attempt to escalate their IT privileges to obtain complete control over the network. It is at this critical stage that all resources, data and information within the company are vulnerable to theft, corruption or erasure, which would of course be costly to organizations in terms of downed systems, missing data and lost productivity. Not to mention potential lawsuits from irate shareholders and angry clients.

"The security team has all the tools, techniques and know-how to stay ahead of the criminal hacking community," says McAdam.

"Clients cite our expertise, reliability and the excellence of our recommendations as qualities that set us apart in the IT security market."

### Common issues

It is keeping up with progress in the IT world that some companies may have trouble with. Once an application or system is online, there may be various patches or exploits that companies usually miss, giving hackers a small but critical window of opportunity.

What's more, with the wealth of intrusion tools freely available on the Internet, anyone with little or no skill can attempt to take over a corporate network.

These "script kiddies" usually lack the knowledge and finesse to steal highly sensitive data, but their attempts on the system can cause some collateral damage.

"Another major issue is that organizations secure the perimeter, but fail to look within the business. We have found that often the internally exploited risks have the biggest impacts," said McAdam.

Most employees have access to the organizations' IT systems and as a result electronic threat is very possible, as is the danger of corporate secrets being sold to competitors. Organizations need to be very careful about who has access to the systems and consider information as a policy issue.

### Ongoing management

Apart from the regular penetration testing and security audit, Pure Hacking also offers ongoing security management to ensure that any new company changes to the system do not introduce new vulnerabilities.

Pure Hacking checks their client's infrastructure every business day to see if there are any intrusion issues. Perhaps most importantly, its reports with its specific tests, results and recommendations can be actionable for all levels of staff as IT security should be a company-wide effort.

In addition to testing work on corporate firewalls and security protections for onsite servers and applications, they now also test the vulnerabilities of RFID systems and are performing security audits for companies deploying RFID technology.