

Infrastructure Testing:

Public Infrastructure

Your public infrastructure is that visible to the general internet. Typically this will include your firewall, upstream router, DMZ and any other devices with an internet-routable public IP address.

These are generally considered to be the most at risk from hacker attack and worm infection, as it is near impossible to restrict access to the hacker, and grant access to the genuine prospective customer using your services.

In general, the more functional a particular server or device, the more likely it is to be attacked. As functionality increases, the opportunity for mis-configuration and vulnerability increases. Hence a web site running a complex transactional web application is far more likely to be successfully hacked than your upstream router. That said, a DOS attack against said router could knock out your internet access, unless you have systems to fail over to.

The core of any penetration test should include your public infrastructure, but don't forget that there are other routes into your network. Many make the mistake of testing just the firewall and DMZ, believing that this offers total security assurance. Don't fall into this trap.

LAN/WAN Testing

Your LAN is that which cannot be routed directly from the internet. Your firewall offers a degree of protection from the casual hacker, but what about other threats?

- The rogue/bogus/disgruntled/inquisitive employee
- The social engineer
- The internet worm
- The Trojan Horse
- and many others

All of the above offer routes into your network, any of which could be used to gain access to sensitive information, or bring down the LAN. The rewards for the hacker are significant, for example in the case of Sumitomo Mitsui, the attacker nearly got away with £220M.

The term 'inside job' is just as relevant to hacking as it is to physical theft!

We test the security of your network at various levels looking for weaknesses in the infrastructure and applications, issues with content and mail filtering, problems with physical and technical security

Infrastructure Testing:

Voice & Video Over IP

VoIP is a particular area of interest for us. We've conducted extensive research into a number of vendors technologies on behalf of clients.

The convergence of the voice and data LAN brings cost savings, but opens up a set of vulnerabilities to anyone who understands IP, rather than the complexities of analogue voice networks.

Many manufacturers have taken the opportunity to embed web servers in the phone handsets themselves, leading to vulnerabilities seen many years ago in conventional web servers. Common issues include poor packet validation leading to DOS attacks against phone switch and handset. Others manufacturers fail to encrypt the traffic, so with a simple packet sniffer one can listen to any phone call on the network.

One of the most depressing solutions to the security issues above came from a manufacturer who suggested segregating the voice and data networks. Wasn't that the point of VoIP in the first place?

Infrastructure Testing:

Mainframe Testing

RS/6000

The RS/6000 (IBM System p5) is a sturdy server platform with many commercial implementations. The most current and widely used RS/6000 Operating systems are AIX 5L, Linux on System p5™, AIX 5L and Linux on POWER community, and AIX Collaboration Center. AIX (Advanced Interactive eXecutive) itself is essentially a hybrid Unix/IBM operating system so it shares many Unix features. Fingerprinting and enumeration are the bread and butter of an attack (identifying operating systems, architecture and topologies) and it is a practice that is heavily reliant on gaining access at server level.

To minimize the risk from such an attack the RS/6000 should be hardened. Because AIX and the RS/6000 are such a good partnership AIX is a very popular server implementation. And because AIX is Unix based securing it and maintaining its integrity is relatively straightforward. Due to advances in server technology on other platforms the RS/6000 is gradually becoming a legacy implementation. This is not a slur against owners and users of the RS/6000, in fact it is the one main reason why there are less vulnerability, less exploits and less attacks.

AS/400

The AS/400 (IBM iSeries and System i5) is powerful and flexible. Its OS/400 operating system can be configured to run i5/OS, Linux, Microsoft Windows Server, AIX 5L, and enable application environments such as WebSphere and Java concurrently. It was created so that platforms could be consolidated and reduce the requirement for large server farms. Even though the AS/400 allows companies to reduce the total number of servers required the security risk is dramatically increased due to the number of services it provides. A single OS system only has vulnerabilities related to that OS. If you multiply the number of OS's you also multiply the number of vulnerabilities.

Similarly, if just one OS, say Microsoft Windows Server, is compromised on an AS/400 there is real potential for all the other OS's to be compromised in turn. It is a similar concept to a single server running multiple services such as DNS, webserver and database. If one of these services is vulnerable and compromised it is likely that all other services will be compromised too. AS/400's are widely used and they have enjoyed new incarnations. But if they are not reconfigured from default they present a considerable corporate risk. To further complicate matters they are highly specialist systems that are difficult to understand and configure securely. Many are being used in legacy environments and therefore often overlooked in any security auditing activities.