

## Network Vulnerability Assessment, The Importance of an Independent Assessment

---

Background .....	1
What are the key threats?.....	3
What Vulnerabilities does an NVA identify?.....	4
When should you perform an NVA?.....	4
How will an NVA help improve your network and organisational security?.....	5
Why Activity? .....	6
More Information .....	6

### **Background**

From a network security perspective, the focus of the threat to organisational security is changing. With the implementation of strong perimeter defence solutions such as firewalls and content filtering, increasingly more breaches are occurring from within.

Many companies are finding that their internal security is being increasingly compromised by the numerous and rapidly growing number of simple methods that enable legitimate users to create a back door into the company network. These simple methods, which can effortlessly circumvent all of the existing gateway security products, pose as great a threat as attacks from outside the corporate network. The Gartner Group recently estimated that more than 80 percent of breaches to a company's security information originate from within the company. The potential damage from such threats varies from the loss of sensitive information to complete network shutdown.

Modern operating systems have increasingly less vulnerabilities present today than they have had in the past few years, however as the pool of easily exploitable Microsoft Windows bugs dries up the number of exploited and exploitable vulnerabilities present in application and server software has exponentially increased. In 2006 the 'Big Yellow' worm actively exploited a vulnerability within the Symantec anti-virus software suite of applications.

There has also been significant growth in the number of client-side vulnerabilities, including vulnerabilities in browsers, office software, media players and in other desktop applications. These vulnerabilities are being discovered on multiple operating systems and are being massively exploited in the wild, often to drive recruitment for bot nets or as a way into the corporate infrastructure.

Although they contain fewer vulnerabilities, the default configurations for many operating systems and services continue to be insecure, such as not mandating default password

changes during installation. As a result, the internal user can compromise many systems simply by knowing the default password for an application.

A number of factors have converged in the marketplace to make internal network security assessments a necessity, including the evolution in corporate information technology focusing on ease of use at the operational end, while exponentially increasing the complexity of the network assets. At the same time the skill level required to discover, execute and exploit network vulnerabilities has steadily decreased; the number of network and web-based applications has increased and the detrimental impact of a security breach on corporate assets and an organisations reputation is greater than ever.

Issues such as un-patched internal servers, default passwords and insecure configurations, will not be identified by an external "Internet" penetration test as these systems are safely hidden behind corporate firewalls. It is only through performing an assessment from the same location on the corporate network as an internal user, that vulnerabilities can be revealed and understood.

Security breaches and successful attacks executed by malicious attackers have recently been a favourite media topic. The smallest of breaches, that historically may well have gone unnoticed by the wider public, are now often widely publicised, greatly increasing the risk to an organisations reputation caused by a security breach.

Commonly the biggest news items are related to identify theft facilitated via compromised personal data, financial fraud using stolen credit card data and data breaches that result in the disclosure of sensitive, embarrassing and proprietary data.

UK Government, in direct response to the recent spate of publicised security breaches and the resultant mood of distrust from the public towards the storage and processing of their data, has initiated the process of revising the Data Protection Act. The proposed changes include legislation to increase the accountability of organisations and individuals; as well as the introduction of a criminal offence in the case of demonstrable neglect towards information security or repeated data breaches.

In addition, regulatory bodies such as the Information Commissioner's Office and the Financial Services Authority (FSA) are calling for UK and EU legislation to require the public disclosure of significant security breaches that result in the loss of personal information and data.

There are also now a wide range of potential groups of attackers, with differing motivations, ranging from individuals looking simply to compromise systems driven by a passion of technology and a 'hacker' mentality, focused criminal organisations seeking potential targets for financial proliferation, political activists motivated by personal or group beliefs, to disgruntled employees and system administrators abusing their privileges and opportunities for a variety of goals.

A Network Vulnerability Assessment can enable organisations to effectively counter these threats through a validation of their enterprise security strategy, by measuring the strength

and effectiveness of the security technologies and policies adopted to protect the network and the network-accessible resources.

Through understanding the threats and performing a programme of assessment of network level vulnerabilities, an organisation can provide evidence to regulators, customers and partners that they are effectively managing the risk that their corporate applications, services and interconnected systems pose.

It is paramount for an organisation to consistently and proactively track and fix vulnerabilities in their network. When most networks are attacked, weaknesses were exploited when patches were already available or obvious mis-configurations went unnoticed. With the right kind of vulnerability management solution and processes in place, weaknesses in a network can be found, brought to attention and shored up.

The remainder of this paper sets out the key threats that your network(s) face, together with their impact on your organisation. The paper then details how you can address these threats with an independent Network Vulnerability Assessment (NVA).

## ***What are the key threats?***

Corporate networks and their services are typically exposed to six generic security threats:

- **Loss or Modification of Data** resulting in the modification or destruction of sensitive customer or organisational data.
- **Disclosure of Sensitive Data** or corporate information to the general public or competitors.
- **Compromise of Interconnected Systems** resulting from exploitation of a trusted path through an insecure application or network resource, resulting in the compromise of partner systems and their data; in turn leading to a loss of organisational reputation and customer confidence.
- **Propagation of Malware** use of affected systems as “bots” (infected machines under the control of persons other than the intended users, used as proxies for attacks on other systems or for storage and distribution of pirated content and pornography).
- **Virus Infection** of client desktops or critical business systems that can cause system outage or modification, destruction or the disclosure of data.
- **Denial of Service** resulting in the unavailability of network and application resources, potentially leading to the loss of revenue.

Successful exploitation of any of these threats could lead to:

- Loss of organisational reputation and customer confidence.

- Modification, leakage or destruction of your sensitive customer or organisational data.
- Loss of service through the unavailability of application and network resources.
- Fines from the Information Commissioner's Office or other regulatory bodies.
- Loss of revenue.

## ***What Vulnerabilities does an NVA identify?***

These key threats are most often realised through the following vulnerabilities within the internal organisational network:

- Default installations of applications and operating systems.
- Missing security patches and service packs.
- Poor internal network design and implementation.
- Default usernames and passwords for privileged access to infrastructure and servers.
- Default services and ports left open and unmanaged.
- Excessive privileges assigned unnecessarily to users within an unrestricted computing environment.
- Poor configuration control procedures.
- Poor or non-existent internal monitoring and auditing policy.

## ***When should you perform an NVA?***

New vulnerabilities with operating systems, applications and network infrastructure appear on a daily basis. Keeping systems patched and configured in line with best practice is often a major challenge for organisations, especially when developers and network administrators are under pressure to make systems work within tight timescales. This can often result in the situation where the task of securing these systems takes a secondary role.

It is therefore critical to perform an assessment of corporate networks and their services both prior to their initial roll out and on a regular basis to ensure that any and all specific security threats are understood, managed and remediated.

A NVA is best utilised as a component within a corporate risk assessment process where it can be used to assist in validating corporate security policies and strategies.

When considering whether to perform a NVA the questions you should ask are:

- Do the networked systems store and process personal information that is covered by the Data Protection Act?
- Do the networked systems store and process financial information?
- Do the networked systems store and process sensitive corporate information?
- Do the networked systems provide connectivity to other systems within your organisation?
- Do the networked systems provide connectivity to other applications or systems outside your organisation?
- Does a third party provider manage the network, its systems or application services?
- Did a third party design and implement the network architecture?
- Is the network architecture and its resources bespoke to your organisation, developed for a specific purpose?
- Is there a suspicion that systems have been compromised?
- Do firewalls indicate an unusually high level of activity?
- Are IDS systems generating alerts on outbound traffic?

If the answer to any of these questions is yes then you should strongly consider an NVA.

## ***How will an NVA help improve your network and organisational security?***

Specifically a Network Vulnerability Assessment will help an organisation:

- Validate the effectiveness of both preventative and detective technical security controls within a network or system.
- Ensure that patching and configuration management practices are followed correctly.
- Understand and identify potential breach points.
- Benchmark security posture.
- Provide input into the organisational security risk assessment process on the key threats and vulnerabilities within a system.
- Reduce security risk and liability and help to shape information security strategy.

- Protect intellectual property and prevent financial loss ensuing from a real and successful attack.
- Aid in protecting brand identity by avoiding loss of consumer confidence and business reputation.
- Demonstrate compliance and conformity with Industry, Government and regulatory security standards.

## **Why Activity?**

- Activity uses proven and repeatable methodologies that build on recognised Industry Standard approaches such as CHECK, Council of Registered Ethical Security Testers (CREST), Open Source Security Testing Methodology (OSSTM) and Open web Application Security Project (OWASP).
- Activity is a CREST member company and as such assessment methodologies and processes have been assessed independently to ensure that they provide the required level of quality and skills in the provision of security testing services.
- Activity consultants have an average of over 5 years security testing and consultancy experience in providing security services to HMG and private sector clients.
- We have a wide range of experience in testing applications of all sizes and shapes, from e-commerce applications to collaborative working applications, document management systems and enterprise CRM systems.
- Activity's internal processes and systems have been certified to ISO 9001 for Quality and ISO 27001 for security, providing confidence to clients that Activity provide a consistent and quality focused service to clients.

## **More Information**

For more information contact:

Activity  
25 Hercules Way  
Aeropark, Farnborough  
Hampshire  
GU14 6UU

Tel 01252 377321  
Fax 01252 377670  
Email [info@activityim.com](mailto:info@activityim.com)  
Web [www.activityim.com](http://www.activityim.com)