



SAPPHIRE

Vulnerability Assessment – Best Practice Summary

The contents of this document are commercial in confidence.

Reproduction of this document in whole or part in any electronic or paper form is not permitted.

Best Practice Summary

Prepared By:

Dave Sexton

Sapphire Technologies Ltd.

Globe House

Station Street

Stockton on Tees

Cleveland, TS20 2AB

Date: June 08



Vulnerability Assessment – Best Practice Summary

1	INTRODUCTION	3
1.1	SCOPE AND OBJECTIVES	3
1.2	APPROACH.....	3
2	INTRODUCTION TO NETWORK VULNERABILITY DETECTION.....	4
2.1	VULNERABILITY DETECTION - WHAT IS IT?	4
2.2	VULNERABILITY DETECTION IN CONTEXT	4
2.3	THREATS	4
2.3.1	<i>Unauthorised Access, Disclosure and Modification</i>	<i>4</i>
2.3.2	<i>Denial of Service</i>	<i>5</i>
2.3.3	<i>Weak Security Management</i>	<i>5</i>
2.4	THE SCOPE	5
2.5	INDUSTRY TRENDS	6
2.5.1	<i>IT Security Awareness and Drivers.....</i>	<i>6</i>
2.5.2	<i>The Need For Vulnerability Detection</i>	<i>7</i>
3	THE CHECK SCHEME	8
3.1	WHAT IS CHECK?	8
3.2	WHY YOU NEED A CHECK SERVICE PROVIDER	8
3.3	CONFIRMING CHECK MEMBERSHIP.....	8
4	VULNERABILITY DETECTION APPROACH	9
4.1	INTRODUCTION.....	9
4.2	VULNERABILITY DETECTION SERVICES.....	9
4.2.1	<i>Introduction.....</i>	<i>9</i>
4.2.2	<i>Basic Services.....</i>	<i>9</i>
4.2.3	<i>Advanced Services.....</i>	<i>9</i>
5	GENERAL WORKING PRACTICES	11
5.1	INTRODUCTION.....	11
5.1.1	<i>Tools Used</i>	<i>11</i>
5.1.2	<i>Project Completion</i>	<i>11</i>
5.2	SECURITY PROCEDURES	11
5.2.1	<i>Staff Clearances.....</i>	<i>11</i>
6	EXTERNAL (PERIMETER) TESTING SERVICES.....	12
6.1	INTRODUCTION.....	12
6.2	PERIMETER CHECKING	12
6.2.1	<i>Internet Vulnerability Scanning</i>	<i>12</i>
6.2.2	<i>Perimeter Network Testing.....</i>	<i>12</i>
6.2.3	<i>E-mail Testing</i>	<i>12</i>
6.2.4	<i>Firewall System Checking.....</i>	<i>13</i>
6.3	SYSTEM ACCESS VIA MODEMS.....	13
6.4	TELEPHONE SCANNING	13
7	INTERNAL TESTING SERVICES.....	14
7.1	INTRODUCTION.....	14
7.2	NETWORK LEVEL TESTING.....	14
7.3	COMPUTER LEVEL TESTING	15
7.4	USER LEVEL TESTING	15
8	CONTACT INFORMATION.....	16



1 INTRODUCTION

1.1 Scope and Objectives

This document provides an overview of the best practices and methods used in performing the Network Vulnerability Detection and Assessment (NVD) of customer's systems. It identifies the range of NVD modules that are usually offered and the methods and practices common to many types of NVD services.

The terms Vulnerability Detection and Penetration Testing are used synonymously within this document to refer only to Network Vulnerability Detection of electronic information processing systems. The term Vulnerability Detection in its widest context covers the identification of the vulnerabilities of some target through a variety of physical, personnel, and electronic means and actions.

It is recommended that this document should not be distributed outside the IT security department, but used as a reference and checklist of the common services available, by IT security staff only.

1.2 Approach

First a brief definition of Vulnerability Detection and a description of the current demand for these types of services. This is followed by the different type and levels of service that a client should expect, and an introduction to the CHECK Scheme.



2 INTRODUCTION TO NETWORK VULNERABILITY DETECTION

2.1 Vulnerability Detection - What is it?

Vulnerability Detection is the security assessment of an information processing system through the use of scanning and probing tools and techniques.

Vulnerability Detection combines professional IT expertise and discipline with the repertoire of the computer system probing and scanning techniques to provide customers with an analysis of their systems vulnerabilities to external and internal attack.

The testing will identify the system architecture by means of standard foot-printing techniques, which will gradually increase the level of penetration from outside the organisation with the ultimate aim of identifying sufficient information to expose the organisation to attack.

2.2 Vulnerability Detection in Context

System Security Analysis and Risk Assessment covers the following, usually iterative, stages:

- *Threat Assessment.* The identification of the various information security threats to a system and the information it holds. Usually this includes an evaluation of the business sensitivity or criticality of the system resources.
- *Vulnerability Analysis.* The discovery of the security vulnerabilities within a system which would allow the identified threats to occur.
- *Risk Assessment.* Objective and subjective assessment of the probability that the identified vulnerabilities would be exploited, leading to agreement as to which vulnerabilities are unacceptable. The evaluation of the risk takes into account the business sensitivity of the threatened system resources and the implications of BS7799 and other appropriate standards.
- *Countermeasure Deployment.* The identification, selection, recommendation (and deployment) of countermeasures to reduce the risks to acceptable levels.

Vulnerability Detection offers one of the most aggressive and effective vulnerability analysis methods. However, It should always be used within a wider system security analysis and management process. As will come apparent from the descriptions of NVD below, it does not cover all of the areas of system vulnerability; thus Vulnerability Detection needs to work closely with other security vulnerability methods.

2.3 Threats

2.3.1 Unauthorised Access, Disclosure and Modification

The primary threat is that of unauthorised system access and use (often referred to as hacking). Unauthorised system access opens up the potential for unauthorised disclosure and modification of the system's resources. Clients may also be familiar with the phrases 'Confidentiality', 'Integrity' and 'Availability', often now also referred to as 'Secrecy' and 'Privacy'.



2.3.2 Denial of Service

To a similar extent, Vulnerability Detection covers denial and distributed denial of service threats. The main emphasis here being on the ways in which an attacker could exploit vulnerabilities in the functionality of the system to reduce or destroy its capability to provide service. NVD does not however extend to cover system exposure to physically destructive acts of man and nature although this area will be covered to some degree during the threat assessment stage.

2.3.3 Weak Security Management

Vulnerability Detection also addresses concerns over the lack of adequate system security awareness. By assessing the target system's vulnerabilities to a variety of known attacks, NVD provides a way of testing the users' and system administrators' responses to security events, the strength of the detection mechanisms, the adequacy of security procedures and the extent to which they are followed.

2.4 The Scope

Vulnerability Detection covers the use of computer-based tools, techniques and skills to perform:

- External Testing. Probing the target system over the communication links and interfaces it provides to the world outside its boundaries with the aim of discovering ways of gaining unauthorized access to the system. External testing applies the methods available to and used by the hacking community.
- Internal Testing. Emulating the large variety of ways available to insiders, people who already have some degree of authorised access to the system, to gain greater access than explicitly or implicitly permitted.

Vulnerability Detection can also be extended to include social engineering methods; the use of non-technical means to acquire system access control information and thus facilitate electronic access. This obviously requires a different set of skills and further discussions with Sapphire should be carried out if you wish to discuss this in more detail.

- One thing is certain about the scope of any Vulnerability Detection; it can be extensive and time consuming. It needs to cover all of the areas in which a system could be vulnerable to unauthorised access. Thus it includes:
- Communications services from simple modem links to complex network services.
- Platform services (operating systems) covering all platform types in common commercial use.
- Application services covering the wide variety of applications used.
- Security services, the range of IT security services deployed across and at various points in a system's architecture. The need is to understand these services and how they could be misconfigured and bypassed. This includes a good understanding of the use of any cryptographic based security solutions.



Vulnerability Assessment – Best Practice Summary

Furthermore, appropriate service providers should ensure that their consultants are fully up to date with IT security vulnerabilities and the exploitation of these, a fast moving field.

2.5 Industry Trends

2.5.1 IT Security Awareness and Drivers

Although the subjects of "Information Warfare" and hacking are probably a little over hyped, there is evidence of growing abuse of information processing systems for criminal, malicious and competitive reasons. Some of the young hackers of the 80's whose initial motivation was usually exhibitionism and at worst mischief are now offering their matured skills for hire. The level of discussion and exposure of this in the general press as well as the computer press is increasing awareness of IT security issues and responsibilities in the higher levels of commercial organisations. At the same time these organisations are discovering business needs and advantages in opening up IT channels with their suppliers, partners and customers. The problem is, how do they take advantage of large scale to global IT communication services without dangerously exposing their current and future systems to the threats they keep hearing about?

Similarly, the use of IT to facilitate communications within the organisations own systems increases the danger from the inquisitive, mischievous or malicious insider. Although this still remains the greater area of risk, there seems to be less corporate level concern over the insider threat at the moment.

Thus the key concern within the higher levels of corporate IT responsibility is how to open their systems to the outside world without having their corporate names appear in the press as another hacking victim or, far worse, discover that they are the victim of external computer assisted fraud or industrial espionage.

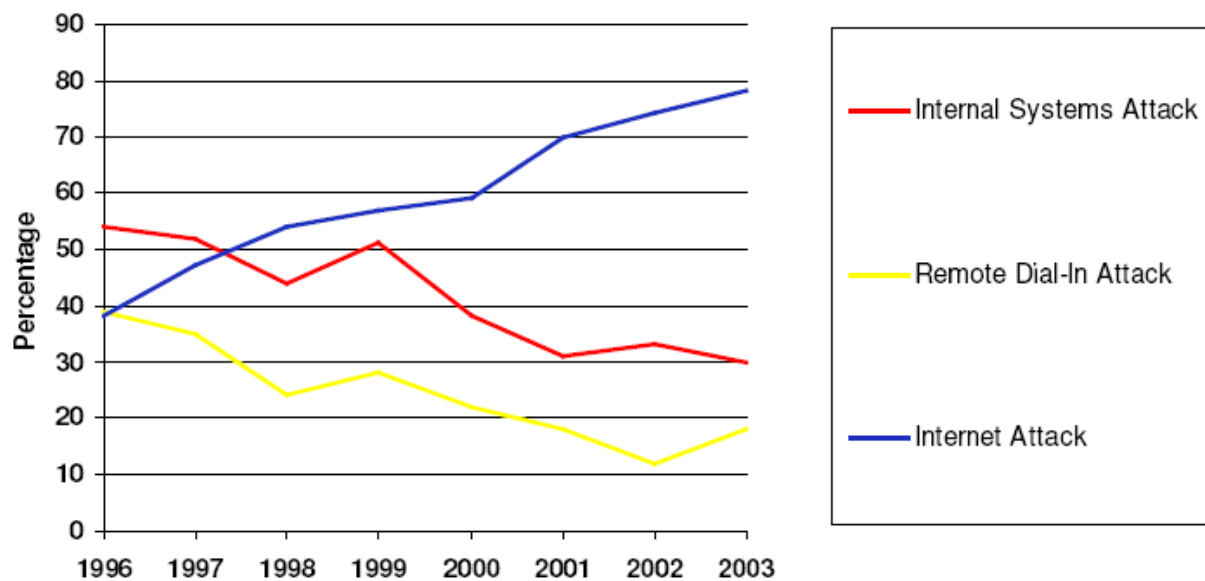


Figure 1 : CS/FBI Survey 2003



2.5.2 The Need For Vulnerability Detection

Firewalling the system is a solution many are being encouraged to adopt however, a number of organisations already realise the limitations of this approach. Effective external firewalls tend to prevent the business's customers, suppliers and partners from gaining access over the channels they guard. They need to open up the appropriate parts of their systems to various types of outsiders and provide communication channels to these.

Thus firewalling their system's interfaces to the Internet and other third-party networks is only a solution to part of the problem. It does not address all the other, authorised and unauthorised, IT communication channels with the outside world. Some of these communication links have existed for sometime, new ones are being added at an increasing rate and workarounds to existing firewall restrictions are constantly being developed.

The demand is growing for ways of identifying all of the organisation's system's exposures and vulnerabilities to outside (and more importantly, inside) attack. Where the organisation has established routes into the system for authorised external users, perhaps via a VPN, then these need to be explored to discover whether they offer greater access than was intended. Finally, having accepted that outsiders will gain access to their systems, organisations must continue to ensure that any authorised user could not exploit the weaknesses and vulnerabilities in the systems to access system resources beyond their authority.

Those that have matured their security concerns to this point have also realised that a practical analysis of the system's vulnerabilities is the only way forward. In other words Penetration Testing; actively scanning and probing the system from various points, emulating various types of attacks, looking for vulnerabilities.



3 THE CHECK SCHEME

3.1 What is CHECK?

IT security health checks identify vulnerabilities in IT systems and networks which may compromise the confidentiality, integrity or availability of information held on that IT system.

CESG has traditionally provided IT health check services for HMG and the wider public sector. Demand for these services has grown. Therefore, in line with similar CESG initiatives, a special partnership with industry is the most appropriate way of meeting this demand. The IT Health Check Service, or CHECK, was developed to enhance the availability and quality of the IT health check services that are provided to Government in line with HMG policy.

Check Service Providers are currently permitted to work on systems processing protectively marked information up to, and including, CONFIDENTIAL. For sensitive HMG or CNI systems, and occasionally other agreed requirements, the IT Health Check service will continue to be provided by CESG personnel. However, there may be occasions where it would be permissible for CHECK Service Providers to undertake tests on such systems.

3.2 Why you need a CHECK Service Provider

Your IT systems probably hold data which is critical to your organisation. You may have created a system that you believe is secure, that uses assured solutions and appropriate security procedures. But how sure are you that your system does not have any vulnerabilities and that it has been correctly configured? _

Increasingly IT and security publications report alarming incidents involving breaches of security on IT systems. According to the DTI sponsored Information and Security Breach Surveys, sixty per cent of organisations suffered a security breach in the last two years. There are indications that the cost of a single security breach could be in excess of £100,000.

A CHECK Service Provider can analyse the systems or networks you rely on to carry out your business securely and effectively by conducting a number of tests designed to identify any weaknesses utilising publicly known vulnerabilities and common configuration faults. You will receive a report detailing any vulnerabilities and recommending effective security counter measures.

3.3 Confirming CHECK Membership

It is important that company's wishing to engage the services of a CHECK Service Provider take steps to verify that the Company they employ is a current member of the CHECK service. The credentials of any Company claiming to be a member of CHECK can be checked using the list of Companies hyperlink (located at www.cesg.gov.uk) to 'finding a CHECK Service Provider'. This list is updated on a daily basis and is therefore the most reliable source of information.



4 VULNERABILITY DETECTION APPROACH

4.1 Introduction

When addressing the need for NVD the client should be comfortable that their chosen supplier will provide for the following service requirements:

- The need for total confidentiality of the system vulnerability information and any other customer sensitive information either discovered or released through NVD. Closely associated with this requirement is the need for mutual trust.
- The capability to test for and discover security vulnerabilities in all aspects of IT systems in an efficient and repeatable manner and to customise the relevant NVD service to match the customer's use of IT.
- The ability to produce and present useful reports on the vulnerabilities discovered and, where required, countermeasures to those vulnerabilities.

The need for confidentiality and trust is fundamental and applies to all aspects of Vulnerability Detection. Consequently the methods and practices used to achieve this are defined in the General Working Practice section of this document.

4.2 Vulnerability Detection Services

4.2.1 Introduction

There will be customers who want to use the NVD as a discrete service and not as part of a wider package of services. The rationale being that they would rather maintain a clear separation between the "attackers", the security testers, and the "defenders" the security solution providers. Other customers may wish use their service provider to assist in the closing of the system security holes discovered by an NVD service.

The rest of this sub-section outlines some of the ways NVD services can be offered.

4.2.2 Basic Services

These services separate into:

- External testing services
- Internal testing services

Each being composed of a set of scanning and probing test modules, selected and tailored to meet the individual customer's requirements as dictated by the types of platform, application and communication services used. In their basic form these service packages produce reports identifying the vulnerabilities found.

4.2.3 Advanced Services

This offers four additional extensions to the basic packages:

- Application testing. An investigation of a specific application. This is a more in-depth analysis looking for programming errors and is typically performed on customized or bespoke web-based software.
- Countermeasure Recommendations. This is the most likely extension to a basic service. It covers the identification and recommendation of countermeasures to the vulnerabilities found.
- Threat and Risk Assessment. An analysis of the various types of security threats to the customer's system, its resources and the business dependency on IT is



Vulnerability Assessment – Best Practice Summary

performed. This will help focus the efforts of the NVD exercise. The Risk assessment assists the customer to properly prioritise the vulnerabilities revealed by the Vulnerability Detection.

- Social Engineering. The Vulnerability Detection is complemented with social engineering techniques to discover information, which may assist in gaining unauthorised access to the target system.



5 GENERAL WORKING PRACTICES

5.1 Introduction

Establishing and maintaining mutual trust is fundamental in the Vulnerability Detection business. The need is for:

- Total confidentiality of the system vulnerability information and any other customer sensitive information either discovered or supplied through the NVD service.
- Customer confidence that the NVD approach is methodological and comprehensive.

5.1.1 Tools Used

A large range of software tools should be utilised during an exercise.

Initial stages of a task will usually require the usage of port scanners and automated tools, such as Nmap or Nessus. Often another automated scanning tool is used in order to gain more confidence in the results generated by the former.

A variety of more specialised scanning applications should then be used (e.g. Whisker, AirSnort, Pandora, NBTScan), depending on what systems and services are discovered during the process.

Available services and applications should be checked manually using applications such as a Webbrowser and netcat. This is often monitored with a packet sniffer (sometimes Ethereal or tcpdump). Also any available client software or problem specific attack software (including published 'exploits') should be evaluated and used as the need arises.

It is often necessary, or useful, to quickly create custom attack tools to exploit discovered software problems or configuration defects. This can be achieved using the 'Perl' language and occasionally using 'C' in the cases where this would be more convenient. The 'NASL' language (part of the Nessus software) should also be applied from time to time which is designed specifically for the creation of vulnerability testing software.

5.1.2 Project Completion

At the end of the project, all copies of reports and intermediate findings produced by the project should be removed from the service providers equipment, with a copy of each being left with the customer. Similarly, the supplier should retain no paper or electronic copies, unless explicitly requested and authorised by the customer.

5.2 Security Procedures

5.2.1 Staff Clearances

All of the service providers staff involved in NVD Projects should have been vetted; this is usually based on HMG security clearances.



6 EXTERNAL (PERIMETER) TESTING SERVICES

6.1 Introduction

There are a variety of routes possibly available to the outsider to gain electronic access to an organisation's systems. They range over telephony (PBX and voice mail systems), dialup modem connections, leased lines, X.25 circuits, ISDN, DSL and Cable. These are used for a variety of business purposes, including; support for remote and home working by staff, dedicated connections with business partners and suppliers, access to public networks (e.g. Internet) and third party networks.

What is to be tested depends on what external communication routes and services the organization believes it is intentionally or possibly accidentally offering. For this reason the client may wish to use a set of External Testing Modules (see following) which can often be separately selected and combined to meet a customer's specific needs.

6.2 Perimeter Checking

This provides various services to build and maintain confidence in the security of the customer's firewall configurations, whether they are deployed at internal network or external (Internet) boundaries.

We recognise that firewall configurations vary, being designed to meet differing security and business needs. Our firewall checking services accommodate this by offering the following modules which can be combined and tailored to meet the customer's particular requirements for firewall checking and testing.

6.2.1 Internet Vulnerability Scanning

This performs a scan of the customer's Internet connection from elsewhere on the Internet to determine what services and associated vulnerabilities may be exposed to the outside world.

6.2.2 Perimeter Network Testing

This module extends the remote testing by checking for vulnerabilities, which may only be visible inside the external router. This helps determine the dependency on the external router, which may be third party supplied and configured.

6.2.3 E-mail Testing

There are a variety of electronic mail services available. Each one has potential and known security vulnerabilities. This will require investigation of each of the type of mail services used and which may be externally visible to determine their vulnerability to:

- Message integrity and confidential attacks by means of message interception and replay.
- Denial of service attacks by flooding the service or individual mailboxes with large volumes of messages.
- System breaking or disruption by either:
 - Overflowing internal buffers
 - Exploiting undocumented features
 - Inclusion of macros or other executable strings to exploit features and facilities in mail readers.



6.2.4 Firewall System Checking

Examines the security hardening and configuration of the firewall, and other exposed systems to establish how resistant they are to further penetration should unauthorised access be achieved.

6.3 System Access via Modems

The objective here is to identify, wherever possible, the type of connection service being offered by active modems, and whether these may present an opportunity to the outsider to gain easy access to a computer system.

Connections to customer systems through modem lines are used for a variety of purposes covering system vendor maintenance, employee, customer, and supplier access needs. The concern is that some of these connection facilities may be configured to allow easy access to unauthorised people.

There are a variety of modem types and communication protocols. From the security point of view there are two types of modem enabled communication links:

- Protected Links. Based on dial back, challenge/response, or one-time password schemes and devices. Generally these are secure.
- Direct Links. Typically the communication links using the cheaper and more popular modem units. The security of these is dependent on the strength of the authentication services configured on the computers to which they provide access.

6.4 Telephone Scanning

The concern here is that there may be unauthorised or 'semi-official' modems connected to company phone lines and providing access to company computers. The scanning techniques for detecting these and any authorised modem lines are those used by the hacking and phone phreaking community.

Scanning for active modem lines is done using a modem and a PC running a scanning program. The scanning program is sometimes referred to as a wardialer or demon dialer. The scanner tries each number in the specified range and records the response it gets. The possible responses are:

- Busy
- Voice
- Time out (after a specified number of rings)
- Tone (indicating a possible; modem, fax machine, or CTI application)
- Carrier, offering a computer connection.
- Other (usually silence).

Scanning during normal operational hours is necessary only where it is believed that some of the modems and their associated computer equipment may only be switched on in this period. However, scanning in normal operational hours can cause minor annoyance, and it will detect far more busy lines. Consequently, within normal operational hours scanning requires closer monitoring and control.

Out of normal operational hours scanning does still require sufficient monitoring to exercise override options where necessary. However, during this time, other more manual scanning analysis activities can be performed.

In all cases we deliver a comprehensive report on our findings and, where required, provide recommendations and guidance on fixing problems. All our findings and reports are handled in the strictest confidence



7 INTERNAL TESTING SERVICES

7.1 Introduction

The principal objective here is to determine what an attacker could achieve, usually with some level of authorised access to the organisation's IT services, by exploiting security weakness and vulnerabilities in the IT system.

There are three levels to Internal Security Testing:

- Network Level. Testing for vulnerabilities in the internal network services, which would allow unauthorised access to computers and services on the networked system.
- Computer Level. Testing for security misconfiguration and vulnerabilities in the operating systems of the computers attached to the organisation's networks. This can be extended to examine the security configuration of computers which are either stand-alone or only intermittently connected. Of particular interest here are portable computers and PDAs used by the organisation's staff.
- User Level. The testing here examines what various types of users could achieve

7.2 Network Level Testing

There are a significant number of known security vulnerabilities in the IP-based networked services provided by different platforms. The presence of these network services vulnerabilities exposes the systems to:

- Unauthorised access attacks
- Denial of service attacks
- Repudiation attacks

And combinations of these attacks from those who have access to the network.

These security vulnerabilities mainly arise through:

- Misconfiguration of the network services and the access control regimes on the machines. The default (out of the box) settings for many of these services are over generous in the connectivity they permit.
- Undocumented features and bugs in the services, which permit those who know about them to bypass or subvert the security-relevant mechanisms deployed.

In exploring the machines attached to an IP based network for such vulnerabilities appropriate tools will be used to:

- Identify all currently connected machines within a given IP address range and determine what IPbased network services they are offering. This includes desktop machines which, given the increasingly use of more powerful and sophisticated desktop platforms, are tending to offer similar network services to those normally associated with server type platforms. An advantage of this IP address range scanning is that it sometimes uncovers unauthorised machines connected to the network.
- Probe each machine offering network services according to platform and service type for a known set of vulnerabilities.
- For each vulnerability discovered, explain and possibly demonstrate what can be achieved through the exploitation of the vulnerability.



Vulnerability Assessment – Best Practice Summary

- Show how vulnerabilities on one machine can pose a security threat to other otherwise secure machines. This indirect vulnerability arises through the common practice of configuring networked machines to trust each other in their sharing of security relevant information on users, data and services.

Sapphire will produce a report detailing the results of the IP address range survey, the vulnerabilities found and the potential or demonstrated exploitation. With respect to the vulnerabilities Sapphire will provide our assessment of the security risk based on the skill level required to exploit it.

An integrated part of this service comprises scans for vulnerabilities arising from the existence of wireless networks, unprotected wireless access points, and unknown activated devices, and generally consists of Sapphire staff walking around the client's premises focusing specifically on high-risk areas.

7.3 Computer Level Testing

Computer level testing extends that done at the network level by using security checking tools and techniques installed and performed on selected computers.

The objective here is explore example or specific computers for vulnerabilities in the configuration of the operating system and underlying services which are only visible to testing conducted on the computer.

The computers selected for this type testing can be:

- Examples of types of computers deployed by the organisation in various roles.
- Computers revealing potential vulnerabilities to network level testing.
- Computers considered being particularly sensitive because of the nature of the information and/or service they contain.

Where appropriate, this testing can be extended to include examination of the business applications, their security configuration, and the extent to which this application security is dependent on the security configuration of the underlying operating systems and their services. It is often the case that access to sensitive business application data can be achieved by using non-application tools and services provided by the operating system.

7.4 User Level Testing

In user level testing we adopt various user roles to determine what operations could a user with some degree of authorisation to use the system and its services do which may be beyond their authorisation.

Typically this type of testing is performed when there is some specific concern over the actions of certain types of users. However, If the customer wishes to have a wide ranging IT security audit performed, including an examination of the user level system security practices and procedures, it is necessary to test and observe how well these are enforced. In this case we recommend that our Project Team be allowed to adopt the various user roles and test how well the user interfaces constrain each type of user to those operations for which they have authorisation, and how easily a mischievous or inquisitive user could escape such constraints.



8 CONTACT INFORMATION

For further information concerning penetration testing service please contact your Sapphire business development manager in the first instance.

If you do not have a business development manager, feel free to contact our team:
info@sapphire.net
01642 702100 (office)

The information in this document is subject to change without notice and must not be construed as a commitment on the part of Sapphire Technologies Ltd. Sapphire Technologies assumes no responsibility for any errors that may appear in this document.

No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, graphic, electronic, or mechanical, including photocopying and recording, without the prior written permission of the copyright owner.

© 1997-2009 Sapphire Technologies Ltd. All rights reserved. Sapphire Technologies and the Sapphire logo are trademarks; Sapphire, and the Sapphire tag line, *Secure in the Knowledge* are trademarks of Sapphire Technologies Ltd. in the UK and certain other countries. Names of other products mentioned are trademarks or registered trademarks of their respective holders.

Sapphire

Globe House, Station Street

Stockton on Tees, Cleveland, TS20 2AB

Tel 0845 58 27001 **Fax** 0845 58 27005

Email security@sapphire.net **Web** www.sapphire.net