

**INTOSAI EDP COMMITTEE PERFORMANCE AUDIT SEMINAR,
SLOVENIA 14-16 MAY 2001 COUNTRY PAPER OF THE OFFICE
OF THE AUDITOR-GENERAL: REPUBLIC OF SOUTH AFRICA
AUDITING IN A NETWORKED PUBLIC SECTOR**

Prepared by: E J PELCHER: Executive Manager: Computer Auditing

1. INTRODUCTION

Due to the widespread proliferation of Internet connections, laptop computers, modems, e-mail systems, Intranets, Extranets, etc., the stakes involved in information protection have risen dramatically. This paper aims to support the Netherlands Court of Audit lead paper by providing an overview of the way in which the Office of the Auditor-General in South Africa conducts network audits.

2. BACKGROUND ON REPUBLIC OF SOUTH AFRICA'S NETWORK ENVIRONMENT

The State Information Technology Agency (SITA) is responsible for providing the infrastructure to link government departments across the country. This networking infrastructure comprises communication links such as Telkom data lines, devices such as routers to direct the data flow over those communication links, and various security mechanisms to

maintain control over the data flow between the various departments connected. SITA also provides connectivity to third parties such as banks and other organisations, as well as to the Internet. The infrastructure is known as OpeNET.

The network is divided into two zones of trust: the OpeNET Intranet internally and the OpeNET perimeter zone connected to the Internet.

The departments have Local Area Networks that are connected to OpeNET.

3. FOCUS AND METHODOLOGY OF NETWORK AUDITS

Networks are like chains in which the link with the weakest security poses a threat to the security of all other links in the chain. Over the past two years the Office of the Auditor-General in South Africa has been conducting network audits to address some of the important issues relating to network security and risks. The Office regards security as an 'end-to-end' process, in that network security is viewed in its entirety. Securing only part of a network provides no guarantee that it cannot be attacked through another 'compromised' machine on the network. The focus of the Office is therefore on securing information through a

combination of securing host machines and a perimeter defence strategy (i.e. securing the perimeter of a network with a single entry point through a firewall).

The Office's network audit methodology consist of the following phases:

- Planning
- Execution :
 - Controlled external penetration testing
 - Controlled internal penetration testing
 - Security diagnostic reviews
- Reporting

3.1 PLANNING

In the planning stage of a network audit information is obtained on the network environment, i.e. on the network architecture, protocols, topology, servers, routers and other network devices. Possible risks are identified, critical aspects of the network are evaluated, and the most appropriate tools and techniques to be applied during the audit are identified. Specific audit procedures have been designed for this purpose.

3.2 EXECUTION

3.2.1 Controlled external penetration testing

Typically, this phase concentrates on perimeter security measures, including the Internet, firewalls, routers, web servers and other externally accessible devices, such as any modems that may have been installed.

The focus is on connections from the Internet via the mainframe and outside-routed connections.

3.2.3 Controlled internal penetration testing

During this phase critical components within the network are targeted. Key communication devices (e.g. routers and switches), security devices (e.g. firewalls, authentication servers), and application devices (e.g. databases and servers) are analysed from the local area network for exploitable vulnerabilities.

Aspects reviewed for critical servers include:

- Security monitor and logging procedures
- System administration procedures
- Change control
- Backup and recovery

Aspects reviewed for the Internet firewall and web server include:

- File permissions
- Password composition
- Key configuration and startup files
- Trust relationships
- Network connections
- Running processes
- Suspicious files and the integrity of existing files
- Control over and use of strong encryption over super user passwords
- Operating system, firmware and patch-level updates that may migrate known vulnerabilities

3.2.3 *Security diagnostic reviews*

In this phase a representative sample of key communication, security and application devices will be evaluated.

Technical tests play a crucial role in identifying areas of weakness. Various probes, sniffers, war dialers, etc., are used to test network security. Some of these tests are listed below:

- Testing router packet filter configurations
- Brute force attempts

- Exploiting anonymous file transfer protocol bugs
- Exploiting network file system misconfigurations
- Exploiting trust relationships
- Denial-of-service attacks
- Intelligence-gathering attacks
- Password attacks
- Internet protocol (IP) source-routing attacks
- IP address-spoofing attacks
- IP forwarding attacks
- Password-guessing attacks

3.3 REPORTING

All tests conducted during the audit are done in the presence of the network administrator. The audit team therefore provides this person with a continuous briefing on the tests performed, vulnerabilities noted and access obtained.

On completion of the execution phase of the audit, the findings, analysis, conclusions and recommendations are discussed with the network administrator and a management report is compiled.

The management report is divided into sections, such as an introduction, an executive summary, detailed findings containing results, detailed explanations, specific recommendations to be implemented, and a conclusion on the effectiveness of the various security and control areas. The accounting officer is requested to comment on the risks and exposures and to indicate what corrective steps are envisaged or have been implemented. The comments are evaluated and a follow-up audit is conducted in due course. A summarised paragraph on the key findings of the audit is presented to the relevant legislative body.

Due to the sensitive nature of some of the information in the management reports, e.g. IP addresses of specific vulnerabilities exploited telephone numbers associated with compromised modems, specific vulnerabilities exploited and data accessed, the reports are classified and distributed to authorised staff only.

Audits conducted by the Office have identified critical weaknesses, mainly in the internal networks at various auditees. The management reports and recommendations included in the audit reports and the resultant corrective steps have contributed significantly to the improvement of security in the South African networked public sector.

4. CONCLUSION

Network security has become increasingly important in view of the increased interconnectivity of systems. The Office of the Auditor-General in South Africa has realised, as did the Netherlands Court of Audit, that the auditing field has changed in a fundamental way. Auditing has to focus on the network vulnerabilities and must ensure that, aspects such as incorrect configuration of services and the exposure of information through (often unnecessary) services in network environments, are addressed. New exposures surface every day, necessitating continuous follow-up network audits and reviews of the audit methodology.