



## **Demystifying Network Security Auditing**

Ian Parker, GCUX, GCFW, CCSA, CCSE  
President  
Sentinel Ridge Consulting Group, Inc.

# 1 Introduction

Due to the proliferation of new industry and government regulations in recent years in relation to the handling of financial and personally identifiable information, when most people think of an IT “security audit”, they usually have in mind a compliance audit. However, network security consultants can perform many different kinds of security audits, depending on the needs of the organization. The terminology used in this field is inconsistent and often confusing to clients and consultants alike. This article attempts to demystify the subject of security audits by applying some definitions to the various terms that are used. Hopefully these definitions will assist clients in choosing the type of security audit that meets their requirements.

## 2 Security Review

A security review is an informal survey of an organization's security posture, based on the professional experience of the consultant. The survey may comprise all or just a portion of the computing infrastructure, depending on the agreed upon scope of work, and may include some or all of the following activities:

### *2.1 Penetration test*

A penetration test is the process of evaluating a network's security controls by actively analyzing it for design weaknesses, technical flaws and vulnerabilities. Unlike other activities discussed in this section, a penetration tester usually follows a well defined testing methodology, thereby ensuring that a quality product results and that similar tests conducted at different times or by different individuals produce consistent results.

The three most widely used methodologies for penetration testing are the Open Source Security Testing Methodology Manual (OSSTMM), the National Institute of Standards and Technology (NIST) Technical Guide to Information Security Testing and Assessment (Special Publication 800-115) and the Information Systems Security Assessment Framework (ISSAF). As each methodology contains strengths and weaknesses, a penetration tester may combine elements of all three methodologies for a given test.

### *2.2 Vulnerability scan*

A vulnerability scan uses automated tools against hosts within a network to determine if and how these hosts can be exploited. The scanner seeks out security flaws based on a database of known flaws, testing hosts for the occurrence of these flaws and generating a report of the findings.

In the early days of security auditing, it was common for a company to hire a security consultant to perform such a scan of the network. The consultant would proceed to run the scan using the tool of his or her choice, which would then generate a thousand page report of vulnerabilities. The consultant would then drop the report on the IT manager's desk and walk away with payment for services rendered.

Needless to say, a vulnerability scan in and of itself is rarely of much value without subsequent analysis by a knowledgeable individual (see Section 3.1) who can determine whether the identified vulnerabilities are a) correct<sup>1</sup> and b) important enough to warrant some kind of control.

### ***2.3 Architecture review***

A review of the overall structure, topology, protocols and framework of a network from a security standpoint.

### ***2.4 Policy review***

A review of the written rules that determine the use of resources within the network. Note that a policy review may not validate that the policies are actually being followed. (See Section 2.5)

### ***2.5 Compliance review***

A review to determine the degree of compliance with the organization's security policies. (See Section 2.4)

### ***2.6 Risk analysis***

An analysis of the likelihood of a successful attack against the network. Enumeration of the risks that are present has limited value unless the business impact is also considered (see Section 3.2) but does provide a starting point to determine the kind of security controls that may be warranted.

---

<sup>1</sup> I once intercepted and reviewed a large vulnerability scanning report that was on it's way to upper management. The report identified several critical vulnerabilities within hosts running Microsoft's Internet Information Server. However, investigation of the IP addresses showed that the hosts in question were actually Cisco routers. Vulnerability scanning tools make mistakes!

## **3 Security Assessment**

A security assessment is similar to a security review and may, in fact, result from a previous review. During a security assessment, the consultant analyzes all potential security weaknesses and determines their relevance and criticality to the organization. For example, a vulnerability scan may determine that the network is vulnerable to a particular exploit against Linux servers (because the Internet firewall doesn't block the traffic). However, such a finding can safely be ignored if the organization uses only Windows servers.

In addition to the activities described in Section 2, a security assessment may also include some or all of the following activities:

### ***3.1 Vulnerability assessment***

The identification and *quantification* of vulnerabilities on a network. The quantification aspect is what distinguishes a vulnerability assessment from a vulnerability scan, discussed in Section 2.2.

### ***3.2 Risk assessment***

Builds on a risk analysis (see Section 2.6) by factoring in the business impact to the organization of each identified risk.

### ***3.3 Architecture assessment***

A more structured and formal analysis of the network architecture. (See Section 2.3.)

### ***3.4 Policy assessment***

A more formalized analysis of the organization's security policies, perhaps involving interviews with employees to assess their awareness and understanding of the policies.

## **4 Security Audit**

A security audit is a comprehensive examination of the organization's security posture against either an industry standard or governmental directive. Whereas, security reviews and assessments deal mainly with security technologies, audits take into account people, processes and technologies.

In addition to the activities described in Sections 2 and 3, a security audit may also include some or all of the following activities:

#### **4.1 Compliance audit**

A comprehensive analysis of an organization's adherence to regulatory guidelines. Examples of industry guidelines and laws that are frequently used as a basis for performing compliance audits are the Payment Card Industry (PCI) Data Security Standard, the Sarbanes-Oxley act (SOX), the Health Insurance Portability and Accountability Act (HIPAA)<sup>2</sup>, the Gramm-Leach-Bliley Act (GLBA) and, in Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA).

#### **4.2 Policy audit**

A comprehensive analysis of the quality of an organization's security policies.

#### **4.3 Procedure audit**

A comprehensive analysis of the quality of an organization's security procedures. Note that an organization may have excellent security policies (see Section 4.2) but may lack procedures under which the policies should be carried out.

#### **4.4 Risk audit**

An analysis to determine if an organization has implemented the security controls necessary to reduce identified risks to an acceptable level.

*Ian Parker is the president of Sentinel Ridge Consulting Group, a firm specializing in the security of corporate computer networks. You can reach him at [sentinelridgeconsulting.com](http://sentinelridgeconsulting.com).*

---

<sup>2</sup> The Canadian version is the Health Information Protection Act (HIPA).