

# STATE OF THE ART VULNERABILITY DETECTION AND SUGGESTIONS FOR IMPROVEMENT

H.S. Venter *[hventer@cs.up.ac.za](mailto:hventer@cs.up.ac.za)*  
J.H.P. Eloff *[eloff@cs.up.ac.za](mailto:eloff@cs.up.ac.za)*  
*Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa.*

**Abstract:** The focus of this paper is to give an overview of current vulnerability scanner (VS) products and to provide ideas for future improvements. Since each VS product available on the software market today is developed by a separate vendor, there are significant differences in these VS products. VS products differ extensively from each other. The main differences between state of the art VS products are the types of vulnerabilities that are detected as well as the number of vulnerabilities that can be detected. This paper suggests the concept of a common set of vulnerability categories, referred to as harmonised vulnerability categories, to be used by different VS products. Furthermore it introduces the concept of vulnerability forecasting.

**Keywords:** Harmonised vulnerability categories, Vulnerability, Vulnerability scanner (VS), Vulnerability mapping, Vulnerability assessment, Vulnerability forecasting.

## 1 INTRODUCTION

Due to the increasing awareness of the public of security issues on the Internet, the number of security products available on the software market today is myriad and still increases. This is why you face a dilemma when choosing the right security product for your organisation's security needs.

There are many ways in which information can be secured by using various information security technologies [VEE1 03]. Computer security in an organisation can generally be addressed in two ways: before a security

incident can take place, or after a security incident has taken place. Security that is addressed before a security incident takes place is referred to as proactive security. Proactive security is implemented by using vulnerability scanner (VS) products. Security addressed after a security incident has taken place, or when the security incident is still taking place, is referred to as reactive security. Reactive security is implemented by intrusion detection systems [BACE 00].

The focus for this paper, however, is to develop a better understanding of current state of the art in VS products. Vulnerability scanning means having an automated scanning program, referred to as a VS, that scans a computer or a network of computers for a list of known weaknesses, referred to as vulnerabilities [SCHN 00]. In other words, vulnerability scanning refers to the application of state-of-the-art information security technology to secure information on the Internet [VEE1 03].

There are many VS products available on the software market. They often refer to the same vulnerability in a different way and this makes it very difficult to see exactly which vulnerabilities are scanned for by the different VS products. This dilemma can be solved by using the framework of **harmonised vulnerability categories** [VEE2 03]. Other aspects of VS products are also considered in this paper, for example, the specific database structure of a VS. These aspects are discussed in an attempt to shed more light on the problems that the different VS products pose.

The sections that follow will discuss VS products in more detail. An overview of the current VS products is discussed. Some of these products are discussed in detail, with the emphasis on the databases that these VS products employ. Some issues on the future of VS products concludes this paper.

Table 1: The harmonised vulnerability categories

Harmonised vulnerability categories	
1	Password cracking and sniffing
2	Network and system information gathering
3	User enumeration and information gathering
4	Backdoors, Trojans and remote controlling
5	Unauthorised access to remote connections & services
6	Privilege and user escalation
7	Spoofing or masquerading
8	Misconfigurations
9	Denial-of-services (DoS) and buffer overflows
10	Viruses and worms
11	Hardware specific
12	Software specific and updates
13	Security policy violations

## 2 VS PRODUCTS

It is important to be aware of the different VS products available on the software market before studying some of them in more detail. There are freeware as well as commercial versions of VS products available and some of the products differ extensively from other products. The section that follows lists some of the major role players in VS technology available today and attempts to place the different aspects of the products in perspective to each other.

### 2.1 VS Product Overview

Table 2 shows a list of two well-known VS products available today in no particular order of preference.

Table 2: VS products

VS product	Commercial or freeware	Reference
bv-Control	Commercial	[BIND 03]
Internet Security Scanner (ISS) 6.2.1	Commercial	[ISSN 03]
Nessus Security Scanner	Freeware	[DERA 03]
Security Administrator's Integrated Network Tool (SAINT) 4.0	Commercial	[SAIN 03]
Security Analyzer 5.1	Commercial	[NETI 03]

The SAINT, the ISS, and the Nessus Security Scanner will be discussed in more detail in the following sections. The focus of the discussion of these products will not be to evaluate and compare them with each other, but rather to comment on the practical experience encountered by the authors while

working with the products. This is followed by elaborative discussions on each product's vulnerability database in terms of differences.

## **2.2 The SAINT**

The Security Administrator's Integrated Network Tool (SAINT) [SAIN 03] is discussed in this paper because it was freely available until recently and supports the use of CVE. CVE is an acronym for "Central Vulnerabilities and Exposures" [MITR 03]. CVE is a list or dictionary that provides common names for publicly known information security vulnerabilities and exposures. The SAINT can run on UNIX and LINUX operating systems and also scans for vulnerabilities on multiple operating systems. The SAINT is also available in an online version.

### **2.2.1 Practical Experience with the SAINT**

Because the SAINT incorporates CVE into its vulnerability database, standard vulnerability names are used. In addition, CVE's Web site also has more information available on how to fix the detected vulnerabilities. This is a major advantage of the SAINT. The disadvantage of the SAINT is that it categorises its vulnerabilities into 177 categories, which makes it difficult to work with. It is better to have fewer vulnerability categories that are more manageable as the harmonised vulnerability categories suggest.

### **2.2.2 The SAINT Vulnerability Database**

Of the 13 harmonised vulnerability categories, Password cracking and sniffing, User enumeration and information gathering, Backdoors, Trojans and remote controlling, Spoofing or masquerading, Viruses and worms, Hardware specific, and Security policy violations are covered in very little detail, if at all, by the SAINT's vulnerability database.

## **2.3 The Internet Security Scanner (ISS)**

The ISS version 6.2.1 is discussed in this paper because the ISS was one of the first VS products available on the software market with a graphical user interface. It is established and widely used in the industry today. There is an ISS version [ISSN 03] that can be downloaded from the Internet free of charge with full functionality, but it is limited to scan only the host on which it is installed.

The ISS supports the CVE standard to enable users to easily determine if issues with different names are the same, and to allow for efficient sharing of security information. A CVE reference, however, may not exist for every

vulnerability check used in the ISS and because of this CVE is only partially supported by the ISS.

### **2.3.1 Practical Experience with the ISS**

The ISS was installed on a Windows workstation and then set up to scan workstations and servers connected to the network for the vulnerabilities as specified in its vulnerability database. The ISS runs on Windows and has a very good user interface, but it can also scan for vulnerabilities on other operating systems like UNIX. Depending on the size of the network and the specific scan policy that is set up before the scan can commence, the ISS scans the network for vulnerabilities and is relatively fast. A scan on a Windows workstation was completed in just over four minutes before a report was generated. Figure 1 shows an extract of one of the vulnerabilities in this report.

The advantages of the ISS report are that it contains good and detailed descriptions and remedy procedures. In addition, a reference to additional information for the specific vulnerability detected is provided as well as information on which operating system platforms the particular vulnerability can occur. Another big advantage is that the ISS classifies the particular vulnerability into a low, medium, or high risk factor so that the rectification of vulnerabilities can be prioritised. The disadvantage of this report is that it requires effort to work through because of its large size.

<b>Modem detected and active (Active Modem)</b>	
Risk Level:	Medium
Platforms:	Windows NT, Windows 95, Windows 98, Windows 2000, Windows ME
Description:	An active modem driver was detected. This situation only occurs when the modem is in use, or when the modem driver program is active. Modems can be a sign of an unauthorized channel around your firewall. Attackers could use a modem within the network to circumvent network security.
Remedy:	<p>The modem must not be active while the computer is attached to the network. You may want to minimize the impact of a security breach caused by an unauthorized modem use by limiting which systems trust the computer using the modem.</p> <p>If using a modem on the network is required, configure all Remote Access Setup ports so that the port usage can dial-out only. Verify that your dial-out network configuration protocols match exactly the protocols you need to access the remote network. Review share permissions and account security to verify that the file system is not accessible from a remote location.</p>
References:	<p><b>ISS X-Force</b>  Modem detected and active  <a href="http://xforce.iss.net/static/1292.php">http://xforce.iss.net/static/1292.php</a></p>

*Figure 1: An extract from the ISS report*

### 2.3.2 The ISS Vulnerability Database

Of the 13 harmonised vulnerability categories, User enumeration and information gathering, Privilege and user escalation, Spoofing or masquerading, Misconfigurations, and Viruses and worms are covered in very little detail, if at all, by the ISS's vulnerability database.

## 2.4 The Nessus Security Scanner

The Nessus Security Scanner is discussed in this paper because it is a widely known freeware product [TALI 00]. The Nessus Security Scanner executes mainly on UNIX-based platforms, but it can scan for vulnerabilities on multiple operating system platforms. The Nessus Security Scanner is built upon client-server architecture where the server works on a UNIX-based platform. Different clients are available that can run on a UNIX or Windows

operating system platform. The Nessus Security Scanner also supports CVE references.

### **2.4.1 Practical Experience with the Nessus Security Scanner**

The Nessus Security Scanner works on the concept of plug-in architecture. This means that there is a plug-in for each vulnerability that the Nessus Security Scanner can check for. This way, it is easy to add new vulnerability signatures as external plug-ins when they become available. These can simply be downloaded from the Nessus Security Scanner Web site [DERA 03] via FTP.

It is also possible to add customised vulnerability signatures. To be able to do this, the Nessus Security Scanner includes the Nessus Attack Scripting Language (NASL), which is a language designed to write customised vulnerability signatures easily and quickly. These plug-ins then also constitute the vulnerability database for the Nessus Security Scanner.

The biggest advantage of the Nessus Security Scanner is that it is very fast. The vulnerability tests performed by the Nessus Security Scanner cooperate so that nothing is done that is not necessary. For example, if an FTP server is found not to offer anonymous logins, then anonymous-related vulnerability checks will not be attempted or performed for anonymous FTP vulnerabilities, which saves time. Some VS products will attempt to scan for anonymous FTP vulnerabilities, if their scan policies were set up to do that, even if no anonymous FTP vulnerabilities are present. This causes those VS products to waste valuable time since it will not continue to scan for the next vulnerability, as defined by its scan policy, until scanning for anonymous FTP vulnerabilities has timed out. Another advantage of the Nessus Security Scanner is that it categorises the risk level of each vulnerability from low to very high in the report that it generates, enabling one to prioritise the urgency of fixing the vulnerabilities found. The disadvantage of this report, however, is that it requires effort to work through because of its large size.

### **2.4.2 The Nessus Security Scanner Vulnerability Database**

Of the 13 harmonised vulnerability categories, *Password cracking and sniffing*, *User enumeration and information gathering*, *Spoofing or masquerading*, *Misconfigurations*, *Viruses and worms*, Hardware specific, and Security policy violations are covered in very little detail, if at all, by the Nessus Security Scanner's vulnerability database.

### **3 SUMMARY OF CURRENT VS PRODUCTS**

In the previous sections different VS products were discussed and the reader should have a better understanding of how different the VS products operate. In essence all these products have one main goal: identifying vulnerabilities. But the way that these VS products go about in accomplishing this goal, often differ extensively from one VS product to another. What is more – these different VS products do not all scan for exactly the same type of vulnerabilities. Fortunately, by making use of harmonised vulnerability categories [VEE2 03], a measure is available to identify how the different VS products comply with harmonised vulnerability categories.

Figure 2 shows a mapping, compiled for this paper, of the vulnerabilities found for each of the five VS products discussed in the previous sections onto the harmonised vulnerability categories. The mapping process was done for each individual VS product. The vulnerability database of a specific VS product was carefully dissected by studying each vulnerability as defined in the vulnerability database. A particular vulnerability is then allocated to one of the 13 harmonised vulnerability categories.

From figure 2 it is clear that the different VS products comply differently with the 13 harmonised vulnerability categories. For example, the Nessus Security Scanner can detect far more network and system information gathering (category 2) vulnerabilities than all the other VS products. The Internet Security Scanner, on the other hand, outperforms all the other VS products when detecting Password cracking and sniffing (category 1), Backdoors, Trojans and remote controlling (category 4), Unauthorised access to remote connections & services (category 5), Spoofing or masquerading (category 7), Software specific and updates (category 12), and Security policy violations (category 13) vulnerabilities. In addition, only one VS product namely the Nessus Security Scanner scans for viruses and worms (category 10) and only for a very limited number of viruses and worms. The ISS, therefore, seems to be the VS product with the best amount of vulnerabilities that it can scan for across the harmonised vulnerability categories.

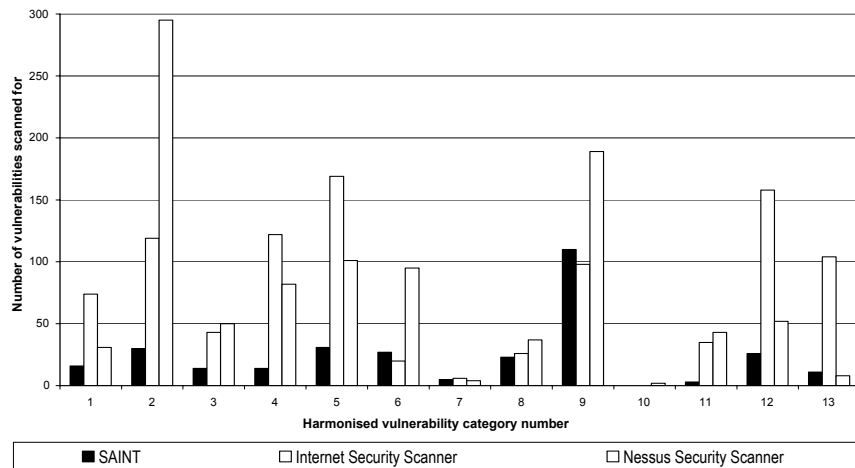


Figure 2: Vulnerability mapping of different VS products onto the harmonised vulnerability categories

## 4 THE FUTURE OF VS PRODUCTS

Although the proactive behaviour of VSs is a positive point, there are still many problems with state-of-the-art VSs. Problems such as the length and complexity of vulnerability reports produced by VS products as well as a complete absence regarding the ability of VS products to contribute to risk management on networks should be addressed. In a bid to address these and other types of problems, a conceptual model is introduced in this section.

### 4.1 Problems with State-of-the-Art VS Products

In summary, table 3 lists the problems identified with state-of-the-art VS products. In order to minimise the impact of these problems, the authors would like to introduce the concept of **vulnerability forecasting** as a future initiative to vulnerability scanning.

The term “vulnerability forecasting” (VF) can be defined as “that attempt to identify potential vulnerable areas on hosts across a network and to what extent such areas on hosts across a network will be vulnerable over a specific period in the near future”. The principal aim of VF is, therefore, to predict trends or patterns in which potential vulnerabilities could occur. Knowing what such a vulnerability forecast is means that proactive action can be taken in a bid to minimise the risks that such vulnerabilities may pose.

Table 3: Problems identified and addressed regarding state-of-the-art VS products

<b>Problems identified</b>	
1.	Conducting vulnerability scans is too time-consuming.
2.	A VS product generally occupies a vast number of network and system resources, leading to the degradation of system performance while vulnerability scans are being conducted.
3.	VS products lack intelligence because they are unable to learn about new vulnerabilities automatically.
4.	The vulnerability database structure differs extensively from one VS product to another.
5.	The types of vulnerabilities being scanned for differ extensively from one VS product to another.
6.	Scans may not always be conducted at regular intervals due to unforeseen circumstances, for example when critical maintenance on servers and the network is carried out.
7.	The vulnerability database should be updated before a scan is conducted, otherwise the scan result may not be accurate enough.
8.	Most rectification procedures cannot be automated and still require the expertise of qualified personnel.
9.	VS products do not provide adequate and sufficient information that would aid high-level risk management.

## 4.2 A Conceptual Model for VF

The high-level design of the conceptual VF model comprises three main components and is depicted in figure 3 below:

A brief description of the main components in figure 3 follows:

### (1) VS Technology (current)

This component constitutes one or more state-of-the-art VS products that are used for collecting the data needed for VF.

### (2) Vulnerability Harmonisation

This component serves as a coupler between the VS technology and the vulnerability forecasting components in a bid to “standardise” the VS product’s output into a harmonised form.

### (3) Vulnerability Forecasting

This component does the actual intelligent vulnerability forecast.

Each of the main components of the conceptual VF model, as introduced in the previous section, contains subcomponents.

### **4.2.1 The VS Technology (Current) Subcomponent**

The reason for using current VS technology in the VF model enables the use of existing technology rather than attempting to design yet another module in the VF model. In addition, any current VS product can be used in the conceptual VF model, rendering the conceptual VF model more flexible. In summary, a VS product analyses the security state of a network of hosts on the basis of information collected, referred to as scans, at different intervals. After a scan is completed, the VS product generates scan results in the form of a report that states all the vulnerabilities found during the scan and leaves it up to a person to rectify these vulnerabilities.

### **4.2.2 The Vulnerability Harmonisation Subcomponent**

The vulnerability harmonisation component is represented as the second subcomponent of the conceptual VF model. This component does not do the actual vulnerability forecasting yet, but serves as an in-between process where the data it received from component 1 of the conceptual VF model is transformed in such a way that it is “harmonised” and, thus, prepared to be “understood” by component 3 of the conceptual VF model. In summary, the output of the VS product in component 1 of the conceptual VF model, namely the scan result, serves as input to the vulnerability mapper in component 2 of the conceptual VF model. The vulnerability mapper maps the vulnerabilities found by the VS product onto the harmonised vulnerability categories and stores the result in the harmonised history database. This process is repeated each time a vulnerability scan is conducted.

### **4.2.3 The Vulnerability Forecasting Subcomponent**

The vulnerability forecast component constitutes the third subcomponent of the conceptual VF model. This main component does the actual vulnerability forecasting. In summary, the output of the vulnerability mapper in component 2 of the conceptual VF model, namely the harmonised history database, serves as input to the vulnerability forecast engine in component 3 of the conceptual VF model. The vulnerability forecast engine attempts to predict trends or patterns, in terms of harmonised vulnerability categories, in which potential vulnerabilities could occur. The Vulnerability forecast engine

constitutes the heart of the conceptual VF model. Intelligent techniques are used in conjunction with history scan data and history forecast data to forecast which harmonised vulnerability category or categories would potentially pose vulnerability problems in the near future.

## 5 CONCLUSION

This paper discussed different VS products and looked at how each respective product differs in the way that they can scan for vulnerabilities and what the impact of vulnerability forecasting may be on VS products.

It was found that VS products differ extensively from each other in terms of the number of vulnerabilities that each different VS is able to detect. In the sections above it is clear that – most of the time – using the vulnerability count is a good way to determining what the differences are between different VS products.

Far from rendering existing VS products obsolete, VF is used proactively to co-ordinate output from existing VS products with that gleaned from intelligent techniques and history data.

The concept of vulnerability forecasting has many advantages. It saves considerable time, because instead of scans being conducted all the time to detect and rectify vulnerabilities; scans can now be conducted less frequently. Having vulnerability forecasts, vulnerability problem areas – in the form of harmonised vulnerability categories – can be attended to before they can erupt. In due course, system resources are occupied less often due to fewer scans that need to be conducted.

Using harmonized vulnerability categories along with vulnerability forecasting renders the process of doing vulnerability forecasting VS product independent. The difference in the types of vulnerability categories that various VS products scan for is therefore bridged by the use of harmonised vulnerability categories. In addition, adequate and sufficient risk management can be done due to the fact that, each time a vulnerability forecast is done, vulnerability forecasts are made available for each harmonised vulnerability category.

## 6 REFERENCES

[BACE 00] BACE, R. G.; 2000; Intrusion Detection; “Intrusion Detection Concepts”, pp. 37-43; Macmillan Technical Publishing; ISBN 1-57870-185-6.

[BIND 03] BINDVIEW CORPORATION; 2003; Proactive security management software and services; "bv-Control: the security solution to manage within and between organizations"; <http://www.bindview.com>.

[DERA 03] DERAISON, R.; 2003; Nessus Security Scanner; "What is Nessus Security Scanner?"; <http://www.Nessus Security Scanner.org/intro.html>.

[ISSN 03] INTERNET SECURITY SYSTEMS; 2003; Internet Security Systems; "ISS"; <http://www.iss.net>.

[MITR 03] THE MITRE CORPORATION; 2003; Common Vulnerabilities and Exposures (CVE); "CVE, The Key to Information Sharing"; <http://www.cve.mitre.org/introduction.html>.

[NETI 03] NETIQ; 2003; Products and Solutions; "Security Analyzer"; <http://www.netiq.com>.

[SAIN 03] SAINT CORPORATION; 2003; About SAINT; "SAINT 4 Vulnerability Assessment Tool"; <http://www.saintcorporation.com>.

[SCHN 00] SCHNEIER, B.; 2000; Secrets and Lies – Digital Security in a Networked World; "Intrusion Detection Systems"; pp. 194-197; John Wiley & Sons Inc.; ISBN 0-471-25311-1.

[TALI 00] TALISKER; 2000; Network Vulnerability Scanners; "Nessus"; [http://www.networkintrusion.co.uk/N\\_scan.htm](http://www.networkintrusion.co.uk/N_scan.htm).

[VEE1 03] VENTER, H.S.; ELOFF; J.H.P.; 2003; Computers & Security; "A Taxonomy for Information Security Technologies"; Elsevier Science; ISSN 0167-4048.

[VEE2 03] VENTER, H.S.; ELOFF; J.H.P.; 2003; South African Computer Journal; "Harmonised Vulnerability Categories"; pp. 24-31; No. 29; Computer Society of South Africa South Africa; ISSN 1015-7999.