Evaluating Vulnerability Scanners Using Harmonised Vulnerability Categories

HS Venter[a] JHP Eloff[b]

Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa
[a]hventer@cs.up.ac.za, [b]eloff@cs.up.ac.za

Abstract

The focus of this paper is to give an overview of current vulnerability detection and vulnerability scanner (VS) products. Since each VS product available on the software market today is developed by a separate vendor, there are significant differences in these VS products. Some VS products can detect more vulnerabilities than others. Some VS products can detect certain vulnerabilities while other VS tools may detect different vulnerabilities. Furthermore, the modus operandi of exactly how vulnerabilities are detected may also differ from one VS product to another. Due to these issues it is difficult to study the differences between these VS products especially when an organisation has to choose which VS product is the right one for their needs. This paper will attempt to point out the differences between some VS products available today by using the concept of harmonised vulnerability categories. These harmonised vulnerability categories attempt to represent the entire population of vulnerabilities as currently known. One of the advantages of using these harmonised vulnerability categories, for example, is to point out whether or not a specific VS product is able to detect specific kinds of vulnerabilities. This paper, therefore, shows salient results of how harmonised vulnerability categories can be used as an evaluation tool for VS products.

Keywords: *harmonised vulnerability categories, vulnerability, vulnerability scanner (VS), vulnerability mapping, VS product evaluation and vulnerability assessment.*
Computing Review Categories: *C.2, H.1.1, K.6.5, D.4.6, K.4.2*

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 [10]. 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 [1].

The focus for this paper, however, is to develop a better understanding of 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 [7]. In other words, vulnerability scanning refers to the application of state-of-the-art information security technology to secure information on the Internet [10].

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** [11], as shown in table 1. 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.

2 VS Products

It is important to be aware of the different VS products available on the software market before studying some of

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

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 five well-known VS products available today in no particular order of preference.

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) [6] 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" [9]. 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.

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 [4] 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 vul-

Table 2: VS products

VS product	Commercial or freeware	Reference
bv-Control	Commercial	[2]
Internet Security Scanner (ISS) 6.2.1	Commercial	[4]
Nessus Security Scanner	Freeware	[3]
Security Administrator's Integrated Network Tool (SAINT) 4.0	Commercial	[6]
Security Analyzer 5.1	Commercial	[5]

nerability 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, often being hundreds of pages long.

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 [8]. 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 [3] 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 co-operate 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 [11], a measure is available to identify how the different VS products comply with harmonised vulnerability categories.

Modem detected and active (Active Modem)

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: 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.
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.

References: **ISS X-Force**
Modem detected and active
http://xforce.iss.net/static/1292.php

Figure 1: An extract from the ISS report

Figure 2 shows a mapping, compiled during this research project, 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.

In summary, table 3 provides an overview of how the SAINT, the ISS, and the Nessus Security Scanner cover the harmonised vulnerability categories. Using such criterion as shown in table 3, an organisation will be able to identify which VS product is best suited for their needs. An organisation's needs may differ from one organisation to the next in terms of which harmonised vulnerability categories are more fatal to control in their specific environment. Consider, for example, the banking industry: they would typically be more concerned with vulnerabilities in the "backdoors, Trojans and remote controlling" harmonised vulnerability category than some of the other harmonised vulnerability categories and would, therefore, opt to choose either ISS or Nessus Security Scanner. The criterion in table 3 would also be useful for VS product vendors so that they can identify the trends of how their VS product may compete against other VS products on the market according to the harmonised vulnerability categories. Such VS product vendors may then potentially adjust their VS product in a bid to detect more vulnerabilities in a specific harmonised vulnerability category, whatever their potential clients' needs may be.

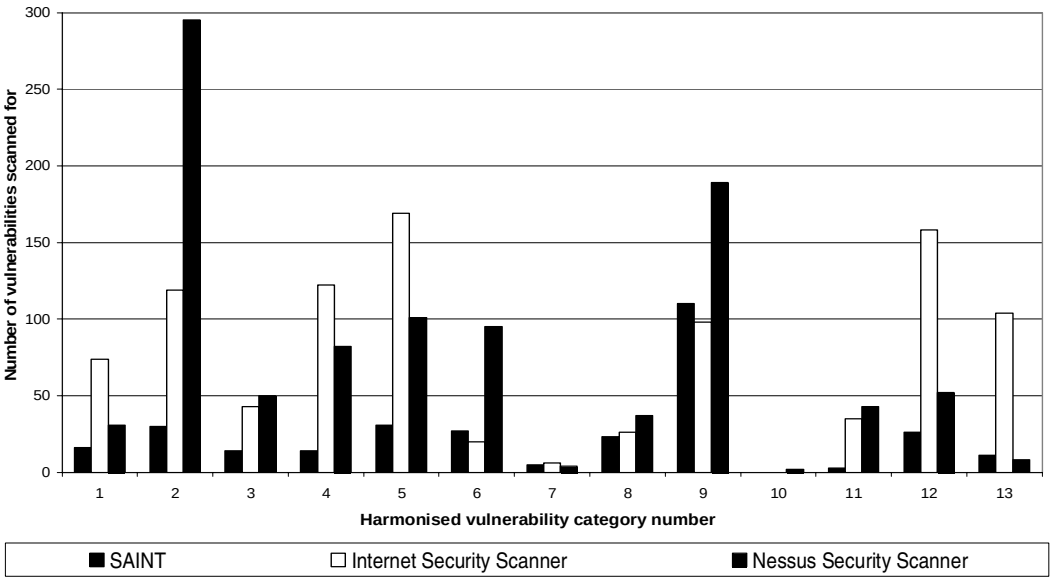

Figure 2: Vulnerability mapping of different VS products onto the harmonised vulnerability categories

4 Conclusion

This paper discussed different VS products and looked at how each respective product differs in the way that they can scan for vulnerabilities.

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. Using harmonised vulnerability categories, furthermore, proved to be a useful tool when evaluating different VS products.

References

[1] R.G. Bace. *Intrusion Detection*, pages 37–43. Macmillan Technical Publishing, 2000. ISBN 1-57870-185-6.

[2] Bindview Corporation. bv-Control: the security solution to manage within and between organizations, 2003. Proactive security management software and services; http://www.bindview.com.

[3] R. Deraison. What is Nessus Security Scanner?, 2003. Nessus Security Scanner; http://www.Nessus Security Scanner.org/intro.html.

[4] Internet Security Systems. ISS, 2003. Internet Security Systems; http://www.iss.net.

[5] NetIQ. Security Analyzer, 2003. Products and Solutions; http://www.netiq.com.

[6] Saint Corporation. SAINT 4 Vulnerability Assessment Tool, 2003. About SAINT; http://www.saintcorporation.com.

[7] B. Schneier. *Secrets and Lies – Digital Security in a Networked World*, pages 194–197. John Wiley & Sons Inc., 2000. ISBN 0-471-25311-1.

[8] Talisker. Nessus, 2000. Network Vulnerability Scanners; http://www.networkintrusion.co.uk/N_scan.htm.

[9] The Mitre Corporation. CVE, The Key to Information Sharing, 2003. Common Vulnerabilities and Exposures (CVE); http://www.cve.mitre.org/introduction.html.

[10] H.S. Venter and J.H.P Eloff. A Taxonomy for Information Security Technologies. *Computers & Security*, 2003. ISSN 0167-4048.

[11] H.S. Venter and J.H.P Eloff. Harmonised Vulnerability Categories. *South African Computer Journal*, 29(1):24–31, 2003. ISSN 1015-7999.

Table 3: Coverage of harmonised vulnerability categories by the discussed VS products

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