During the penetration test, the test team may have uploaded tools and scripts to your servers. The team should have kept a log of all test activities undertaken (see above) and should therefore provide you with sufficient information to enable an easy clean up of your systems.

Reporting

The final report is the testers' main output to you, the hiring organization. It therefore makes to sense to view sample reports before deciding on your supplier. As a minimum the report should contain:

- Details of tests carried out (whether successful or not).
- Full details of successful attacks – containing enough information to enable you to repeat the tests if necessary.
- Evidence of intrusion (screenshots, files grabbed etc.).
- Complete recommendations for remedial actions — including links to hotfixes and patches where necessary.

Penetration testing is a good way of proving the security of your systems. With careful planning you will achieve useful results and make a real improvement to your security. Without careful planning you could end up no better off, and with a bunch of broken systems into the bargain!

paul.midian@insight.co.uk

Assessment Of Vulnerability Scanners

H.S. Venter and J.H.P. Eloff

Securing information over the Internet can be facilitated by a multitude of security technologies. Technologies such as intrusion detection systems, anti-virus software, firewalls and crypto devices have all contributed significantly to the security of information. This article focuses on vulnerability scanners (VSs). A VS has a vulnerability database containing hundreds of known vulnerabilities, which it scans for. VSs do not scan for the same type of vulnerabilities since the vulnerability databases for each VS differ extensively. In addition, there is an overlap of vulnerabilities between the vulnerability databases of various VSs. The concept of harmonised vulnerability categories is introduced in this paper. Harmonised vulnerability categories consider the entire scope of known vulnerabilities across various VSs in a bid to act as a mediator in assessing the vulnerabilities that VSs scan for. Harmonised vulnerability categories, thus, are used to do an objective assessment of the vulnerability database of a VS.

Introduction

Any security professional will agree that security, and specifically Internet security, is a cumbersome topic that gets worse each day. With the advent of the Internet, computer hardware and software started to play an integral part in Internet security. Unfortunately, as the Internet kept on expanding, weaknesses in hardware and software applications became evident. These hardware and software weaknesses are referred to as vulnerabilities since such weaknesses, once they are discovered, are exploited by computer hackers and, thus, are vulnerable to attack.

The risk of being attacked, however, can always be minimised by using state-of-the-art security technologies, for example, firewalls, anti-virus software, intrusion detection systems (IDSs) and vulnerability scanners (VSs). Although these security technologies evolved with great success over recent years in combating attacks on computers and networks, they still fall short in many ways. Examples include too many false alarms detected by IDSs, responses are not prompt, too much redundant work is done and huge reports are generated[1]. Furthermore, firewalls are not intelligent enough and require too much user input so that they can be configured correctly. The problem with anti-virus software is that it has to be kept up-to-date. Amongst other problems, the predominant problems with VSs is the large amount of time involved in conducting VS scans and responding to the scans as well as the degradation of system performance whilst conducting VS scans.

The relationship between intrusion detection system (IDS) and VS technologies is an interesting one and needs to be expanded on. An IDS is a piece of software or hardware that monitors the events occurring in a computer system, also referred to as a host, or network. The IDS analyzes events detected with the aim of identifying signs of intrusions[2]. IDS technology, thus, works in a reactive manner. This means that these technologies will detect possible attacks and attempt to react on such attacks as soon as they occur. Often when an attack

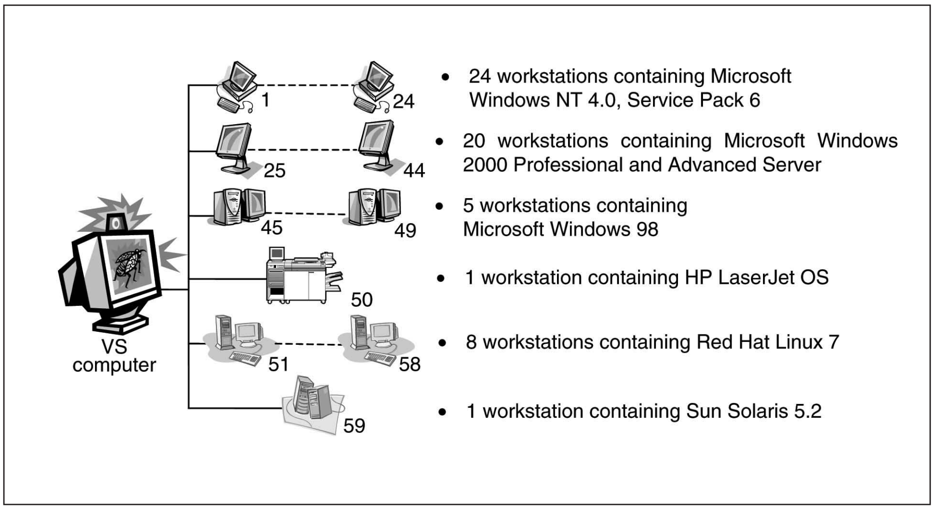

1
24
• 24 workstations containing Microsoft Windows NT 4.0, Service Pack 6
25
44
• 20 workstations containing Microsoft Windows 2000 Professional and Advanced Server
45
49
• 5 workstations containing Microsoft Windows 98
50
• 1 workstation containing HP LaserJet OS
VS computer
51
58
• 8 workstations containing Red Hat Linux 7
59
• 1 workstation containing Sun Solaris 5.2

Figure 1: Case scenario environment and configuration

occurs, however, it is too late to react. VSs, on the other hand, attempt to secure computers in a proactive manner. This means that VSs scan for vulnerabilities in a bid to find them before they occur. The unique proactive nature of VSs inspired the authors to focus specifically on VSs for this research project.

The International Standards Organisation (ISO) defines VSs, also referred to as vulnerability assessment technologies, as the type of technologies allowing an organization to find vulnerabilities, and in most cases recommend corrective actions, before the intruder has an opportunity to exploit them. The relationship between IDS and VS technologies can therefore be summarized by saying that VSs can significantly reduce the number of attacks that an IDS looks for[2].

The current state of VS technologies, the scope of commercially available products and the differences regarding which types of vulnerabilities to scan for, hinders VS technology from developing into a mature information security technology.

Current state-of-the-art VS technologies differ extensively from each other in the sense that they do not necessarily scan for similar vulnerabilities on a host. For example, one VS might scan for 10 vulnerabilities defined for password sniffing, whereas another VS might only scan for three vulnerabilities defined for password sniffing. The number of vulnerabilities in the vulnerability databases of comparable VSs differs significantly, however, the mismatch regarding the types of vulnerabilities between the vulnerability databases of comparable VSs, is even more important.

The best way for an organization to determine whether a specific VS would fulfil the VS needs of the organization, is to assess the vulnerability databases of various VSs in a bid to identify which type of vulnerabilities each specific VS scans for. But which criteria should be used when assessing the vulnerability databases of various VSs? Some organizations could argue that their needs require VSs with strong features in detecting hardware vulnerabilities. Others might argue that their needs require VSs that are capable of detecting software or networking vulnerabilities. An organization might also consider acquiring more than one VS in a bid to detect vulnerabilities that another VS would not necessarily be able to detect. For example, VS X might detect many remote procedure call vulnerabilities on the network level, while VS Y might detect many password guessing and grinding vulnerabilities on the host level. Various VSs might even address the same kind of vulnerability in a different way, for example one VS might audit passwords by using a dictionary attack, whereas another VS might audit passwords by using a brute-force attack. Before an organization is able to decide which VS would fulfil its needs in the best way, some "harmonised" vulnerability categories need to be specified to have an unbiased method in assessing various VSs. Harmonised vulnerability categories represent the entire scope of vulnerabilities across various VSs.

A list of harmonised vulnerability categories were identified, as shown in Table 1, through comprehensive research that was conducted from current literature, current VSs, and the Internet[3]. It should be mentioned that these harmonised vulnerability categories may be subject to change in the future as new types of vulnerabilities emerge, however, these 13 harmonised vulnerability categories represent the entire range of vulnerabilities

Table 1: Harmonised vulnerability categories

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

that are currently known. The order in which the harmonised vulnerability categories are displayed in Table 1 and the category numbers are of no significant value.

For the rest of this article, only the category numbers are displayed to indicate the different vulnerability categories. The next section presents a case scenario in which the vulnerability databases of two specific VSs, CyberCop Scanner[4] and Cisco Secure Scanner[5], are assessed. Other well-known and widely used VSs include Nessus[6] and NMap[7], however, these VSs will not be discussed here

The assessment is facilitated by means of the harmonised vulnerability categories. Note that these two VSs are not explicitly compared with each other, but specifically the vulnerabilities in their vulnerability databases are assessed against the harmonised vulnerability categories.

Using harmonised vulnerability categories to assess vulnerabilities

A case scenario

CyberCop Scanner and Cisco Secure Scanner were used to scan workstations in an environment with multiple configurations and platforms. This scan scenario is shown in Figure 1 with the following configuration:

- The scan was performed using CyberCop Scanner version 5.5 and Cisco Secure Scanner version 2.0.1.2, both installed on an Intel Pentium III, 750 MHz computer with 128MB memory running on a Windows 2000 platform.
- The scan was performed on a network containing 59 workstations. These workstations included various platforms, as shown in Figure 1.

CyberCop scanner results

After CyberCop Scanner completed the scan, it generated a report. The following results were observed in this report:

- The scan duration was two hours and 12 minutes.
- A report of 405 pages was generated. Figure 2 shows an extract of one of the vulnerabilities in this report.

The following advantage and disadvantages of the report were identified:

Advantage

- Good and detailed description and rectification procedures that are aimed specifically at one or more technical assistants.

Disadvantages

- This report is too long and will take days for one or even a few people to study.
- The report is very technical and requires skilled human resources to rectify the vulnerabilities.
- Of the 13 harmonised vulnerability categories in Table 1, categories 3, 4, 7, 10 and 11 are covered in very little detail, if at all, by CyberCop Scanner for this specific scan, as shown in Table 2.
- The report does not prioritise the vulnerabilities detected.

Cisco Secure Scanner results

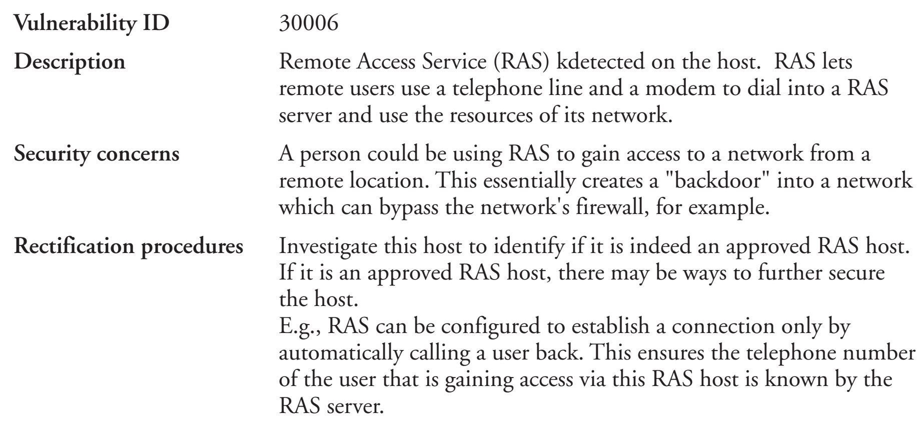
Cisco Secure Scanner created a report after the scan was completed and the following observations are made from this report:

- The scan duration was 33 minutes and 47 seconds.
- A report of 78 pages was generated.

Table 2: CyberCop Scanner harmonised vulnerability categories

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

Figure 2: An extract from the CyberCop Scanner report



Vulnerability ID	30006
Description	Remote Access Service (RAS) kdetected on the host. RAS lets remote users use a telephone line and a modem to dial into a RAS server and use the resources of its network.
Security concerns	A person could be using RAS to gain access to a network from a remote location. This essentially creates a "backdoor" into a network which can bypass the network's firewall, for example.
Rectification procedures	Investigate this host to identify if it is indeed an approved RAS host. If it is an approved RAS host, there may be ways to further secure the host. E.g., RAS can be configured to establish a connection only by automatically calling a user back. This ensures the telephone number of the user that is gaining access via this RAS host is known by the RAS server.

Table 3: Cisco Secure Scanner harmonised vulnerability categories

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

Figure 3 shows an extract of one of the vulnerabilities in this report.

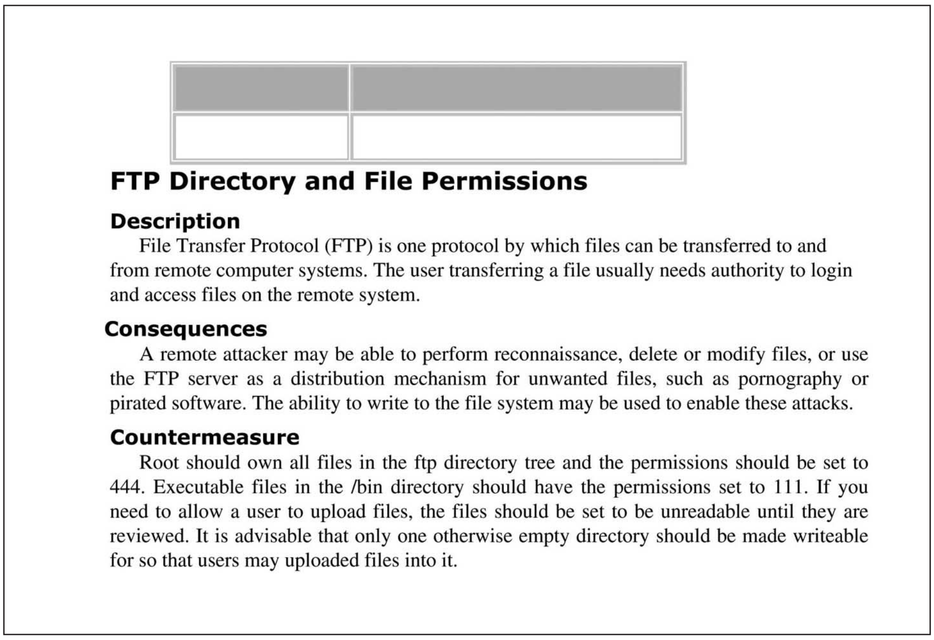
The following advantages and disadvantages of the report were identified:

Advantages

- The report contains good and detailed description, consequences and countermeasure procedures that are aimed specifically at technical assistants.

Disadvantages

- It requires effort to work through the complete Cisco Secure Scanner report owing to its large size.
- Of the 13 harmonised vulnerability categories in Table 1, categories 3, 4, 7, 8, 10, 11, 12 and 13 are covered in very little detail, if at all, by Cisco Secure Scanner for this specific scan, as shown in Table 3.



FTP Directory and File Permissions

Description

File Transfer Protocol (FTP) is one protocol by which files can be transferred to and from remote computer systems. The user transferring a file usually needs authority to login and access files on the remote system.

Consequences

A remote attacker may be able to perform reconnaissance, delete or modify files, or use the FTP server as a distribution mechanism for unwanted files, such as pornography or pirated software. The ability to write to the file system may be used to enable these attacks.

Countermeasure

Root should own all files in the ftp directory tree and the permissions should be set to 444. Executable files in the /bin directory should have the permissions set to 111. If you need to allow a user to upload files, the files should be set to be unreadable until they are reviewed. It is advisable that only one otherwise empty directory should be made writeable for so that users may uploaded files into it.

Fig. 3: An extract from the Cisco Secure Scanner report

When observing the results of CyberCop Scanner and Cisco Secure Scanner, one should realise that there are many shortcomings in current VSs. One of the most important harmonised vulnerability categories, viruses and worms, is not addressed at all by the vulnerability databases of the two assessed technologies. Current viruses and worms are dynamic in the sense that they spread through email and networks. Therefore current viruses should be considered as intrusive objects and should be incorporated into VS technologies nowadays. It should be a major concern for VS technology vendors to merge the virus scanning technology with VSs. In addition, the reports are not sufficient in the world of interconnectivity today because it takes up too much time for a person to study them in order to identify the weak security spots in an organization's network. The reports also represent mere history rather than an outlook on the future security status of the organization's hosts.

The biggest concern is that the two VSs do not consider each harmonised vulnerability category in the same level of detail. For example, CyberCop Scanner is able to scan for approximately 260 vulnerabilities in harmonised vulnerability category 8 (misconfigurations), whereas Cisco Secure Scanner scans for approximately 10 vulnerabilities in the same category. In addition, the two VSs refer differently to the same harmonised vulnerability category. For example, CyberCop Scanner defines certain vulnerability categories, i.e. "Information Gathering" and "Windows NT Information Gathering". Cisco Secure Scanner, on the other hand, does not group vulnerabilities in vulnerability categories. Finding the vulnerabilities in Cisco Secure Scanner's vulnerability database that correspond to the vulnerability database of CyberCop Scanner is, thus, a very confusing and difficult task when manually trying to match the types of vulnerabilities of both VSs.

The problems with assessing the VSs as described above can be addressed by using harmonised vulnerability categories. Harmonised vulnerability categories address the entire scope of vulnerabilities, categorised in relevant

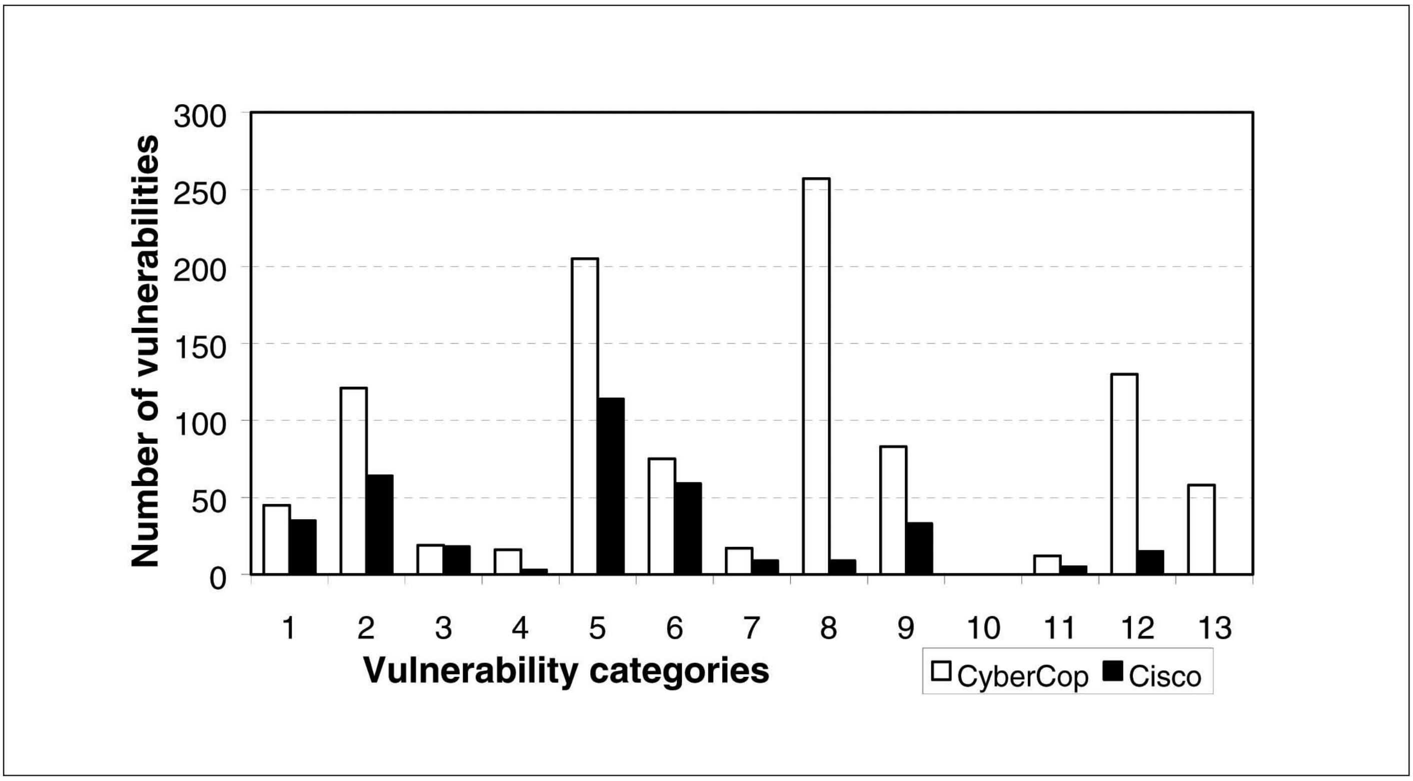


Figure 4: Adherence of CyberCop Scanner and Cisco Secure Scanner to the 13 harmonised vulnerability categories

vulnerability categories. The vulnerabilities of two or more VSs can then be mapped to the harmonised vulnerability categories for each VS respectively.

It is clear from the above that harmonised vulnerability categories can be helpful when assessing the vulnerability categories of various VSs. It is for this reason that the authors mapped the vulnerabilities found in both VSs assessed, onto the 13 harmonised vulnerability categories. These results are discussed in the next section.

Assessment of CyberCop Scanner and Cisco Secure Scanner using the 13 harmonised vulnerability categories

It is necessary to first get an idea of how CyberCop Scanner and Cisco Secure Scanner adhere to the 13 harmonised vulnerability categories according to the vulnerability databases of each. This is done by mapping the vulnerabilities of each VS, as contained in the vulnerability databases of each specific VS, to the 13 harmonised vulnerability categories. The CyberCop Scanner vulnerability database adheres mainly to eight of the 13 harmonised vulnerability categories, as shown in Figure 4. These categories are 1 - password cracking and sniffing, 2 - network and system information gathering, 5 - unauthorized access to remote connections and services, 6 - privilege and user escalation, 8 - misconfigurations, 9 - denial-of-service and buffer overflows, 12 - software-specific updates, and 13 - security policy violations. Cisco Secure Scanner's vulnerability database adheres mainly to five of the 13 harmonised vulnerability categories as shown in Figure 4. These categories are as follows:

1 - password cracking and sniffing, 2 - network and system information gathering, 5 - unauthorized access to remote connections and services, 6 - privilege and user escalation, and 9 - denial-of-service and buffer overflows.

It is interesting to note the differences in the number of vulnerabilities for categories 2, 5, 8, 9, 12 and 13 between CyberCop Scanner and Cisco Secure Scanner in Figure 4. Consider harmonised vulnerability category 8, misconfigurations, for example. CyberCop Scanner can potentially detect approximately 260 misconfiguration vulnerabilities, whereas Cisco Secure Scanner can detect about 10. The fact that there is a big difference in the number of vulnerabilities that these two VSs can potentially detect, however, does not necessarily mean that there is a big difference in the quality of the technologies. The vulnerability databases of many VSs available on the market are simply updated and the old and redundant vulnerabilities are not removed. The aim of Figure 4, therefore, is to show where the concentration point of vulnerabilities for a specific VS lies, rather than to compare the results of the two VSs in Figure 4 directly with each other. It is clear that these two VSs focus almost on the same vulnerabilities, except for harmonised vulnerability categories 8 and 12. When assessing the two VSs over a real scenario, the results better indicate what the abilities of the two VSs are in detecting vulnerabilities. A representation of the scan results for each specific VS is shown in Figure 5.

Figure 5 shows how many vulnerabilities were found in specific scans by CyberCop Scanner and Cisco Secure Scanner, respectively, for each of the 13

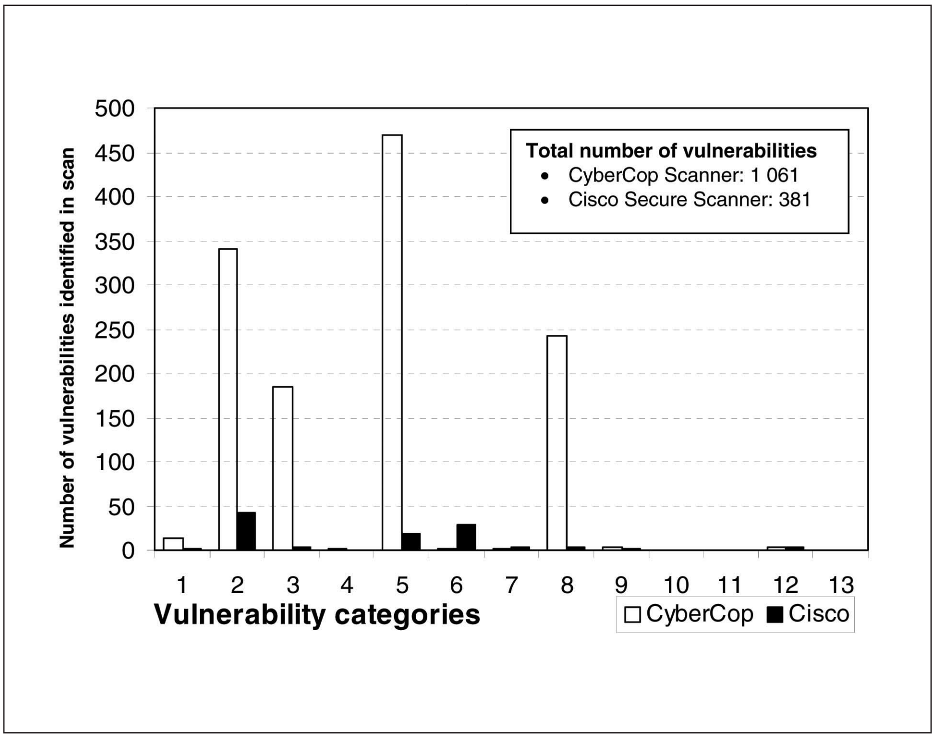


Figure 5: CyberCop Scanner and Cisco Secure Scanner scan results for the specific scenario

harmonised vulnerability categories. By looking at Figure 5, one is able to view the overall picture of the organization's security status by identifying the vulnerability 'problem areas' on an organization's hosts. It is clear that category 2 - network and system information gathering and category 5 - unauthorized access to remote connections and services are identified as vulnerability problem areas, because the most vulnerabilities that were found in this specific scenario by both VSs belong to categories 2 and 5.

It should be stressed again that, although the size of the vulnerability databases of the two VSs differ significantly, the aim is to assess the vulnerabilities in the vulnerability databases of VSs against the harmonised vulnerability categories. An organization might also consider using more than one specific VS in a bid to detect as many as possible vulnerabilities. For example, Cisco Secure Scanner covers harmonised vulnerability categories 6 and 7 well, whereas CyberCop Scanner covers harmonised vulnerability categories 1, 2, 3, 5, and 8 well.

The final outcome of this assessment against the harmonised vulnerability categories is to identify where the focal points of a specific VS lies in terms of the harmonised vulnerability categories, and then to assess that against the unique information security needs of the organization. In other words, an organization will be able to tell how their information security needs are addressed by a specific VS. It might also be the case that an organization is only interested in a subset of the proposed 13 harmonised vulnerability categories. If the organization might find that a specific VS does not meet their information security needs, they should consider using an alternative VS, or a combination of VSs in a bid to cover their needs.

Conclusion

Choosing the right VS for a specific organization's interconnected environment is critical.

Instead of traversing all the vulnerabilities in the huge reports in a bid to determine which VS to use, organizations can adopt harmonised vulnerability categories to assess the vulnerability databases of different vulnerability scanners.

A solution to the problem — that of assessing VSs which differ extensively regarding the vulnerabilities in their respective vulnerability databases — has been found. Utilising harmonised vulnerability categories will now enable an organization to have an unbiased view of different vulnerability scanners.

Department of Computer Science
University of Pretoria, 0002, Pretoria, South Africa
Tel: +27 12 420-2361
email HS Ventor — hventer@cs.up.ac.za
Jan Eloff — eloff@cs.up.ac.za

References

[1]SCHNEIER, B.; 2000; Secrets and Lies, Digital Security in a Networked World; "Intrusion Detection Systems"; John Wiley & Sons Inc.;

[2]BRACKNEY, D.; 2002; ISO/IEC WD 18043 (SC27 N 3180); "Guidelines for the implementation, operation and management of intrusion detection systems".

[3]VENTER, H.S.; ELOFF, J.H.P.; December 2002; Computers & Security; "What are the vulnerabilities that we are looking at today?"; Elsevier Science; ISSN 0167-4048.

[4]NETWORK ASSOCIATES; 2002; PGP Securities; "CyberCop Monitor"; http://www.pgp.com/products/cybercop-monitor/default.asp.

[5]CISCO SYSTEMS, INC.; 2000; Cisco Secure Scanner; Version 2.0.1.2; http://www.cisco.com.

[6]DERAISON, R.; 2002; Nessus; "What is Nessus?"; http://www.nessus.org/intro.html.

[7]VASKOVICH, F.; 2002; Insecure.org; "Nmap"; http://www.insecure.org/nmap/index.html#intro.

BACE, R.G.; 2000; Intrusion Detection; "Password-Cracking"; Macmillan Technical Publishing; ISBN 1-57870-185-6; pp. 3, 31, 136, 150-151, 179, 279-280.

SECURITYFOCUS.COM; 2002; Bugtraq; "Bugtraq Archives"; http://www.securityfocus.com/forums/bugtraq/intro.html.