Comparing Intrusion Detection Tools Using Generic Vulnerability Categories

H.S. VENTER (heins@adam.rau.ac.za)
J.H.P. ELOFF (eloff@rkw.rau.ac.za)
Department of Computer Science
Rand Afrikaans University
PO Box 524
AUCKLAND PARK
2006
South Africa
July 2002
Tel: +27 11 489-2847   Fax: +27 11 489-2138

Key words: Intrusion detection system (IDS), generic vulnerability categories, network security.

Abstract: Any organisation connected to the Internet that is serious about security cannot be without an intrusion detection system (IDS) these days. Is one IDS sufficient to cover all possible vulnerabilities in a network? In a sea of security products available today, which IDS tool(s) will be sufficient for your organisation's needs? The only way to find out is to compare various IDS tools with each other. But how? Each IDS tool has a vulnerability database containing hundreds of known vulnerabilities it scans for to resolve the vulnerabilities it has found. Not one IDS tool contains the same number of vulnerabilities it scans for. In addition, many vulnerabilities that are present in the vulnerability database of a specific IDS are also present in the vulnerability databases of other IDS tools. In other words, many IDS tools scan for the same vulnerabilities. On the other hand, certain IDS tools scan for unique vulnerabilities. This paper suggests the method of using generic vulnerability categories, which may act as a standard in comparing IDS tools.

1. INTRODUCTION

Any security professional will agree that security, and specifically Internet security, is a cumbersome topic that gets worse each day as the Internet keeps expanding. When is it going to stop? The bad news is – probably never! But there is good news…

The risk of being attacked can always be minimised by using state-of-the-art security utilities, for example firewalls, up-to-date virus detectors and intrusion detection systems (IDSs). Although IDSs are more advanced security tools than the others mentioned here, they still fall short in many ways. Examples include too many false alarms, responses are not prompt, too much redundant work and the huge reports generated [SCHN 00].

Recent research conducted [VENT 02] shows that various IDS tools differ extensively in the sense that they do not address and check for the same kind of problem areas, referred to as vulnerabilities, in a network, a host or a certain platform. For example, some IDS tools are marketed for the fact that they check for vulnerabilities at host or application level, whereas other IDS tools check for vulnerabilities at network level or on a specific target. An example of a host-level vulnerability is a badly chosen password. An example of a network-level vulnerability includes the ability to trace a route to a specific host. In addition, IDS tools do not all check for exactly the same vulnerabilities because the number of vulnerabilities that each IDS tool scans for differs for each IDS tool. For example, one IDS tool might have 10 vulnerabilities defined for password sniffing, whereas another might only have 3.

Which IDS tool, then, should **you** use? Which one is the best? The best way for an organisation to determine which IDS tool(s) would benefit it the most is to compare IDS tools with each other. But which criteria should be used? Some could argue that IDS tools available on the market with strong features in hardware and technology should be considered as major criteria. Others might argue that software and networking capabilities are more important to them. An organisation might also consider having more than one IDS tool to have a combination of the best qualities from various IDS tools. For example, IDS tool X might perform well at network level, but IDS tool Y might perform well at host level. Various IDS tools might even address the same kind of vulnerability in a different way, for example one IDS tool might audit passwords by using a dictionary attack, whereas another might audit passwords by using a brute-force attack. Whatever the organisation's need may be, some generic vulnerability categories need to be in place to have a generic measurement tool in comparing various IDSs.

These vulnerability categories (shown in table 1) have been identified in previous research by the authors [VENT 02].

Table 1. The 13 generic vulnerability categories

Generic vulnerability category number	Generic 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 / 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

In the sections that follow, only the category numbers are shown. The next section presents a case scenario in which two specific intrusion detection tools, CyberCop Scanner [CYBE 02] and Cisco Secure Scanner [CSSC 00], are compared to the 13 vulnerability categories as shown in table 1. In appendix A, a more detailed study of CyberCop Scanner and Cisco Secure Scanner is shown for an overview of how current IDSs work, what kinds of vulnerabilities they detect and to what degree they detect them.

2. 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 fig. 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 Microsoft Windows 2000 platform. (See the IDS computer in fig. 1.)

- The scan was performed on a subnet containing 59 workstations. These workstations included various platforms, as shown in fig. 1.

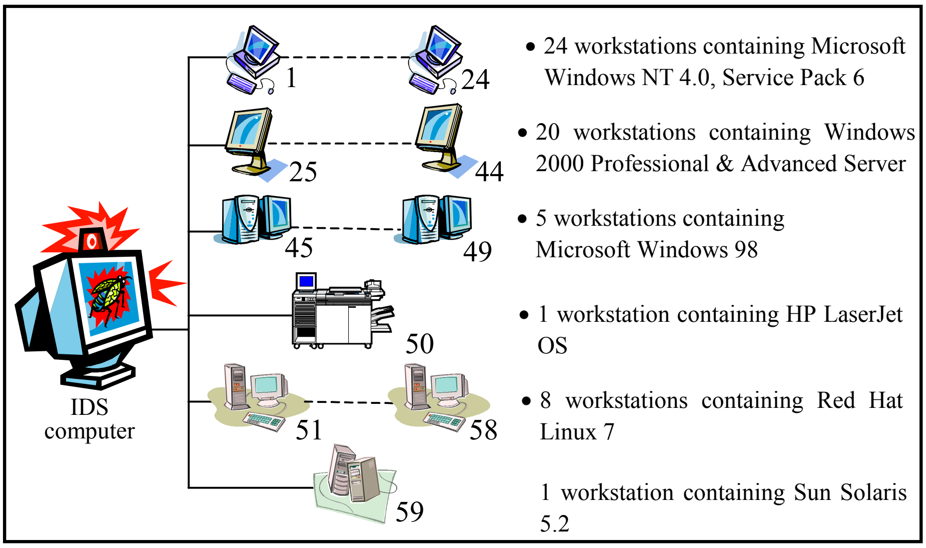

1
24
• 24 workstations containing Microsoft Windows NT 4.0, Service Pack 6
25
44
• 20 workstations containing Windows 2000 Professional & Advanced Server
45
49
• 5 workstations containing Microsoft Windows 98
IDS computer
50
• 1 workstation containing HP LaserJet OS
51
58
• 8 workstations containing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

Figure 1. Case scenario environment and configuration

On completion of the scan, CyberCop Scanner and Cisco Secure Scanner reported results, as shown in the following section.

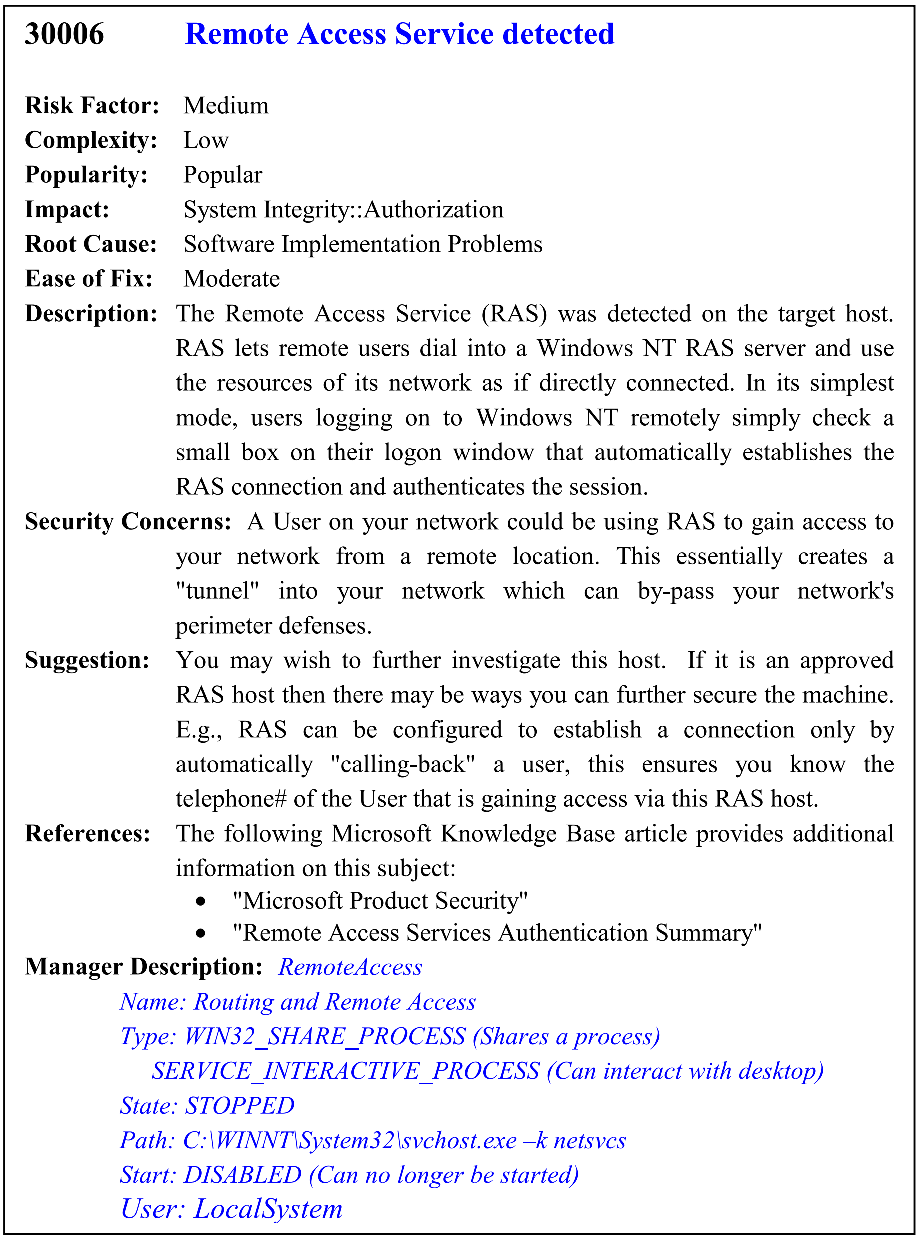
2.1 Viewing the Scanners' Results

2.1.1 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 2 hours and 12 minutes.
- A report of 405 pages was generated. Fig. 2 shows an extract from 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.



30006 **Remote Access Service detected**

Risk Factor: Medium
Complexity: Low
Popularity: Popular
Impact: System Integrity::Authorization
Root Cause: Software Implementation Problems
Ease of Fix: Moderate

Description: The Remote Access Service (RAS) was detected on the target host. RAS lets remote users dial into a Windows NT RAS server and use the resources of its network as if directly connected. In its simplest mode, users logging on to Windows NT remotely simply check a small box on their logon window that automatically establishes the RAS connection and authenticates the session.

Security Concerns: A User on your network could be using RAS to gain access to your network from a remote location. This essentially creates a "tunnel" into your network which can by-pass your network's perimeter defenses.

Suggestion: You may wish to further investigate this host. If it is an approved RAS host then there may be ways you can further secure the machine. E.g., RAS can be configured to establish a connection only by automatically "calling-back" a user, this ensures you know the telephone# of the User that is gaining access via this RAS host.

References: The following Microsoft Knowledge Base article provides additional information on this subject:

- "Microsoft Product Security"
- "Remote Access Services Authentication Summary"

Manager Description: *RemoteAccess*
Name: Routing and Remote Access
Type: WIN32_SHARE_PROCESS (Shares a process)
SERVICE_INTERACTIVE_PROCESS (Can interact with desktop)
State: STOPPED
Path: C:\WINNT\System32\svchost.exe –k netsvcs
Start: DISABLED (Can no longer be started)
User: LocalSystem

Figure 2. An extract from the 405-page CyberCop Scanner report

- 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.
  - The "Manager Description" (fig. 2) is not comprehensible to a manager who does not have the necessary technical skills.
  - One almost gets the impression that such a report contains data rather than information.
  - CyberCop Scanner has the facility to display graphical summary reports. Unfortunately, triggering this feature caused CyberCop Scanner to be invalidly terminated by the system.
  - The report does not intelligently sort or regroup the various vulnerabilities found according to generic vulnerability categories. Grouping the information in the report in this fashion would be very useful when attempting to intelligently identify problem areas in a network.
  - Of the 13 generic 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.

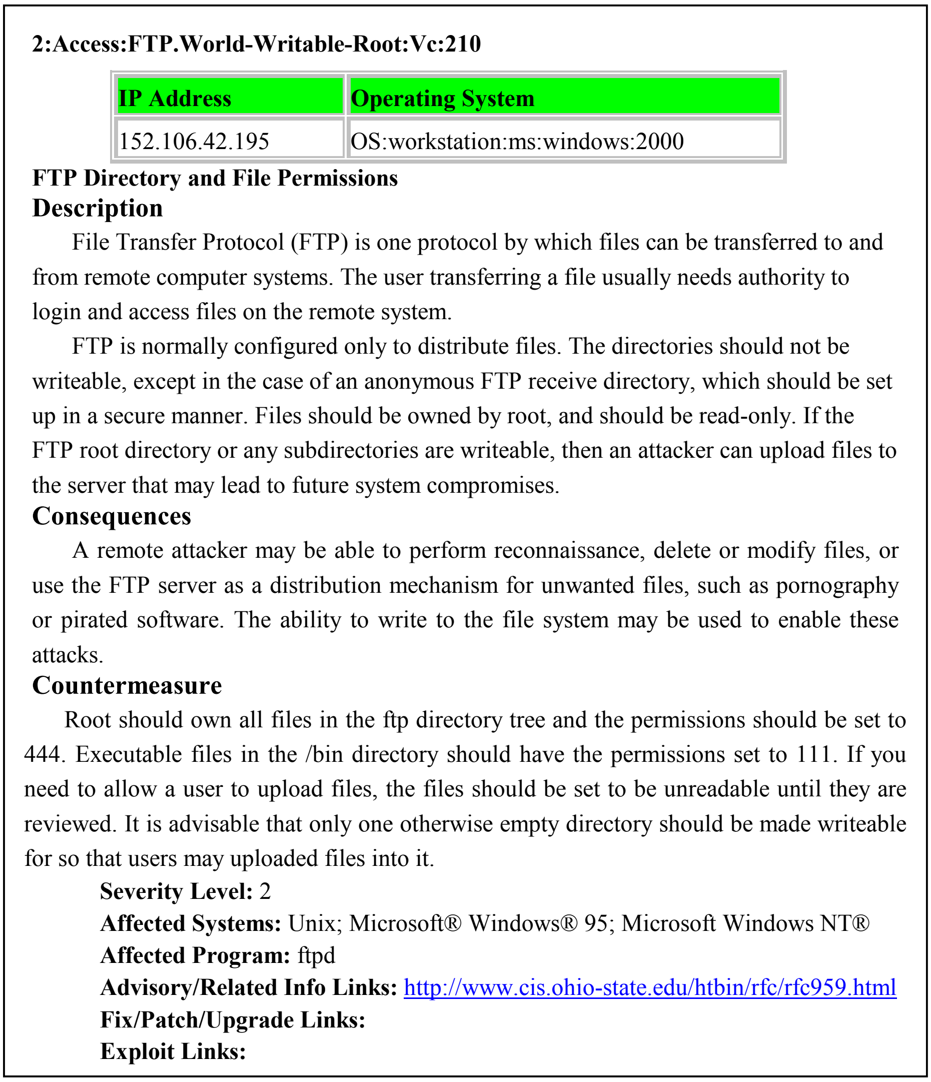
Table 2. The 13 generic vulnerability categories covered by CyberCop Scanner

Generic vulnerability category number	Generic vulnerability category description	CyberCop Scanner
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 / 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	✓

2.1.2 Cisco Secure Scanner Results

The 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. Fig. 3 shows an extract from one of the vulnerabilities in this report.



2:Access:FTP.World-Writable-Root:Vc:210

IP Address	Operating System
152.106.42.195	OS:workstation:ms:windows:2000

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.

FTP is normally configured only to distribute files. The directories should not be writeable, except in the case of an anonymous FTP receive directory, which should be set up in a secure manner. Files should be owned by root, and should be read-only. If the FTP root directory or any subdirectories are writeable, then an attacker can upload files to the server that may lead to future system compromises.

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.

Severity Level: 2
Affected Systems: Unix; Microsoft® Windows® 95; Microsoft Windows NT®
Affected Program: ftpd
Advisory/Related Info Links: http://www.cis.ohio-state.edu/htbin/rfc/rfc959.html
Fix/Patch/Upgrade Links:
Exploit Links:

Figure 3. An extract from the 78-page Cisco Secure Scanner report

- The following advantages and disadvantages of the report were identified:
  - Advantages
    - The report is structured in an HTML web-based format with links.

  - It contains an executive summary section as well as a Cisco Secure Scanner process overview.
  - It also contains good and detailed description, consequences and countermeasure procedures specifically for technical assistants.
  - Furthermore, the report contains graphics, for example charts, that can be customised and included in the report.
- Disadvantages
  - It requires effort to work through the complete Cisco Secure Scanner report owing to its large size.
  - Graphics in the report were not clearly readable.
  - Although an executive summary is given, a manager or executive that reads this summary stills need the necessary technical skills to understand the problems.
  - Of the 13 generic vulnerability categories in table 1, categories 3, 4, 7, 8, 10, 11 and 12 are covered in very little detail, if at all, by Cisco Secure Scanner for this specific scan, as shown in table 3.

Table 3. The 13 generic vulnerability categories covered by Cisco Secure Scanner

Generic vulnerability category number	Generic vulnerability category description	Cisco Sec. Scanner
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 / 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	✓

When observing the results of CyberCop Scanner and Cisco Secure Scanner, one should realise that there are many shortcomings in current IDSs. One of the most important vulnerability categories, viruses and worms, is not addressed at all by the two tools evaluated. It is of utmost importance to have virus detectors incorporated into IDS tools nowadays, since virus and worm attacks currently cause shocking and disastrous effects worldwide and should be a major concern for IDS tool vendors. In addition, the reports are not sufficient in the world of interconnectivity today because it takes too long for a person to study them in order to identify the weak security spots in an organisation's network. The reports also represent mere history rather than an outlook on the future security status of the organisation's network.

Another concern that needs to be mentioned is that the two IDS tools do not consider each generic vulnerability category on the same detail level. For example, CyberCop Scanner is able to check for approximately 250 vulnerabilities in generic vulnerability category 8 (misconfigurations), whereas Cisco Secure Scanner checks for approximately 10 vulnerabilities in the same category. In addition, the two IDS tools refer differently to the same generic vulnerability category. For example, CyberCop Scanner defines certain vulnerability groups, i.e. "Information Gathering" and "Windows NT Information Gathering". Cisco Secure Scanner, on the other hand, also groups certain vulnerabilities together, but these groups do not seem to have names allocated to them. 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 trying to compare the vulnerabilities of both IDS tools.

It is clear from the above that generic vulnerability categories are a must when comparing the vulnerability categories of various IDS tools. It is for this reason that the authors mapped the vulnerabilities found in both IDS tools evaluated here onto the 13 generic vulnerability categories. These results are discussed in the next section.

2.2 Comparison of CyberCop Scanner and Cisco Secure Scanner using the 13 generic vulnerability categories

It is necessary to first get an idea of how CyberCop Scanner and Cisco Secure Scanner adhere to the 13 generic vulnerability categories. This is done by mapping each IDS tool's vulnerabilities to the 13 categories. The CyberCop Scanner vulnerability database adheres sufficiently to only 8 of the 13 vulnerability categories in general, as shown in fig. 4. These categories are 1 – password cracking and sniffing, 2 – network and system information gathering, 5 – unauthorised 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 sufficiently to only 5 of the 13 vulnerability categories (fig. 4). They are categories 1 – password cracking and sniffing, 2 – network and system information gathering, 5 – unauthorised access to remote connections and services, 6 – privilege and user escalation, and 9 – denial-of-service and buffer overflows.

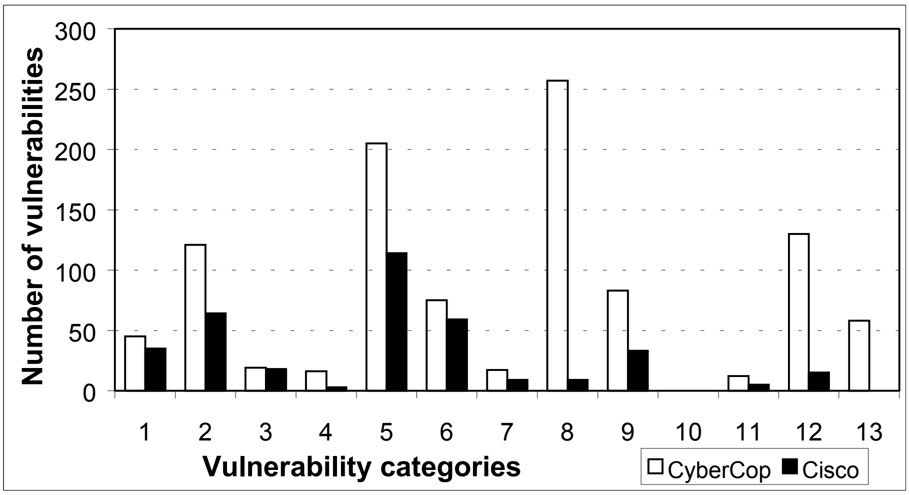


Figure 4. Adherence of CyberCop and Cisco Secure Scanner to 13 vulnerability categories

It is interesting to note the major differences in the number of vulnerabilities for categories 2, 5, 8, 9, 12 and 13 between CyberCop Scanner and Cisco Secure Scanner in fig. 4. Consider vulnerability category 8, misconfigurations, for example. CyberCop Scanner can potentially detect approximately 260 misconfiguration vulnerabilities, whereas Cisco Secure Scanner can detect only about 10. It is clear that the two IDS tools will not be able to detect intrusions at the same level of detail if these different results between the two evaluated IDS tools are considered. The results are even more staggering when comparing the results of a specific scan done by each of these tools over exactly the same scenario. A unique representation for each of the IDS tools' specific scan results is shown in fig. 5.

Fig. 5 shows how many vulnerabilities were found in specific scans by CyberCop Scanner and Cisco Secure Scanner, respectively, for each of the 13 generic vulnerability categories. By looking at fig. 5, one sees the overall picture of the organisation's network security status by identifying the vulnerability "problem areas" in an organisation's network. It is clear that category 2 - network and system information gathering and category 5 - unauthorised access to remote connections and services are definitely identified as vulnerability problem areas, because the most vulnerabilities that were found in this specific scenario belong to categories 2 and 5. Category 3 - user enumeration and information and category 8 - misconfigurations also identify scan problem areas, although not as big as for categories 2 and 5.

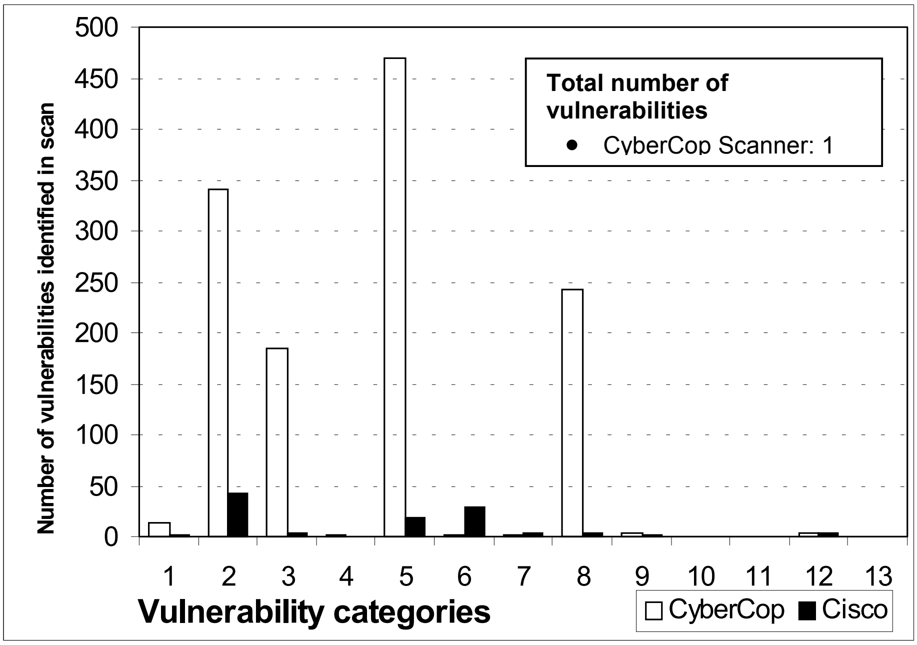


Figure 5. CyberCop Scanner/Cisco Secure Scanner scan results for the specific scenario

There is a significant difference between the CyberCop Scanner and Cisco Scanner scan results. The reason for this is the difference in the size of the two tools' vulnerability databases: remember that CyberCop Scanner has a larger vulnerability database and scans for approximately 700 vulnerabilities, whereas Cisco Secure Scanner scans for only 230 vulnerabilities. Hence, CyberCop Scanner will return more vulnerabilities.

From fig. 5, the following results can also be seen:

- Categories 2 and 5 (network and system information gathering and unauthorised access to remote connections and services) are found to be the major vulnerability problem areas. Management should prioritise the employment of expertise in rectifying problems in these two categories immediately, since they pose the greatest threat.
- Categories 3, 6 and 8 (user enumeration and information, privilege and user escalation and misconfigurations) are found to be the intermediate vulnerability problem areas. Management should employ expertise in rectifying problems in these three categories only once the major vulnerability problem areas are resolved and under control.
- Categories 1, 7, 9 and 12 can be considered as minor vulnerability problem areas and should not pose a real threat to the organisation's network at this stage. These problem areas can be resolved on a low-priority basis, that is, as soon as time allows or expertise becomes affordable or available for this purpose.
- Vulnerabilities from categories 4, 10, 11 and 13 pose no threat at all in this specific scan scenario.

An organisation might take a risk when using only one IDS tool, for example Cisco Secure Scanner, in this case. From the results it is clear that using only Cisco Secure Scanner as a tool would not detect the additional 680 vulnerabilities that CyberCop scanner detected.

Another aspect evident from the scan scenario is that the two tools that were tested did not adhere sufficiently to the 13 vulnerability categories. If no vulnerabilities for categories 4, 10, 11 and 13 (fig. 5) were found in the scan scenario, this does not mean that these categories should be completely ignored. For example, none of the IDS tools evaluated in this paper adhered to category 10, viruses and worms, at all! Therefore category 10 should be tested with additional virus detection software, or better yet, an IDS tool must be used that adheres to this category. The bottom line is that you can use these 13 generic vulnerability categories to test your IDS tools to see how they adhere to the categories. You can also opt to test those categories that are not adhered to.

The only disadvantage in the process of comparing and evaluating IDS tools using the 13 generic vulnerability categories is the mapping of the vulnerabilities from IDS tools onto the 13 generic vulnerability categories. This is, however, a one-off exercise, as the authors have shown in this paper, and should not pose such a great concern.

3. CONCLUSION

Instead of jumping head over heels into the huge reports by traversing all the vulnerabilities in a bid to determine which IDS tool to use, organisations can use the 13 generic vulnerability categories to compare different IDS tools.

Face the facts: Current IDS technology is no longer sufficient in the fast- and ever-changing Internet environment, unless a dramatic breakthrough is made in current IDS technology. Choosing the right IDS(s) for your interconnected environment is therefore very critical. Did you choose the right IDS? Which IDS should you choose? These questions can be answered by using the 13 generic vulnerability categories to compare your IDS tool(s) or desired IDS tool(s) with each other to find out tool(s) would best suit your needs.

4. REFERENCES

[BACE 00] 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.

[BUGT 02] SECURITYFOCUS.COM; 2002; Bugtraq; “Bugtraq Archives”; http://www.securityfocus.com/forums/bugtraq/intro.html.

[CSSC 00] CISCO SYSTEMS, INC.; 2000; Cisco Secure Scanner; Version 2.0.1.2; http://www.cisco.com.

[CYBE 02] NETWORK ASSOCIATES; 2002; PGP Securities; “CyberCop Monitor”; http://www.pgp.com/products/cybercop-monitor/default.asp.

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

[VENT 02] VENTER, H.S.; ELOFF, J.H.P.; April 2002; Computers & Security; “What are the vulnerabilities that we are looking at today?”; Elsevier Science; ISSN 0167-4048.

5. APPENDIX A: BACKGROUND OF CYBERCOP SCANNER AND CISCO SECURE SCANNER

CyberCop Scanner and Cisco Secure Scanner are the two IDSs that were specifically chosen in this study because they are popular, freely available for evaluation, comprehensive and support multiple operating systems. Both tools were evaluated in exactly the same scenario so that results could be compared.

5.1 CyberCop Scanner

CyberCop Scanner [CYBE 02] is a proactive vulnerability scanner tool. It contains a vulnerability database, which contains signatures of vulnerabilities across multiple operating system platforms. These vulnerabilities are known, because they were already exploited and reported by system security checkers, for example administrators or security groups, i.e. Bugtraq [BUGT 02].

The proactive approach that CyberCop Scanner follows can be described as using a predetermined set of "generated" intrusions from its vulnerability database and directing these intrusions to one or more specified hosts on a network [BACE 00]. It then uses a pattern matcher to monitor whether the intrusions were successful. CyberCop Scanner's report generator then generates a report on completion of the scan.

The vulnerability database in CyberCop Scanner is comprehensive, with more than 700 vulnerabilities that it can detect. As an example, and to give an idea of how the vulnerabilities are categorised, consider only one of the 13 categories, **password cracking and sniffing**. When traversing the complete CyberCop Scanner vulnerability database, the vulnerabilities shown in table 4 are found to belong to this category:

Table 4. Password cracking and sniffing vulnerabilities in CyberCop Scanner

ID	Brief Description
1001	Finger access control check
1002	Finger 0@host check
1004	Finger .@target-host check
1038	S/Key Banner Check
1039	Ascend Configurator Identification Check
2006	WFTP invalid password check
2018	FTP - PASV core dump check
2019	FTP - argument core dump check
2024	FTP - password file contains hashes

ID	Brief Description
3001	Unpassworded laser jet printer check
3002	Unpassworded Gatorboxes check
3003	Portmaster default password check
3006	Ascend Port 150 Check
3008	Ascend SNMP/TFTP Configuration File Retrieval
3009	Ascend SNMP/TFTP Full Configuration File Retrieval
3010	Unpassworded Ascend router check
3011	Unpassworded Netopia router check
9000	Password Guessing/Grinding
9001	FTP Password Guessing
9002	Telnet Password Guessing
9003	POP Password Guessing
9004	IMAP Password Guessing
9005	Rexec Password Guessing
9006	Rlogin Password Guessing
9007	Password(s) guessed via WWW server
10032	PHP mlog Example Script Check
10033	PHP mylog example script test
15005	POP shadowed password vulnerability
15007	Kerberos server check
15025	Kerberos user name gathering check
15040	Qualcomm "qpopper" POP3 PASS Overflow
15043	TFTP (Trivial File Transfer Protocol) readable
16001	Unpassworded NetBIOS/SMB check
16002	Guessable NetBIOS/SMB password check
16024	NetBIOS Samba password buffer overflow
17020	DNS Cache Corruption, Guessable Query Ids
18002	Password Grinding (through IPC$)
18004	Password Database Retrieved
18005	LSA Secrets Retrieved
18007	Lan Manager Authentication Enabled
18008	Force server to use SMB message signing
18009	Force client to use SMB message signing
18015	Password Filter Registry Key Changed
18021	NDIS 4.0 bit set for "promiscuous" mode
31006	Authentication test-password sent in Clear Text

5.2 Cisco Secure Scanner

Cisco Secure Scanner [CSSC 00] is a proactive IDS tool. It scans for approximately 230 vulnerabilities for the specific version evaluated. Cisco Secure Scanner allows for graphical reporting. These graphical reports, however, are not clear and prove to be yet another example of a problem in many of the reports of current IDSs – readability.

When traversing the complete Cisco Secure Scanner vulnerability database for the category Password cracking and sniffing, the following vulnerabilities shown in table 5 are found to belong to this category:

Table 5. Password cracking and sniffing vulnerabilities in Cisco Secure Scanner

ID	Brief Description
1	General password vulnerabilities
2	Weak passwords
3	Default dangerous accounts
5	Default accounts with no or the same password
207	Live /etc/passwd file in FTP directory
214	FTP list core bug
319	HTTP IIS view source bug
322	IIS Dot Dot view
329	CGI websendmail file access
331	CGI htmlscript bug
332	HTTP IRIX performer bug
350	IIS ShowCode vulnerability
802	NFS Export Everyone
810	NFS system files export
1100	RPC bootparamd active
1110	RPC selection_svc bug
1115	SunOS NIS vulnerabilities
1117	RPC yppasswdd
1120	RPC admind active
1122	RPC ruserd active
1305	Back Orifice active
1315	Same username and password for Windows NT guest account
1316	NULL password for Windows NT administrator
1317	Same username and password for Windows NT administrator
1319	NT registry prior to service pack 3
1400	Sendmail decode Alias
1413	IMAP active
1700	TELNET active
1708	IOS command history

ID	Brief Description
1800	TFTP active
1802	TFTP get ../.. bug
10020	FrontPage extensions exposed
14118	Cisco Catalyst enable bypass
14126	HTTP jj vulnerability