# Vulnerabilities categories for intrusion detection systems

*H.S. Venter [1] and J.H.P. Eloff [2]*

*[1]Department of Computer Science, Rand Afrikaans University, PO Box 524, Auckland Park, South Africa, email: heins@adam.rau.ac.za*

*[2]Department of Computer Science, University of Pretoria, Pretoria, South Africa email: eloff@cs.up.ac.za*

The Internet is a rough sea.

Vulnerability upon vulnerability arises as the Internet community grows enormously on a daily basis. The SANS Institute has identified several reasons why vulnerabilities may remain [FURN 01] [NOAC 00]:

- 1.2 million new computers are added to the Internet every month.
- There is lack of security experts to address the problems.
- The number of vulnerabilities continues to grow and there is no priority list for dealing with them.

The bottom line is that vulnerabilities are real — deal with it! But how? Certainly, your vulnerability assessment and intrusion detection tools must do the work for you. "Which one of the hundreds out there should I use then?", I hear you asking. Well, here are 13 generic vulnerability groups that should be addressed by these vulnerability assessment tools:

### 1. Password cracking

This category involves vulnerabilities with a root cause of having accounts with weak or no passwords [NCF1 01] [BACE 00].

### 2. Network and system information gathering

This category involves vulnerabilities concerned with scanning a network to discover a map of the available hosts, as well as to detect vulnerable services on the hosts and the network [NCF2 01]. Synonyms for this category include *network mapping*, *target acquisition*, *network reconnaissance* or *footprinting* [SMK1 01].

### 3. User enumeration

This category involves vulnerabilities concerned with retrieving information of user accounts from a specific system [SMK2 01]. As soon as an intruder has retrieved a list of the user names registered on a specific system, it is often only a matter of time before he/she obtains the password by using a password-cracking program, for example L0pht Crack [LOPH 01]. After all, the user names have to be obtained before any attempt can be made to crack passwords.

### 4. Backdoors, Trojans and remote controlling

This category involves vulnerabilities concerned with having access mechanisms installed on a system which are almost hidden and not obvious [SMK3 01]. In other words, a covert channel is created. Often a backdoor is installed with the aim of controlling a system remotely. The backdoor becomes a hidden entry point where the intruder can connect to the system unnoticed at any given time.

### 5. Gaining access to remote connections and services

This category involves vulnerabilities concerned with the risk that an unauthorized person has the ability to remotely connect to a system with the aim of misusing the system [NCF3 01]. For example, an intruder can try to connect to port 21 (FTP) in a bid to see whether the FTP service is enabled on that machine. If the intruder is successful, he/she can try to exploit further vulnerabilities in the FTP service, for example intercepting clear text passwords or seeing whether the FTP root directory is write-enabled.

### 6. Privilege and user escalation

This category involves vulnerabilities concerned with the risk that the authorization properties of an existing (probably compromised) system account can be changed

so that this user account has more privileges or more powerful access rights allocated to it. More privileges and more powerful access rights will allow a specific user account to access data or system resources that it was initially unauthorized to access [SMK4 01].

### 7. Spoofing

This category involves vulnerabilities concerned with the risk that an intruder can fake an IP packet's source address in a bid to hide an intruder's identity or activity amongst a storm of other network traffic [NCF4 01] [SMK5 01].

### 8. Misconfigurations

This category involves vulnerabilities concerned with the risk that software or hardware packages have been incorrectly configured, leaving the package vulnerable to the other vulnerability categories mentioned here [NOR2 01].

### 9. Denial-of-service (DoS) and buffer overflows

This category involves vulnerabilities concerned with the risk of one or more intruders launching an attack designed to disrupt or completely deny legitimate users' access to networks, servers, services or other resources [NCF5 01] [SMK6 01] [GREE 02]. Such a vulnerability, therefore, is not concerned with stealing information or changing data, but simply with downgrading the performance of the computer and/or network resources to such a level that services are disrupted significantly or completely.

### 10. Viruses and worms

Viruses and worms are different types of software applications, but with the same goal of spreading from one system to another in a bid to conduct malicious activity. This category involves vulnerabilities concerned with the risk that such viruses or worms can spread to any system in a network [NCF6 01] [NOR3 01].

### 11. Hardware specific

This category involves vulnerabilities concerned with having hardware peripherals which do not run software applications, but which rather run ROM-based or firmware-based programs. These peripherals also contain exploits that cannot be easily updated, patched or corrected, except if the hardware is replaced or the firmware is updated [NOR4 01]. Examples of such hardware peripherals are network switches, routers and terminals.

### 12. Software specific and updates

This category involves vulnerabilities concerned with the risk that software applications contain specific, well known bugs [SMK8 01]. Because these bugs or exploits are published widely on the Internet [BUGT 01], anyone is able to access the Internet and collect information about these bugs in a bid to exploit them. Therefore, these software applications must be updated to *patch* their exploitations in an effort to fix security bugs or loopholes to avoid successful future attacks on them.

### 13. Security policy violations

This category involves vulnerabilities concerned with the risk that a system's security policy is violated. A security policy is a set of rules or guidelines and typically stipulates the standard of security that must be maintained on an organization's computer systems and network [KING 01]. When a security policy violation is found, it means that a different configuration setting on the system was detected and thus violates the prescribed policy setting.

## Conclusion

Perhaps there is no vulnerability assessment or intrusion detection tool that covers all these categories extensively. However, when you are buying these tools, look for ones that cover as

many of these categories as possible. It is worthwhile spending money on these tools, because one major attack on your systems and you could stare bankruptcy in the face!

## References

[BACE 00] Bace, R.G., 2000, "Password-Cracking"; *Intrusion Detection*; Macmillan Technical Publishing; ISBN 1-57870-185-6; pp. 150-151.

[BUGT 01] SecurityFocus.Com, 2001; *Bugtraq*; "Bugtraq Archives"; http://www.securityfocus.com/forums/bugtraq/intro.html.

[FURN 01] Furnell, S.M., Chilliarchaki, P., and Dowland, P.S., 2001; *"Security analysers: administrator assistants or hacker helpers?" Information Management & Computer Security*;; MCB University Press; ISSN 0968-5227; Vol. 9/2; pp. 93-101.

[GREE 02] Greenstein, M. and Vasarhelyi, M., 2002; "Risks Associated with Viruses and Malicious Code Overflows*", Electronic Commerce – Security, Risk Management, and Control*; Second Edition;; McGraw-Hill; ISBN 0-07-241081-7; pp. 242-245.

[KING 01] King, C.M., Dalton, C.E. and Osmanoglu, T.E., 2001; *"Security Policies, Standards, and Guidelines" Security Architecture – Design, Deployment & Operations*; RSA Press/Osborne/McGraw-Hill; ISBN 0-07-213385-6; pp. 13-39.

[LOPH 01] @STEAK.COM, 2001; *L0pht Crack*; "L0pht Crack Version 3.0"; http://www.atstake.com/research/lc3/index.html.

[NCF1 01] Northcutt, S., Cooper, M., Fearnow, M. and Frederick, K., 2001; "Passwords", *Intrusion Signatures and Analysis*; New Riders Publishing; ISBN 0-7357-1063-5; pp. 76-85.

[NCF2 01] Northcutt, S., Cooper, M., Fearnow, M. and Frederick, K., 2001; "Network Mapping"; *Intrusion Signatures and Analysis*; New Riders Publishing; ISBN 0-7357-1063-5; pp. 149-168.

[NCF3 01] Northcutt, S., Cooper, M., Fearnow, M. and Frederick, K., 2001; "Remote Procedure Call Weaknesses"; *Intrusion Signatures and Analysis*; New Riders Publishing; ISBN 0-7357-1063-5; pp. 57-65.

[NCF4 01] Northcutt, S., Cooper, M., Fearnow, M. and Frederick, K., 2001; "IP Spoofing Stimuli"; *Intrusion Signatures and Analysis*; New Riders Publishing; ISBN 0-7357-1063-5; pp. 134-143.

[NCF5 01] Northcutt, S., Cooper, M., Fearnow, M. and Frederick, K., 2001; "What is a DoS Attack?"; *Intrusion Signatures and Analysis*; New Riders Publishing; ISBN 0-7357-1063-5; p. 189.

[NCF6 01] Northcutt, S., Cooper, M., Fearnow, M. and Frederick, K., 2001; "Trojans"; *Intrusion Signatures and Analysis*; New Riders Publishing; ISBN 0-7357-1063-5; pp. 233-250.

[NOAC 00] Noack, D., 2000; "The back door into cyber terrorism". *APBnews.com report*.

[NOR2 01] Northcutt, S., Novak, J. and McLachlan, D., 2001; "Misconfigured Systems"; *Network Intrusion Detection*; Second Edition; New Riders Publishing; ISBN 0-7357-1008-2; p. 159.

[NOR3 01] Northcutt, S., Novak, J. and McLachlan, D., 2001; "Virus Industry Revisited"; *Network Intrusion Detection*; Second Edition; New Riders Publishing; ISBN 0-7357-1008-2; pp. 213-214.

[NOR4 01] Northcutt, S., Novak, J. and McLachlan, D., 2001; "Virus Industry Revisited"; *Network Intrusion Detection*; Second Edition; New Riders Publishing; ISBN 0-7357-1008-2; pp. 188, 214.

[SMK1 01] Scambray, J., McClure, S. and Kurtz, G., 2001; "Footprinting"; *Hacking Exposed*; Second Edition; Osborne/McGraw-Hill; ISBN 0-07-212748-1; pp. 5-34.

[SMK2 01] Scambray, J., McClure, S. and Kurtz, G., 2001; "NT/2000 User and Group Enumeration"; *Hacking Exposed*; Second Edition; Osborne/McGraw-Hill; ISBN 0-07-212748-1; pp. 87-95.

[SMK3 01] Scambray, J., McClure, S. and Kurtz, G., 2001; "Back Doors"; *Hacking Exposed*; Second Edition; Osborne/McGraw-Hill; ISBN 0-07-212748-1; pp. 252-257, 433-437, 533-558.

[SMK4 01] Scambray, J., McClure, S. and Kurtz, G., 2001; "Privilege Escalation"; *Hacking Exposed*; Second Edition; Osborne/McGraw-Hill; ISBN 0-07-212748-1; pp. 164-174, 238-241, 308, 339-340.

[SMK5 01] Scambray, J., McClure, S. and Kurtz, G., 2001; "Spoofing Attacks"; *Hacking Exposed*; Second Edition; Osborne/McGraw-Hill; ISBN 0-07-212748-1; pp. 170-172, 287-290, 453-456.

[SMK6 01] Scambray, J., McClure, S. and Kurtz, G., 2001; "Denial Of Service (DoS) Attacks"; *Hacking Exposed*; Second Edition; Osborne/McGraw-Hill; ISBN 0-07-212748-1; pp. 483-506.

[SMK8 01] Scambray, J., McClure, S. and Kurtz, G., 2001; "Software Hacking"; *Hacking Exposed*; Second Edition; Osborne/McGraw-Hill; ISBN 0-07-212748-1; pp. 507-653.

[SCH1 00] Schneider, B., 2000; "Intrusion Detection Systems"; *Secrets and Lies, Digital Security in a Networked World*; John Wiley & Sons Inc.; ISBN 0-471-25311-1; pp. 194-197.