GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

A generic threat analysis for an Internet enabled organisation.

GIAC CSEC Practical paper for Paul Wright Version 1.4b submitted 28-06-03.

1. Abstract 2
2. Why is Information Security important? 2
2.1 Globally for Society in general 2
2.2 For Businesses to protect IP 3
2.3 For the Individual 4
3.0 The threat analysis. 4
3.1 The threat to an organisations network from hackers is.. 4
3.2 Hacker gains information about the companies network. 4
3.2.1 Reconnaissance 4
3.2.2 Scanning the actual network to map its structure 5
3.3 Attempt to make unauthorised connection to the Network. 5
3.4 Attacking a known Vulnerability. 5
3.4.1 Session Hijacking 6
3.4.2 Buffer Over Flow. 6
3.4.3 Automation of Vulnerability Scanning 6
3.4.4 IDS Evasion. 6
3.4.5 Denial of service attacks 7
3.5 Software put onto the machine by the attacker 7
3.5.1 Netcat 7
3.5.2 Worms and Viruses 7
3.5.3 Backdoors and Trojans 7
3.5.4 Rootkits 8
3.6 Escalating privilege 8
3.7 Covering the tracks. 8
4. A Top Ten of current Topics. 9
4.1 Rootkits 9
4.2 Stegonagraphical encryption 10
4.3 NIDS to be replaced by Firewalls? 10
4.4 Centrino Wireless in all laptops. 10
4.5 Smoothwall 10
4.5 BIOS attacking VIRI 11
4.6 Web application security and OWASP 11
4.7 Trusted computing, DMCA and Microsoft's Palladium 11
4.8 Use of the Image tag in HTML email 12
4.9 LICQ and encrypted Instant Messaging. 12
4.10 "Stumbler" the New Threat 13
5.0 Summary. 13
6.0 references. 14

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

1. Abstract

This paper is a summary of the threats that an organisation faces when they start to use the WWW and a description of the methods used by hackers to enact these threats. I have prefaced this summary with a discussion of why Information Security is important and finalised the paper with my current top ten topics of interest to Information Security Professionals. This paper has value as it describes in logical plain English the stages involved in hacking and what can be done to counter the threat. As such it should be useful to both management and technical personnel.

This analysis is informed by the World class teaching of Ed Skoudis, Chris Brenton, Jason Fossen, Mike Poor and Jim Herbeck who have taught me during my time at the SANS institute as a conference volunteer.

2. Why is Information Security important?

Reading through the many fine practical papers that have been submitted over the years for Track 1 there is no shortage of good technical documents. At the moment I am thinking how I can best contribute to this field when much of my experience is at a strategic business level as well as technical? I have noticed that the importance of what we are doing has not been discussed as heavily as many experts take this point "as read". This point is something I would like to explore from my personal point of view before I move onto the detail of my analysis.

Information security is important on Three major levels.

a). Globally for Society in general.
b). For Businesses to protect IP (intellectual property).
c). Individual personal level.

2.1 Globally for Society in general

Until you have something really worth knowing then Information Security's true worth is not apparent. The details of a future war plan are a good example of something worth knowing. Information Security arguably has its roots in the Caesar Cipher used at the height of the Roman Empire to secure future plans of this nature. This Cipher helped the Romans control a large expanse called the European continent and the only time a united Europe included England economically, so far. The power of Information Security allowed the Romans to control Europe.

As I am writing this paper whilst attending the London Hammersmith SANS conference it is fitting that Jim Herbeck-SANS Director for Europe has informed the GIAC Certification briefing that this is the biggest SANS conference outside of the US so far. This coincides with increased Internet

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

enabled business in Europe as exemplified by the new .EU domain name (1 - http://www.dns.be/eng/News/whatsnew22may2003.htm).

SANS is enabling European organisations to protect their sensitive information in the future, which can help them to compete globally. This is a sophisticated policy which leads by example.

2.2 For Businesses to protect IP

The major battlefield of the modern world is increasingly its business markets and the weapons of a company are its IP (intellectual property). The ability to take away those weapons from an insider position or outsider attack has been made easier now with the technological tools available to the averagely IT-literate person. Knowledge is power and the skills learnt at SANS help companies protect this knowledge.

What is for sure is that Information security is relevant to the businesses of Europe as can be seen by the big name attendees at this years London-Hammersmith SANS conference.

While organisations like SANS exist companies and individuals will be able to protect knowledge that they wish and have the right, to keep private. Parties can act independently which promotes competition and allows differing views to exist and flourish.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.3 For the Individual

We have all experienced invasions of personal privacy and the skills learnt at SANS can help stop oppressive regimes, intrusive competitors, overbearing marketing companies or individual snoopers from taking advantage by accessing your information. GPG, Enigmail and Mozilla provide powerful cross platform methods for any user to have "pretty good encryption" of their communications.

SANS are giving the ability to make information secure whether you are a government, company or individual. This distributes power in a way that helps keep equilibrium and helps stops any one "party" from dominating another by their power to exclusively access all information including that which is not theirs.

3.0 The threat analysis.

3.1 The threat to an organisations network from hackers is..

- Hacker gains information about the company and its network
- Hacker uses this information to access, deny access or modify data on that companies network.
- The hacker activities adversely impact Business via its IT systems.

This paper will describe the hacker's techniques and then give a brief counter-defence to each threat.

3.2 Hacker gains information about the companies network.

3.2.1 Reconnaissance

Data is collected in a reconnaissance phase before attempting any attack on a network. This is done without alerting the target by using these third parties.

- WhoIs Internet searches.
- DNS and NS Lookup.
- Googles cache.
- SamSpade (2 - http://www.samspade.org/).
- Netcraft (3 - http://www.netcraft.com).

Primary Defence - Opt out of domain name information requirements.
- Email Google to clear cache.
- Publish emails on website as images not text.
- Obfuscate OS fingerprint.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3.2.2 Scanning the actual network to map its structure

- Scans of the actual network are made using standard tools such as NMAP which is built into some Linux distro's and is available for windows. (4 - http://www.insecure.org/nmap/). This tool will show the services that are running on the machine. These services can then be checked for corresponding exploits at a site like (5- www.securityfocus.com).
- A diagrammatic map of the network may be made using a tool such as Cheops-ng. (6 - http://cheops-ng.sourceforge.net).
- TCPIP Traffic may be intercepted, read and analysed using a tool such as Ethereal at (7 - http://www.ethereal.com/).
- Network mapping can even be done through a firewall using tools such as firewalk. (8 - http://www.packetstormsecurity.com/UNIX/audit/firewalk).
- Network mapping can also be done through a switch by changing the entries in the ARP cache that maps IP addresses to MAC addresses. DSNIFF is a tool that can achieve this at (9 - http://www.monkey.org/~dugsong/dsniff/).

Primary Defence – Use a good firewall like Checkpoint or Smoothwall

3.3 Attempt to make unauthorised connection to the Ne twork

- Null sessions are used by NTs communication structure to enable networking but can be used by a hacker to identify information about the machine such as USERS and unprotected file shares on the machine.
- Once a username and share is identified then an attempt can be made to connect using a password generated by password cracker such as John. (10 - http://www.openwall.com/john/).
- Later on in the hacking process when the target machine has been entered by the attacker then the actual password file can be "cracked". See the section 3.6.

Primary Defence – Enforce a strong password policy and only allow remote log in using a VPN/IPSEC.

3.4 Attacking a known Vulnerability.

Vulnerabilities can take many forms but it is commonly a design fault in a piece of software and can be researched at Security Focus (11 - http://www.securityfocus.com) where the famous "bugtraq" list of software faults is held.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3.4.1 Session Hijacking

Session hijacking is where information in a communication connection can be added to or completely replaced. Session hijacking can be done using tools like Juggernaut at http://www.rootshell.com (12) or powerful tool called Ettercap. The threat here is that a malicious user could act on behalf of a legitimate user in an online banking application for instance. Session tracking mechanisms such as the IDs that are generated by a web server application can be guessed especially if they are incremental IDs or generated with a discernible pattern.
Primary Defence – Use random IDs

3.4.2 Buffer Over Flow.

Aleph One described the buffer overflow technique in his paper "smashing the stack for fun and profit". Essentially it consists of a command that is entered into a user input field onto the executable memory stack that a program allocates. This is due to poor input validation, as all input should be parsed.
The buffer overflow can be used to gain access to a box as the normal operation of the Software is interrupted. Once this is done then a program of the attackers choice can be run.
Primary Defence – Validate all input code and implement a non-executable system stack.

3.4.3 Automation of Vulnerability Scanning

The threat from hacker activity is increased by the tools used to automate the vulnerability identification process.
The threat from hackers is largely due to the automated tools that make checking for vulnerabilities faster. Nessus has over 800 exploits preloaded ready at the press of a button. (13 - http://www.nessus.org).
Whisker provides automated vulnerability scanning for web servers also from http://www.wiretrip.net/rfp (14). It also includes IDS evasion and password auditing via brute force.
Primary Defence – Apply patches regularly

3.4.4 IDS Evasion.

Intrusion Detection systems can be evaded by dividing code between separate packets so it cannot be recognised. This is called fragmentation and tools such as Fragroute can be used to do this. (15 - http://packages.debian.org/unstable/net/fragrouter.html).
IDS systems can also be evaded by mutating the structure of the program in a way that does not affect its functionality but does mean that it cannot be identified by the IDS system.
Primary Defence – Use behavioural IDS systems as well as signature based IDS with increased Defence in Depth provided by Intrusion Prevention Firewalls (Checkpoint NG) as well as Network based IDS like SNORT 2.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3.4.5 Denial of service attacks

By directing more network traffic than a server can handle a server can be stopped from carrying out its function. The same effect can be made by simply crashing the machine with input that it cannot deal with as in the "ping of death" attack that uses a larger than normal window size.
A denial of service attack may need many machines to act together in order to gain the necessary bandwidth to deny the victims ability to provide the service. If an attacker can gain administrative rights on many machines, one attacker can control many machines in unison to create a distributed denial of service attack or DDOS.
Primary Defence – Load Balancing, Firewall/router configuration, clustered server structure. Collaborative lines of communication with service provider to minimise the risk.

3.5 Software put onto the machine by the attacker

3.5.1 Netcat

Netcat is a small program that can be easily placed onto a victim's machine after an exploit has been executed. Netcat can be placed into the scheduler or start up folder to run at boot. Netcat is very flexible as it can send and receive large and small files from the victim and attackers machine. The attacker can then install and run many number of programs on the target machine using Netcat. Netcat can be set up in chains to make a complicated connection that effectively helps to hide the true source of the attacker's machine through a long chain. Netcat can be used in a bidirectional chain that can feedback a command shell to the attacker through a process called "shovelling a shell".
Primary Defence – Netcat has many uses good and bad. To stop remote access via netcat the previous vulnerabilities need to be fixed so that the application cannot be run.

3.5.2 Worms and Viruses

Worms and Viruses are usually transferred by an automated process that infects the victims machine. The goal can be to inhibit the working of the machine or to install a backdoor on the target machine.
Primary Defence – Antivirus definitions kept upto date.

3.5.3 Backdoors and Trojans

SubSeven is an example of a backdoor that can be installed on a target machine. The idea is that this program can be used to maintain access to the target machine for future use by the attacker. The attacker may then patch the vulnerability to the machine so that no other attackers can gain access to the exploitable machine. In order to execute a program such as this sometimes a higher privilege than that gained by the original exploit may be required.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Primary Defence – Tripwire and windows file protection/MD5 hashes of sensitive files. Plus check the logs. Perhaps print the logs in real time.

3.5.4 Rootkits

The idea of the rootkit is to maintain access to the victims machine over time. It may be necessary to hide the prescence of the software on the machine so that the legitimate user does not uninstall the software. A good example of root kit is Knark which is a kernel level rootkit.(16 - http://www.securityfocus.com/guest/4871).
In order to gain and maintain Root Access which is the Unix admin account a process of privilege escalation may be needed as inward communication methods such as telnet cannot be done using the Root account. A User account needs to be used and then administrative rights gained.
Primary Defence – Need a method to verify the integrity of the operating system files. See 3.5.3.

3.6 Escalating privilege

Now that access to the machine has been made the attacker can attempt to increase their privileges on that machine by cracking the password database using an application such as L0phtcrack. LanMan passwords are very susceptible and UNIX passwords least susceptible due to the salt system that they use to increase the permutations needed to be tried before guessing a correct password. Once root administration rights have been gained on a machine then all control passes to the hacker. The only problem then is maintaining this access over time.
Primary Defence- Disable LanMan. Authentication, enforce complex passwords.

3.7 Covering the tracks.

A hacker may destroy the logs that have recorded the hacking techniques used by simply deleting the log files. Processes on the victims machine can be hidden or given the same name as an existing process which effectively hides the fact that the hacked process is running.
Primary Defence – print out the log files in real time. Or can send log entries to Syslog server but sniff them using snort to backup which does not need an IP address and is harder to find for hacker. (Snort your logs! see the Honeynet.org project).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4. A Top Ten of current Topics.

During the research for this paper I have come across some subjects that do not appear to have been covered as yet in the track 1 practical and SANS reading room. These issues are from many sources but mainly from speaking to my friends at the Hammersmith conference. Two items that narrowly missed this list are War Walking AIBOS and Mike Poors Underpants. "***War Walking***" With AIBO is a "***very advanced***" form of Wireless Network Auditing that is referenced from Mike Poors study group at a Tysons Corner BOF (birds of a feather meeting). Essentially the AIBO was programmed to act as a wireless LAN sniffer that found unauthorised access points by walking around the company premises and then alerting the administrator by automatically barking at them.

Mike Poors unusually useful underpants can be seen at (17 - http://www.counterhack.net/unusual_devices_running_snort.html).

I will now outline my top ten for you briefly and perhaps some one may wish to pick up the baton.

4.1 AFX Rootkit.
4.2 Stegonagraphical encryption.
4.3 NIDS to be replaced by Firewalls?
4.4 Centrino Wireless in all laptops.
4.5 Smoothwall.
4.5 BIOS attacking VIRI.
4.6 Web application security and OWASP.
4.7 Trusted computing, DMCA and Microsoft's Palladium.
4.8 Use of the Image tag in HTML email.
4.9 LICQ and encrypted Instant Messaging.
4.10 "Stumbler" - the New Threat?

4.1 Rootkits

Rootkits such as the new AFX rootkit for windows by Aphex, which hide process names from the user, are increasing in sophistication. Aphex uses DLL injection to hide in the explorer.exe process and does not show on Netstat.
(18 - http://www.megasecurity.org/trojans/a/afx_win_rootkit/Afx_win_rootkit2003.html).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4.2 Stegonagraphical encryption

Stegonagraphical encryption is of huge current interest the point being that I can encrypt my message as normal and then use a stegonagraphical tool to obfuscate the encrypted message within a file. This is very hard indeed to detect especially when combined with the Polymorphic capabilities of a tool like HYDAN (19 - http://www.crazyboy.com/hydan/).
Please see Eric Coles new book "Hiding in Plain Sight" for further depth.

4.3 NIDS to be replaced by Firewalls?

An area of interest is the recent article highlighted in SANS newsbytes by Gartner (20 - http://thewhir.com/marketwatch/gar061103.cfm) that Network based Intrusion detection functionality was too expensive and would be replaced by Firewall Inline IDS functionality by 2005. This is clearly the ravings of a mad person as SNORT is free ("beer" and "speech" i.e. GNU). How can this be too expensive? Also why would a company choose to only rely only on a firewall based Intrusion Prevention type system when it can have Network based Intrusion detection in addition. This is Strength in Depth which is preferable by any standard of common sense.

4.4 Centrino Wireless in all laptops.

The introduction of Centrino laptops means that WIFI capabilities will be built into Laptops when purchased. This provides a significant future security threat in that many users will not realise that they are in fact advertising a wireless connection. Centrino comes as standard with weak WEP encryption and has to be upgraded to the more secure WPA and Leap. (21 - http://www.internetnews.com/infra/article.php/2108381).
This problem could be compounded by the fact that Centrino has had problems with VPN compatibility, which is the best way to have really secure laptop communications.
(22 - http://www.idg.net/ic_1318899_9677_1-5045.html)

4.5 Smoothwall

Smoothwall is a hardened Internet firewall and routing device and is "free" as it is produced under the GNU Public License with a commercially supported version also available.

Smoothwall is highly recommended and used by many of the smaller companies that have come to the Hammersmith conference. A group of us installed it on the conference network and it worked very well.
(23 - http://www.smoothwall.org/about/).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4.5 BIOS attacking VIRI

There has been a lot of discussion over the ability to access the BIOS via an Internet connection similar to the Chernobyl virus. I personally have a dual BIOS motherboard that automatically changes to the backup in case of attack but there have been discussions about how a virus may write itself to the BIOS and stay there in memory instead of the less subtle methods of the Chernobyl (24 - http://www.cert.org/incident_notes/IN-99-03.html) virus. The possibilities of using the BIOS as part of the application memory has been explored by the Linux Bios project (25 - http://www.linuxbios.org/index.html) which plans to run the whole Linux operating system from the BIOS memory.

A cure to the threat of a virus that sits in the BIOS memory has been suggested by password protecting the BIOS. I am going to do this in the future.

Ed Skoudis' new book is on the subject of Malware in general and if it is anything like Counter Hack will be required reading.
(26 - http://www.amazon.com/exec/obidos/tg/detail//0131014056/ref=pd_sim_art_elt/103-5105968-1722221?v=glance#product-details).

4.6 Web application security and OWASP

Web applications are notoriously insecure. Applications like Achilles allow the manipulation of non-persistent cookies so that user sessions can be hijacked. It is available at www.digizen-security.com. This is a great resource full of really very good resources for web application security. (27 - http://www.owasp.org/).

4.7 Trusted computing, DMCA and Microsoft's Palladium

AKA "next-generation secure computing base" which will allow the control of electronic format intellectually property protected by law. IP protection procedures like this that will occur through changes at the Physical and Application layer that will affect Windows and Linux.
For many interesting ideas on this subject a vendor neutral view can be found at Ross Andersons website at Cambridge University.
(28 - http://www.cl.cam.ac.uk/users/rja14/).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4.8 Use of the Image tag in HTML email

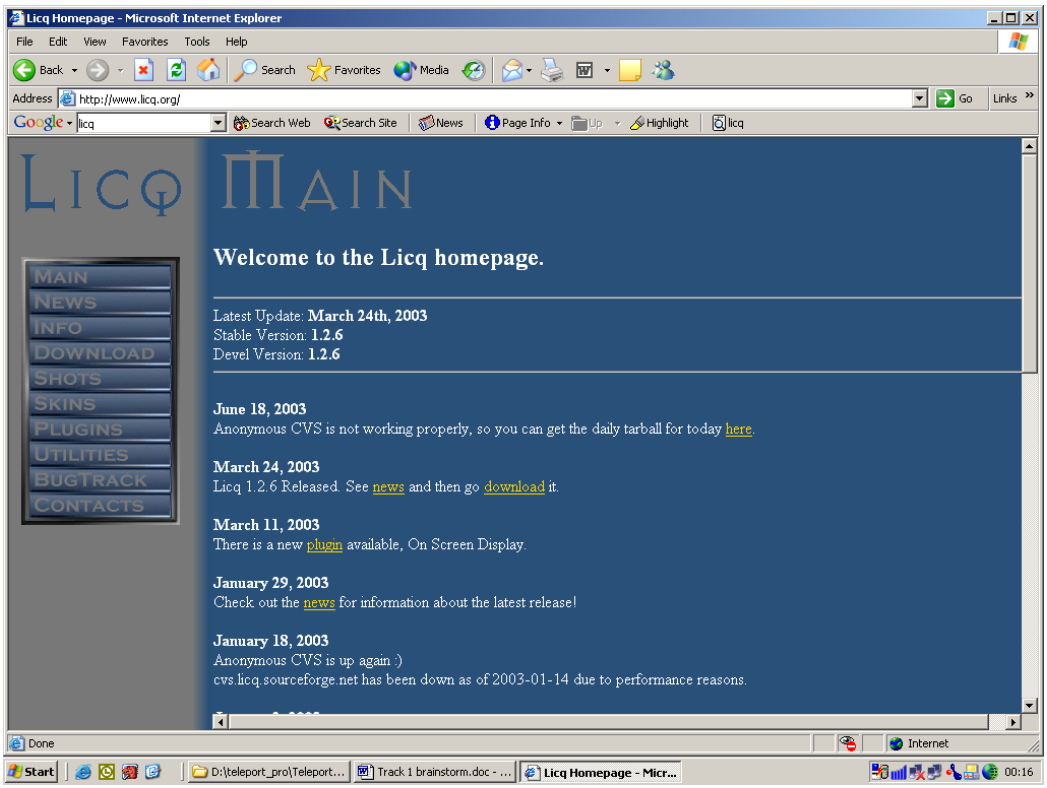
HTML email can be used to execute a script on a remote web server that can be used to pass information from the users machine. This is done using the "img" html tag that is linked to a web based image usually and called in from the Internet to the users email. Instead the link can be made to a script such as..

<img source=tellmethereci pienthasopenedtheiremail.asp?recipient@emailaddress.c om>

Which passes the sent html emails request for an image to the web based application as long as the email user can receive HTML email online. This is why I never accept HTML based email.

4.9 LICQ and encrypted Instant Messaging.

LICQ is an ICQ client used by European Hackers and Crackers in order to have encrypted communication over ICQ. It also has the built in ability to run an exploit such as trying to run Back Orifice on a contact in the ICQ database. LICQ only runs on Linux. Used in conjunction with GPG, Enigmail and Mozilla it can give powerful communication privacy that help protect the interests of the individual but is also used by many hackers. (29 - http://www.licq.org/).



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4.10 "Stumbler" the New Threat

Proof that new threats are rising all the time is shown by the rise of scanning by an unknown application using a window size of 55808. (30 - http://www.theregister.co.uk/content/55/31341.html).

5.0 Summary.

Hopefully this paper will be of some use to the average and skilled user. In order to stay a step ahead of the blackhat hacker community, organisations need to empower their professional IT security personnel. As there are so many new threats arising it is certain that the SANS information security training conferences will be busy for many years to come.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

6.0 References.

1. Marc Van Wesemael, Franco Denoth, Anders Janson, 22 May 2003, The European Commission chooses EUR*id* to manage .*eu* domain names URL: http://www.dns.be/eng/News/whatsnew22may2003.htm
2. 28-06-03, URL: http://www.samspade.org/
3. 28-06-03**,** URL: http://www.netcraft.com
4. FYODOR, 28-06-03**,** URL: http://www.insecure.org/nmap/
5. 28-06-03, URL**:** www.securityfocus.com
6. Brent Priddy, 28-06-03, URL: http://cheops-ng.sourceforge.net
7. Authors http://www.ethereal.com/introduction.html#authors, 28-06-03 URL: http://www.ethereal.com/
8. Mike Schiffman and David Goldsmith , 28-06-03, URL: http://www.packetstormsecurity.com/UNIX/audit/firewalk
9. Doug Song, 28-06-03, URL: http://www.monkey.org/~dugsong/dsniff/
10. Open wall project, 28-06-03, URL: http://www.openwall.com/john/
11. 28-06-03, URL: http://www.securityfocus.com
12. 28-06-03, URL: http://www.rootshell.com
13. Renaud Deraison, 28-06-03, URL: http://www.nessus.org
14. Rain Forest Puppy, 28-06-03, URL: http://www.wiretrip.net/rfp
15. Simon Law, 28-06-03, URL: http://packages.debian.org/unstable/net/fragrouter.html
16. Toby Miller, 28-06-03, URL: http://www.securityfocus.com/guest/4871
17. Aphex, 28-06-03, URL: http://www.megasecurity.org/trojans/a/afx_win_rootkit/Afx_win_rootkit2003.html
18. Ed Skoudis, 28-06-03, URL: http://www.counterhack.net/unusual_devices_running_snort.html
19. Rakan El-Khalil, 28-06-03, URL: http://www.crazyboy.com/hydan/
20. Richard Stiennon (quoted by thewhir.com), 28-06-03, URL: http://thewhir.com/marketwatch/gar061103.cfm
21. Erin Joyce, March 12, 2003 Intel's New Wireless Platform: Centrino URL: http://www.internetnews.com/infra/article.php/2108381
22. BOB BREWIN, A work-around disabling some of the Centrino features, 29.05.03, URL: http://www.idg.net/ic_1318899_9677_1-5045.html
23. Richard Morrell and Lawrence Manning , 28-06-03, URL:http://www.smoothwall.org/about/
24. 28-06-03, URL: http://www.cert.org/incident_notes/IN-99-03.html
25. Authors http://www.linuxbios.org/contributors/index.html , 28-06-03, URL: http://www.linuxbios.org/index.html
26. Ed Skoudis , Counter Hack , 28-06-03, URL: http://www.amazon.com/exec/obidos/tg/detail//0131014056/ref=pd_sim_art_elt/103-5105968-1722221?v=glance#product-details
27. Authors http://www.owasp.org/aboutus/, 28-06-03, URL: http://www.owasp.org/
28. Ross Anderson, 28-06-03, URL: http://www.cl.cam.ac.uk/users/rja14/
29. Jon Keating, Dennis Tenn, Thomas Reitelbach, 28-06-03, URL: http://www.licq.org/
30. John Leyden, Meet Stumbler: Next Gen port scanning malware 20/06/2003 URL:http://www.theregister.co.uk/content/55/31341.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.