



# 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 permitted 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>

## **Hackers, Crackers and Web Attackers**

**Colin Chow  
SANS Security Essentials  
GSEC Practical Assignment  
Version 1.4b, Option 1  
February 20, 2003**

© SANS Institute 2003, Author retains all rights.

## Table of contents

Abstract.....	3
Background.....	4
Infamous hackers/crackers.....	6
Worms and DoS attacks.....	7
Attack Trend.....	8
Hacker's Methodology.....	10
Downloading and evaluating the tools.....	12
Web hacking.....	20
Hacking with Linux.....	21
Useful hacking links and resources.....	27
Conclusion.....	29
References.....	30

## Abstract

News reports regarding viruses, worms and other Internet attacks disrupting our lives are becoming a more common occurrence today. The *Melissa* virus, *SQL Slammer* worm, *Code Red* worm, *I Love You* worm, to name a few, have the power to take down servers and can cost millions in lost revenue. We have come to depend on the Internet and any down time in any portion of the Internet affects not only the business world but increasingly, is causing disruption in our personal lives. On the face of it, the apparent increase in the frequency of Internet attacks could be related to the rise in the numbers of Hackers.

The primary purpose of this paper is to determine if the rise in hacking can be related to the ease with which tools and resources devoted to hacking can be obtained. An examination on the background of hacking, some of the methodology of hacking, as well as attack trends, will be undertaken. In addition, research into the availability of hacking tools and evaluation of their ease of use, and effectiveness, will be applied. Furthermore, it will examine how the widespread nature of Internet sites devoted to identifying Internet and network security vulnerabilities, and hacking exploits contribute to further spread of hacking.

## Background

Generally speaking, in today's world a Hacker is one who is proficient at using or programming computers to enable illicit or unauthorized access to systems, networks or applications.

However, it seems those that exhibited proficiency with "computer" technology were not always seen in a negative light. During World War II, those people that worked on cracking the code of the Enigma, a typewriter-like machine that encoded messages, could be seen as some of the very first hackers. In the 50's and 60's, hackers were portrayed as "heroes of the computer revolution", (Thomas, Douglas p.14) their work kept in absolute secrecy by the Department of Defense. They were the brains behind technological advancement, from early computer research to projects like ARPANET, which eventually evolved into today's Internet.

Attacks that have a large impact receive the headlines but they are a relatively small percentage of the total number of attacks. The largest numbers of attacks are not of the catastrophic variety. "Today's hack attempts are quicker and, surprisingly, simpler. Attackers are going after the low-hanging fruit. The aggression of attacks has dropped off, and they're now going after easy vulnerabilities", according to Michael Murphy, General Manager of Symantec Canada. (Channel Business, February 26, 2003). It is the "simpler" attacks that may be the result of the increase in the numbers of hackers.

Today however, hackers can be anyone, of any age, with any intentions, anywhere in the world. The reasons people hack systems, networks or applications are many and varied and can range from a thirst for knowledge to achieving fame and glory among their Hacking peers. Just as there are many different reasons for Hacking, there are also several different categories of Hackers, according to Marc Rogers, a behavioral sciences researcher at the University of Manitoba. Some of the categories of Hackers are:

### Old School Hackers:

These hackers are generally computer programmers, usually with a university degree in Computer Science that analyze and crack code to provide free access to information. Their primary motivation is the belief that the Internet is an open resource and should be free to all. They are respectable, technical wizards and usually not malicious or destructive.

In 1982, the movie *Tron* captured the public imagination with the vision of the ultimate old-school hacker who creates, according to Scott Bukatman, “a phenomenological interface between human subject and terminal space, a literal fusion of the programmer and the computer, the ultimate cyberpunk fantasy.” (Thomas, Douglas. p.xiv).

#### Cyber Punks or Script Kiddies:

These hackers are young and their ability with computers and technology can range from novice to intermediate. Those hackers that deface websites and create other cyber-graffiti inhabit this category. They are often referred to as cyber-vandals and, like all vandals they are more nuisances than anything else. They also may be distinguished by the fact that they brag about their exploits in the online chat rooms. Figure 1 shows the top reasons why hackers deface web sites.

#### **By attack reason:**

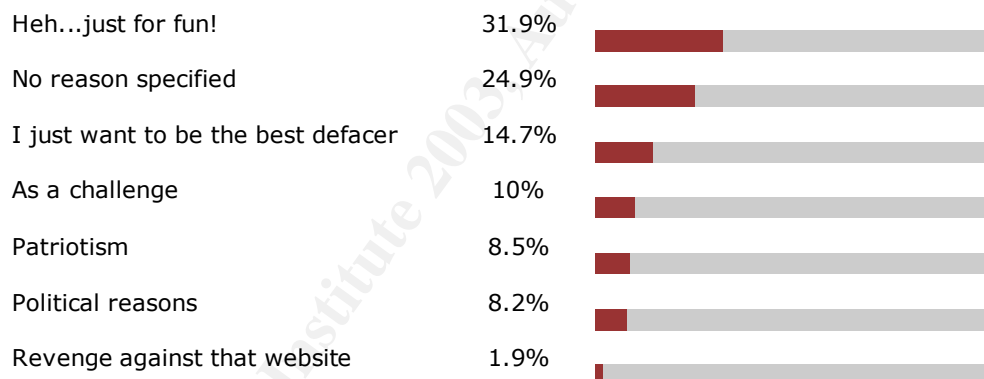


Figure 1. Reasons for defacing web sites. (<http://zone-h.org/en/stats>)

#### Professional Criminals or Crackers:

These hackers may work for the government, large corporations, or also may be involved in organized crime. They hack to obtain secrets from competing corporations and governments, to sell. In an effort to harness the work of these hackers, Secure Digital Music Initiative offered to pay any that found flaws in the SDMI's copy protection scheme. “Hacking for Corporate Profit - SDMI Pays Hackers \$5000” (Alley, Byron. “SDMI Pays Hackers \$5000” URL:

<http://www.winplanet.com/winplanet/opinions/2717/1/>)

#### Code and Virus Writers:

These people are young adults or teens that have basic programming skills and write code for viruses and worms. They don't always release them to the unsuspecting public but when they do, they enjoy the sense of power, as well as the feeling that they are in the elite. Some just get a "kick out of it", while others believe they are doing the community a favor. "Better that you find out about a hole in your system through my virus, than through some unethical cracker smashing into your machine and stealing all your so-called private data." (Delio, Michelle. "Virus writers here to help". Jan. 07, 2002. URL: <http://www.wired.com/news/technology/0,1282,49483,00.html>)

#### White Hat Hacker

The primary motivation of this type of hacker is to provide a service to corporations and governments. White Hat hacking may be considered ethical hacking, that is done for all the right reasons. They are not destructive. Some charge a fee for services like Denial of Service exploitation, Data Transfer Channel Integrity testing, Backdoor checking, Penetration testing, Password Structure Verifying, and vulnerability research. Rent-A-Hacker (<http://www.rent-a-hacker.com/>) is an example of a company that provides these services. Moreover, training institutes are now offering courses on ethical hacking. The Intense School offers Professional Hacking Boot Camp Training for Ethical Hackers, CEH (Certified Ethical Hacker) Certification, URL: <http://www.intenseschool.com/bootcamps/security/hacking/default.asp?bc=hacking>

#### Black Hat Hacker

A Black Hat Hacker takes advantage of the break-in, perhaps destroying files or stealing data for some future purpose. They may also make the exploit known to other hackers and/or the public without notifying the victim and may create back doors for later access.

#### Grey Hat Hacker

Are known as the White Hat Hacker, sometimes wearing the Black Hat to exploit systems and obtain information for personal reasons.

### **Infamous Hackers/Crackers**

The following are some hackers and crackers that appeared in the newspaper headlines:

John Draper, known as "Cap'n Crunch", discovered that the toy whistle from some cereal boxes produces a 2600 Hz tone that authorizes a free telephone call. He was arrested for illegal use of the telephone company's system in May 1972.

Robert Morris, known as "RTM", accidentally released the first Internet worm in 1988 that infected thousands of computers. He was the first person convicted under the Federal Computer Fraud and Abuse Act of 1986.

Kevin Mitnick, known as “Condor”, was arrested in 1995 for hacking and downloading 20,000 credit card numbers. Mitnick became the first hacker to be on the FBI’s Most Wanted List. He gained notoriety by cracking into the security system at the San Diego Supercomputer Center, ironically, by hacking information from the network security chief’s, Tsutomu Shimomura, computer.

Kevin Polsen, known as “Dark Dante”, was arrested in 1990 for hacking into the phone system of a radio station so that he could be the 102nd caller in a contest to win a Porsche. He also hacked into the FBI’s computer to obtain undercover business names and was featured on NBC’s Unsolved Mysteries.

Vladimir Levin was the first to rob a bank through the institution’s own network, from a laptop in London, England. The Russian hacker group hacked into the Citibank system, obtained accounts, and passwords, and transferred \$10 million to various accounts in United States, Finland, the Netherlands, Germany, and Israel.

Ian Murphy, known as “Captain Zap”, hacked into the AT&T system and changed the internal clocks, which changed the phone rates for day and night time users.

## **Worm and DoS attacks**

### Worms

The most common and damaging attacks on systems and networks are accomplished by releasing computer worms. These incidents are usually headline news and cause millions of dollars in damage and lost revenues. The difference between worms and viruses is that worms can propagate on their own and viruses require a user to initiate. The main characteristic common to both worms and viruses is their ability to infect other hosts by spreading through various media, such as floppy diskettes, file transfers and email attachments. Each new attack can cause a variety of effects, such as abnormal performance, equipment damage, opening back doors for system access at a later time or cause a Denial of Service.

The *Code Red* worm attack in 2001 exploited the `idq.dll` buffer overflow vulnerability, which attacked unpatched Microsoft IIS servers. There were more than 700,000 computers affected and it spread so quickly that investigators could not trace its origin.



In 2003, the *SQL Slammer* worm infected Microsoft SQL 2000 servers that did not have the latest security patch. This worm affected the operations of several major corporations, including Bank of America, where its 13,000 ATM's halted customer withdrawals. Continental Airlines also reported problems with their computer reservation system and had to revert to a manual system using pen and paper. "Experts called it the most damaging attack on the Internet in 18 months as networks across Asia, Europe and the Americas were effectively shut down." (Sieberg, Daniel and Bash, Dana. "Computer worm grounds flights, blocks ATMs" URL:

<http://www.cnn.com/2003/TECH/internet/01/25/internet.attack/>)

The Top 10 worms and viruses for 2002 were *Klez*, *Bugbear*, *Badtrans*, *Elkern*, *Magistr*, *Myparty*, *Sircam*, *Yaha*, *Frethem-Fam* and *Nimda*.

### Denial of Service Attacks

The Denial of Service or DoS, attack is becoming more common today as several readily available tools enable anyone with rudimentary knowledge, and a thirst for causing mischief, to crash systems. This type of an attack can be launched by software tools or by a worm. DoS attacks use various tools, such as ICMP echo, SYNC flood, SYNC requests, out of bounds TCP or overlapping fragment bugs to cause bandwidth consumption and resource starvation. Bandwidth consumption occurs when the attacker has greater bandwidth than the target and floods the target's network with enormous quantities of packets. Resource starvation attacks focus on flooding a system's resources, like CPU, memory, system files and processes.

Distributed DoS (DDoS) attack uses an amplified attack on the target, where the attacker gains access to multiple systems, or networks and commands a DoS attack at a target. This type of attack is much more difficult to trace as the attacker uses so many different sources, and can *spoof* their own IP.

A well known DDoS attack occurred in 2002 when a young Canadian hacker known as "Mafia Boy" launched a DDoS attack causing extended downtime to eBay, Amazon and Yahoo, to name a few. It was estimated that this attack caused \$1.7 billion in lost revenue and damages.

### **Attack trend**

Since the conflict in Iraq began in March 2003, the latest trends on Internet hacking are from "Hacktivists". Peace activists, patriotic Americans and Islamic extremists are changing, or displaying pro-, or anti-war sentiments and slogans

on web sites. In a time span of 2 weeks, over 10,000 defacements have been reported.

One site displayed red, white and blue US map with words "God Bless Our Troops". A web site in Spain expresses "no to war" at URL: <http://www.noalaguerra.org/>. The web site [www.conrado.net](http://www.conrado.net) was hacked and turned into al-Qaeda propaganda in support of attacking the United States.

This growing trend of web site defacements is on the rise, according to Security consultant Andrew Antipass of London's TechServ. "Website defacements are on the rise simply because there are more websites for defacers to hit and fewer companies who are willing to invest time and money into securing their sites." (Delio, Michelle. "Attrition Offs Its Hacker Monitor." URL: <http://www.wired.com/news/culture/0%2C1284%2C43991-2%2C00.html>) According to CSI and FBI, web defacement is estimated to occur on 30 - 40 sites per day and has become a growing underground sport to Cyber Punks.

The growing number of hackers is a major contributor to the increasing number of hacks and attacks reported every day. The increase in the number of hackers may come from the exploits of some famous hackers, their influence on the hacking culture and the growing trend of Internet activists, or "Hacktivists". As hacking becomes more prevalent it is seen more in popular culture, in such video games and movies as "The Net", "Hackers", "Matrix" and "Pi", which may in turn, serve to accelerate the number of hacks. "The 1980s and 1990s also saw the productions of several films that had hackers as primary figures, further imbedding their status as cultural icons." (Thomas, p.xiv)

Computer games can increase popularity in hacking, as well, influence the hacker culture. The computer game "Uplink, Hacker Elite" simulates hacking as an agent, with the game objective of hacking into computers, stealing data, sabotaging other companies, transfer money and erasing evidence.

Other possible reasons for the increase in attacks are the many flaws or weaknesses in software that is released, seemingly, before it is completely debugged. Also, the increasing number of users on the Internet, the automation of attack tools and the availability of hacking materials has surely contributed to the increase in hacking.

“Vulnerable platforms: Windows is still the winner. Microsoft Windows is still the most frequently used platform to launch attacks at 78 per cent on popularity chart. According to the report, this is mostly due to its dominant market share.”  
(Channel Business. February 26, 2003)

As shown in figure 2, from 1999 to 2003, the total incidents that are reported have increased by more than 22 times. At the same time, the number of Internet users grew from 190 million to 544.2 million, about 3.5 times more.

With the increasing number of novice Internet and Microsoft Windows users, the growth in vulnerabilities has given hackers a much larger range of easy targets.

<b>Incidents Reported</b>				6	132	252	406	773	1,334	2,340	2,412	2,573	2,134		3,734	21,756	52,668	82,094
<b>Vulnerabilities</b>											171	345	311	262	417	1,090	2,437	4,129
<b>Internet</b>	213 Hosts		10,000 + Hosts		+							10 million+ Hosts, 45 million users, over 150 countries			150 million users			544.2 million users
<b>Software</b>	MSDOS	MS Windows / System V R3			System V R4	Windows 3.0	Linux 0.01	System V R4.2	Windows NT		Windows 95 / UNIX 95		Internet Explorer 4.0	UNIX 98	UNIX 30	Windows 2000	Windows XP	
<b>YEAR</b>	1981	1983	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000+	2001	2002

Figure 2 - Timeline comparison

(Sources URL: <http://www.cert.org/stats/>,  
<http://www.microsoft.com/museum/mustimeline.mspx#>,  
<http://trident.mcs.kent.edu/~bennett/class/kernel/sum99/notes/unixtimeline.html>,  
<http://www.caffeine.co.za/content/UnixHistory.html>)

## Top Vulnerabilities to Windows Systems

1. Internet Information Services
2. Remote Data Services
3. SQL Server
4. NETBIOS unprotected shares
5. Anonymous Logon – null sessions
6. LAN Manager Authentication – weak LM hashing

7. General Windows Authentication – weak/no passwords
  8. Internet Explorer
  9. Remote Registry Access
  10. Windows Scripting Host
- Figure 3. (March SANS. URL: <http://www.sans.org/top20/#index>)

### Top Vulnerabilities to Unix Systems

1. Remote Procedure Calls
  2. Apache Web Server
  3. Secure Shell
  4. Simple Network Management Protocol
  5. File Transfer Protocol
  6. R-Services – Trust Relationships
  7. Line Printer Daemon
  8. Sendmail
  9. BIND/DNS
  10. General UNIX Authentication – weak/no passwords
- Figure 4. (SANS. URL: <http://www.sans.org/top20/#index>)

### Hacker's Methodology – The 9 steps

#### 1. Footprinting

Footprinting is the process of gathering information on the target. Useful information that is obtained by footprinting are, finding out what systems are internet/intranet, remote access availability, domain names, IP addresses, locations, contact names and email addresses.

Tools for Footprinting are *Unix client*, *web sites*, *search engines*, *nslookup* and *whois* (<http://www.networksolutions.com/whois>).

#### 2. Scanning

This is listening and assessing possible entries with TCP/UDP port scanners by ping sweeping a range of IP addresses and network blocks to determine which ones are alive. Other information obtained by scanning is whether the operating

system is Linux, Microsoft or Novell. Tools for scanning are *fping*, *Superscan*, *nmap*, *Cheops* and *fscan*.

### 3. Enumeration

Enumeration is the process of extracting user accounts and exporting resource names. It is looking for an active connection to the system by probing for user or group accounts, applications and shared resources.

Null session command (`net use \\192.10.10.10\IPC$ "" /u:""`) uses TCP port 139. This will attempt to connect to the IP address (192.10.10.10), IPC\$ (share), as anonymous user (/u:) and null password ("").

Tools for enumeration are *Null sessions*, *Onsite Admin*, *Dumpsec*, *showmount*, *NAT* and *Legion*.

### 4. Gaining access

This is the attempt to access the target, eavesdrop on passwords and use the password guessing, or brute force method on password file shares.

Tools used are *Tcpdump*, *NAT*, *Legion*, *L0phtcrack* and *TFTP*.

### 5. Escalating privilege

The purpose here is to gain full control of the system as administrator, and crack passwords. Tools used for escalating privilege access are *John*, *L0phtcrack*, *Getadmin* and *Sechole*.

### 6. Pilfering

Once the administrator access has been obtained, the hacker can concentrate on the data, and files, and attempt to gain access to other trusted systems.

Tools used for pilfering are *rghost*, *LSA Secrets*, *user data* and *registry*.

### 7. Covering tracks

This is an important step in the attempt to prolong system access by hiding tools from the administrator. Methods for accomplishing this include disabling auditing tools, clearing event and security logs, and clearing the file history. Tools used for covering tracks are *Zap*, *Event log GUI*, *rootkits* and *file streaming*.

### 8. Creating back doors

Back doors are created in order to regain easy entry into the target system in the future. Some methods for creating back doors include creating rogue accounts or installing remote control services, monitoring tools and trojans.

Tools used for back doors are *Netcat*, *remote.exe*, *BO2K*, *Keystroke loggers* and *AT*.

### 9. Denial of Service: DoS or DDoS

It can be used as a hacker's method to have the remote target rebooted by the system administrator, so that changes can take effect. If access to the system was not possible the attacker could cripple the target as a last step.

Tools for DoS attacks are *Smurf*, *Synk4*, *Teardrop*, *Bonk*, *Supernuke* and *ping of death*.

### **Downloading the tools**

The search for hacker tools through the Internet with the key words "Hacker tools" found 758,000 results

(<http://search.yahoo.com/bin/search?p=hacker+tools>). These results included links to sites where hack tools could be downloaded, documentation on how to hack, links to other hack sites, free scripts and procedures to protect your own network. The objective here is to show that tools can be downloaded for each methodology stage and to briefly test the functionality of each tool.

### Footprinting

1. *Sampade* (figure 5) can be downloaded from [www.sampade.com](http://www.sampade.com). This utility is easily installed and takes little harddrive space. The help option can answer most questions on how to use this program. In addition to the *whois* function, *Sampade* also has a ping utility, trace route, finger and nslookup. For example, enter the domain name in the appropriate space; click on *whois* and the screen will display the information.

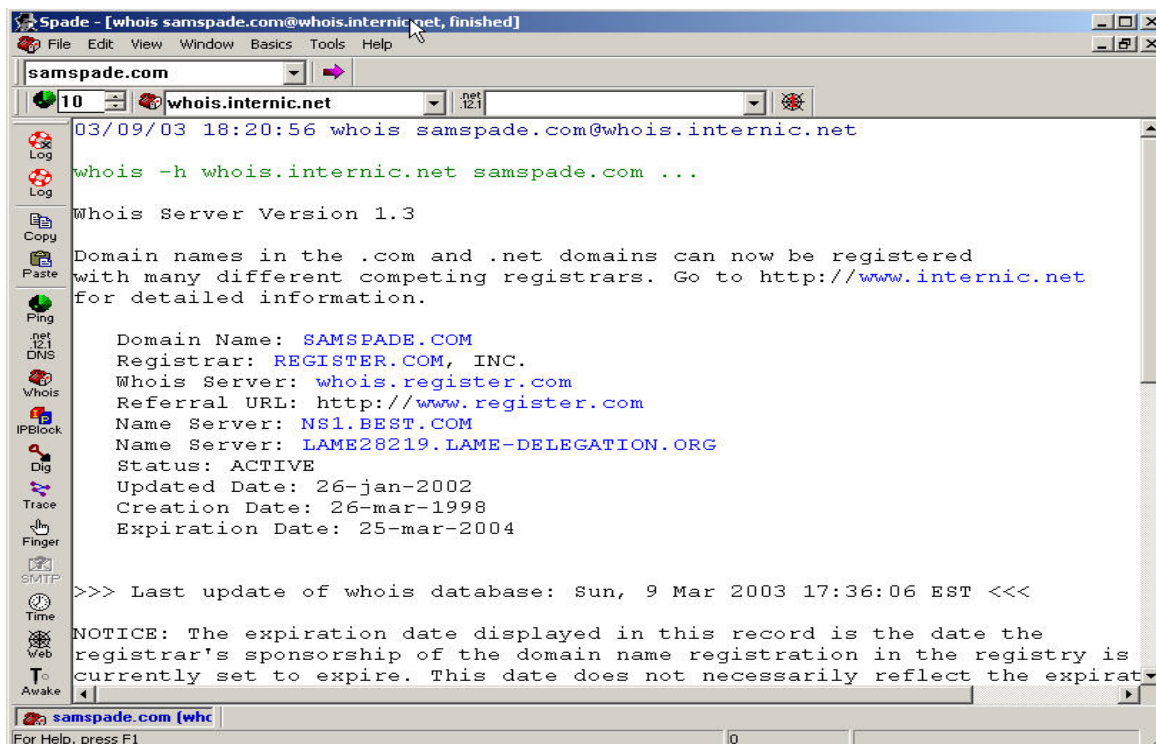


Figure 5 - Samspade

2. NetworkSolutions (<http://www.networksolutions.com>) has an online *whois* utility that can provide information about a domain (figure 6). Click on the *whois* option, type the domain name, choose domain name or network card interface handle and click on *go*. If it is successful, it may display a company name, street address, phone number, fax number, email address and DNS IP address.

a VeriSign® company  
**Network Solutions**

HELP WHOIS VIEW ORDER

HOME DOMAIN NAMES WEB SITES E-MAIL BUSINESS BUILDERS RENEW SERVICES ACCOUNT MANAGER

## WHOIS Search Results

### WHOIS Record for

**networksolutions.com** [Back-order this name](#) [Make an unsolicited offer](#)

Registrant:  
Network Solutions Registrar ([NETWORKSOLUTIONS5-DOM](#))  
505 Huntmar Park Drive  
Herndon, VA 20170-5142  
US

Domain Name: NETWORKSOLUTIONS.COM

Administrative Contact:  
Network Solutions, Inc. ([NSOL-NOO](#))  
Network Solutions, Inc.  
21555 Ridgetop Circle  
Dulles, VA 20166  
US  
888-642-9675 fax: 703-326-7000

Technical Contact:  
idNames Technical Mgr. ([ITM-ORG](#))  
idNames from Network Solutions, Inc.  
440 Benmar  
Suite #3325  
Houston, TX 77060  
US  
281-447-1044  
Fax - 281-447-1160

Record expires on 27-Apr-2011.  
Record created on 27-Apr-1998.  
Database last updated on 6-Mar-2003 00:39:28 EST.

Domain servers in listed order:

NS1.NETSOL.COM	216.168.229.228
NS2.NETSOL.COM	216.168.254.69

customerservice@networksolutions.com

tech@IDNAMES.COM

**Transfer your domain names for only**  
**\$19**  
**a year**  
includes 1 year extension  
[Learn more](#)

Figure 6 – NetworkSolutions whois

## Scanning

Now that contact information has been obtained, the IP address from footprinting can be used in *Superscan* (figure 7). It can be downloaded from the following web site [www.PacketStormSecurity.com](http://www.PacketStormSecurity.com), URL:

(<http://209.100.212.5/cgi-bin/search/search.cgi?searchvalue=superscan&type=archives>).

1. *Superscan* can ping the host and scan TCP ports. It will create a list of each scan adding new hostnames and removing duplicates. When hostnames have been found, clicking on “Browse and Extract from files”, the hostnames can be resolved to the IP addresses. IP addresses then can be used for port scanning or simply scan from the range of addresses, ports, list of ports or list of host names.



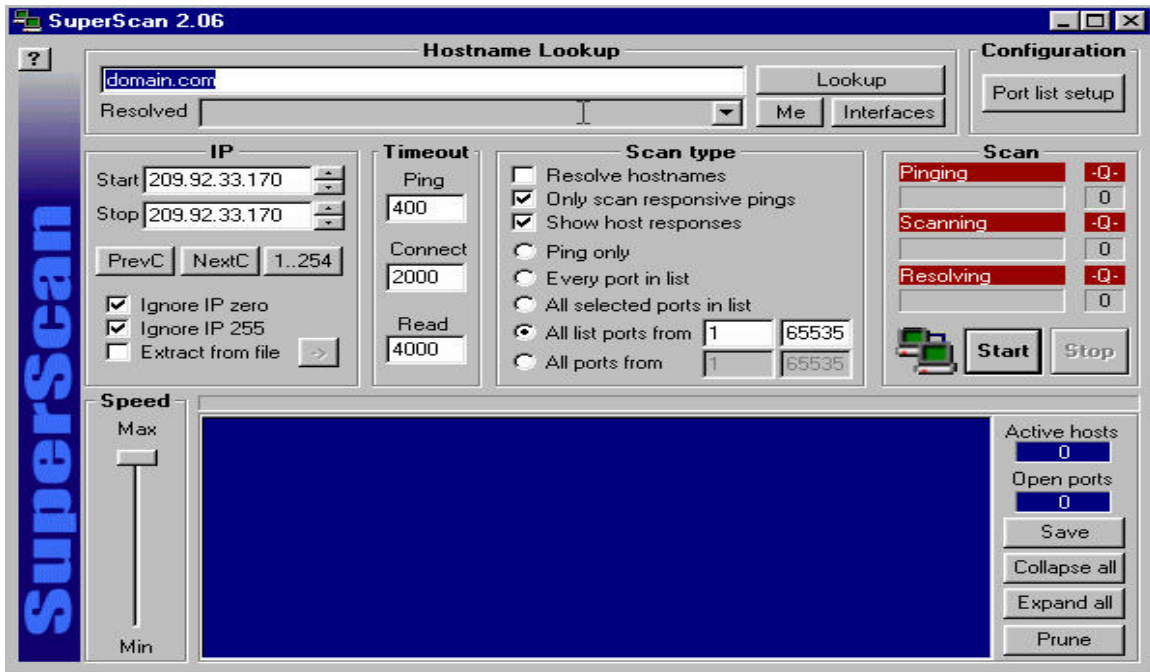


Figure 7 - Superscan

2. *Netscan Pro 3.3* (figure 8) has the option to show graphical or text of all open ports and connections. Installs and creates a desktop shortcut icon and is great tool to look at active port connections from the target system. It can be downloaded from the following URL:

[http://www.answerthatwork.com/Downright\\_pages/downrights\\_internet.htm](http://www.answerthatwork.com/Downright_pages/downrights_internet.htm).

© SANS Institute



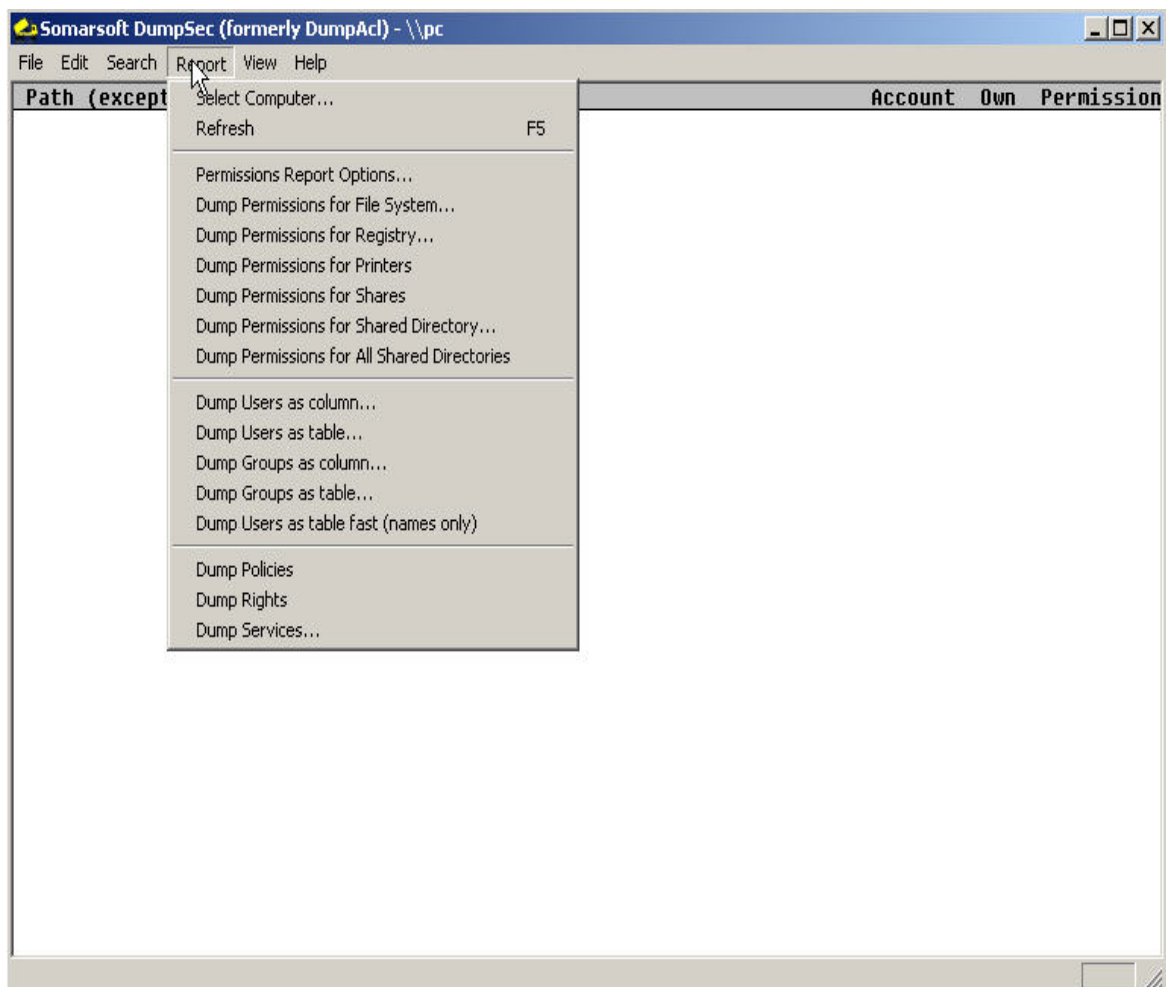


Figure 9 – *Dumpsec*

### Gaining access

*Legion* (figure 10) can be downloaded at <http://packetstormsecurity.nl/>. It can scan IP address ranges for NETBIOS shares and allows you to map to the drive. New versions of *Legion* allow the brute force method for password hashing on protected shares. A successful scan will display the IP address and the share names.

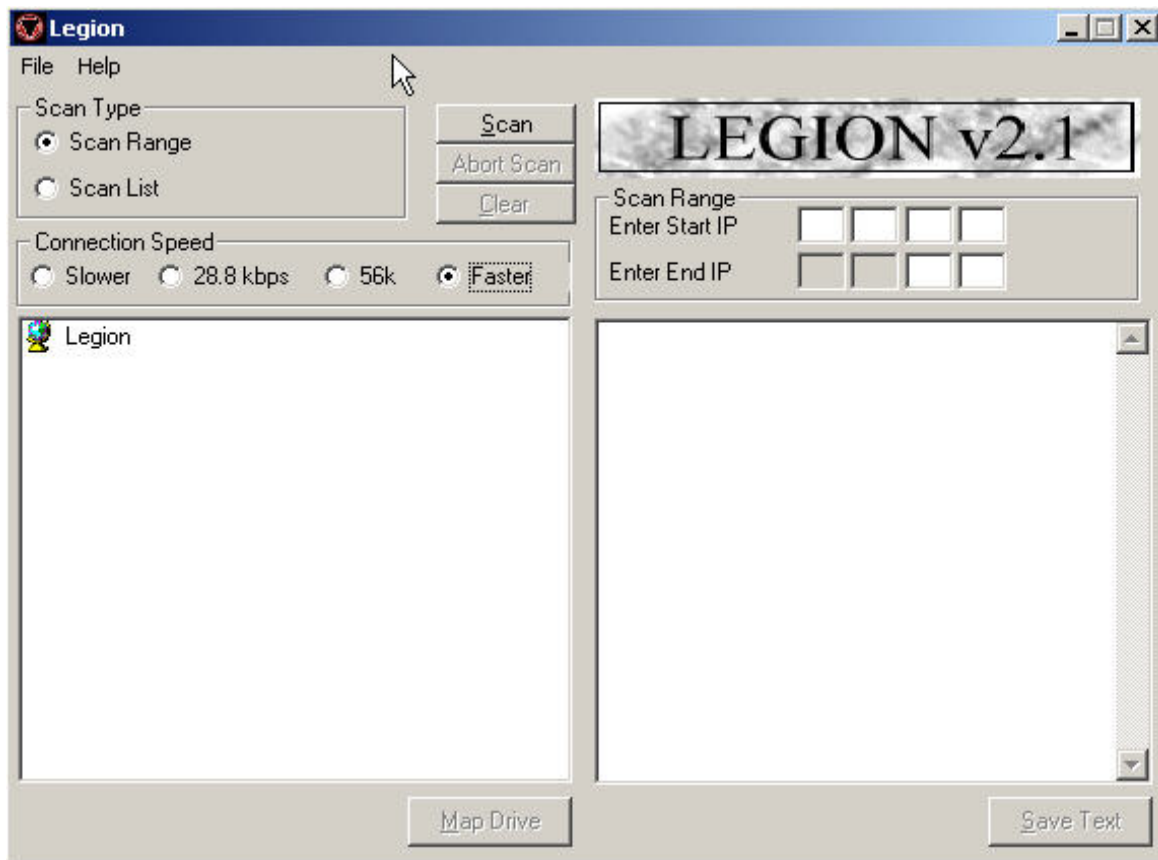


Figure 10 – *Legion v2.1*

### Escalating privilege

@*Stake LC4* (figure 11) is a password audit and recovery tool. It has the capability for sniffing passwords through the network using SMB Packet Capture.

It can recover passwords from local or remote machines, as well as from an NT 4.0 emergency repair disk. A trial version can be downloaded from URL: <http://www.atstake.com>.

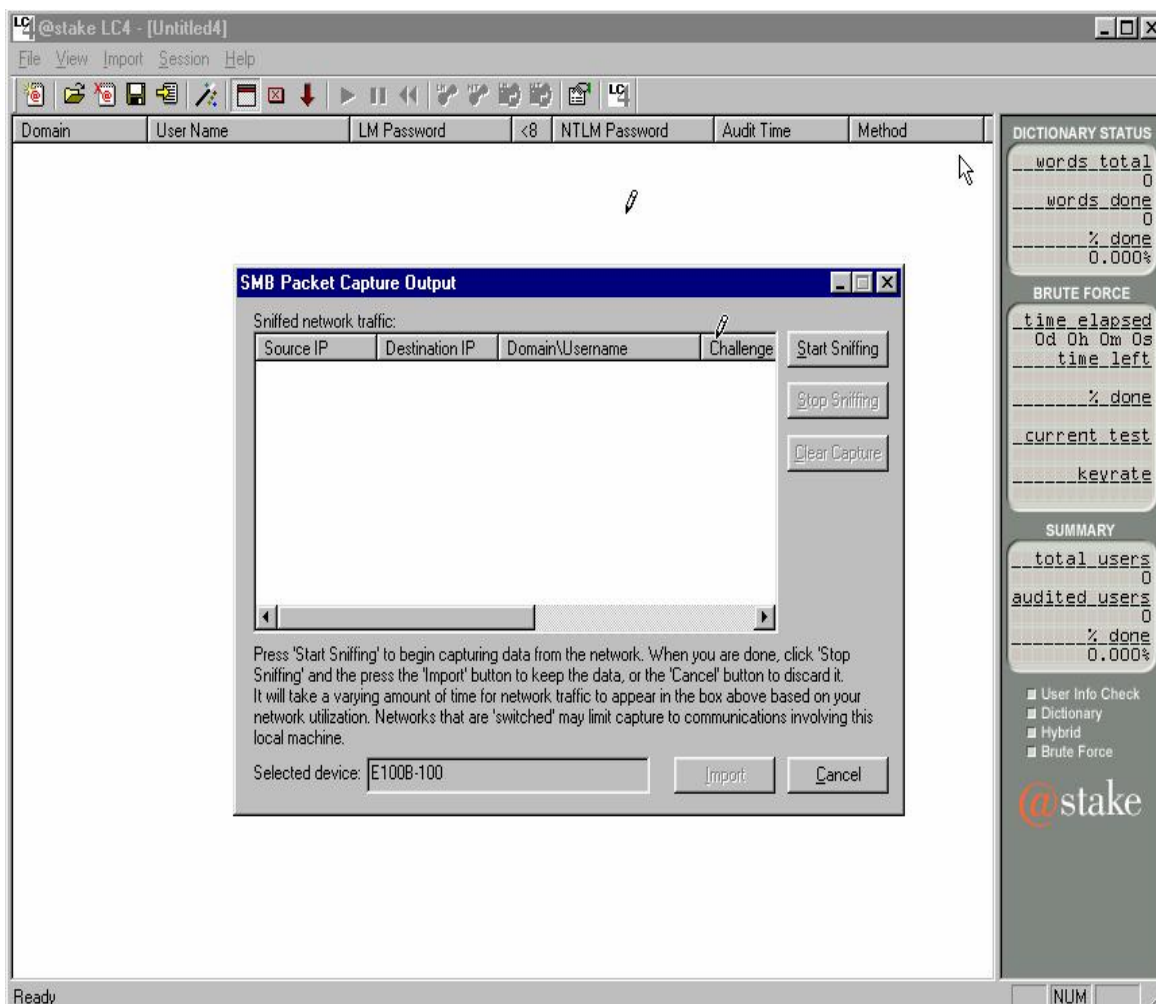


Figure 11 - @Stake LC4

## Covering tracks

*Clear Logs* (figure 12) can be downloaded from <http://www.ntsecurity.nu/toolbox> and is a DOS command that allows one to clear local and remote system logs. Command usage and options are shown when the command is typed and entered.

```
C:\WINNT\System32\command.com
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>clearlogs

ClearLogs 1.0 - (c) 2002, Arne Uidstrom (arne.uidstrom@ntsecurity.nu)
               - http://ntsecurity.nu/toolbox/clearlogs/

Usage: clearlogs [\\computername] <-app / -sec / -sys>

        -app = application log
        -sec = security log
        -sys = system log

C:\>
```

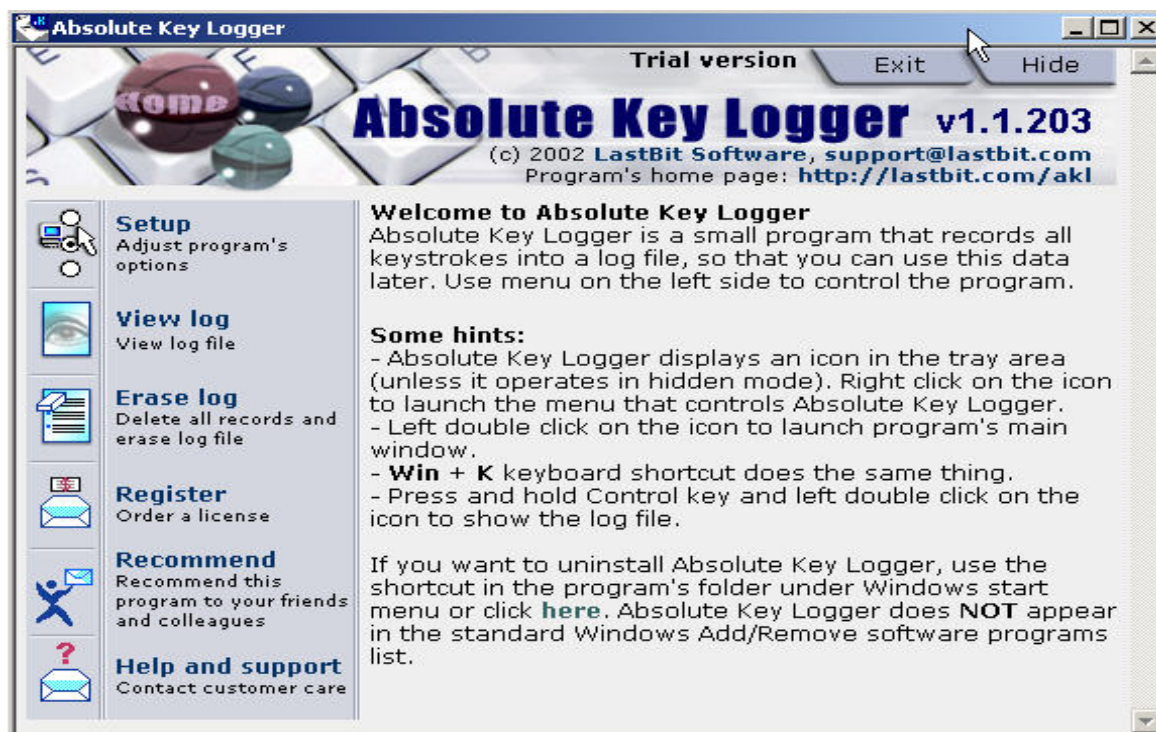


Figure 13 – Absolute Key Logger

## Denial of Service

*Aggressor\_Exploit Generator v0.85* (figure 14) can be downloaded from URL: <http://209.100.212.5/cgi-in/search/search.cgi?searchvalue=smurf&type=archives>.

The utility works on Windows 95 or 98 and requires a modem and Internet dialup connection. The program doesn't require installation and runs on execution. The program has the following options: packet builder, debug mode, smartports, spoofed attack, land attack, smurf, nestea and boink attack. It also comes with a manual.txt file explaining all the functions.



Aggressor Exploit Generator v0.85 Prerelease
info@aggressor.net

Hook 2F8
Device Cannot Detect Modems..
CTS
DTR
TxD
RxD

[WSA] WinSock 2.0Running  
[WSA] Local Host is co-doig3xrdb4xz  
[DDH] NO MODEMS DETECTED , Configure Manually ..(Using default value 2f8)  
[DDH] VERSION : Aggressor Direct Device Library V0.7(c)  
[PPP] VERSION : WinPPP 2.7.Aggessor  
[PPP] Running for , DR0-4 Hooked

MTU Size 1500
RWINSize 2048
HWR. WState 3
Modem CT Normal

IP HEADER

IP Protocol 0
IP Version 4 HL 5
Time to live 255
Fragment Off 40

IP SRC 127.0.0.1 139
IP DST 255.255.255.0 139

IP Tos 0
Packet len. 40
P. ID 0
Checksum 0

TCP
ICMP
☐ Override IP Protocol

Src Port 139
Dst Port 139
TCP Seq. 65536
ACK 255
Offset 20

WinSize 20
URP 255
Load Data

Flags
☐ Urgent Flag
☐ Reset Flag
☐ Fin Flag
☐ Push Flag
☐ ACK Flag
☐ SYN Flag

delay between packets 500
# of packets to be send : 1

Send Packet
Listen Port
Save attack
Load Attack
Simple mode
Terminate
About

Figure 14 – Aggressor Exploit Generator v0.85

## Web hacking

Web pilfering is the process of gathering information about the host or network from web pages and HTML source code. When pilfering larger web sites automated tools or scripts can be used for keyword searching.



*Grinder v1.1* (figure 15) is a tool that can scan a range of IP addresses and provide a list of the web server name and version. *Grinder* can scan a specific web site name if a name is entered in the URL field. A successful scan will display the server name, web server version and all the vulnerabilities it has. *Grinder v1.1* can be downloaded from the following URL:  
<http://www.siamstreet.com/kenny/www/warez.html>.

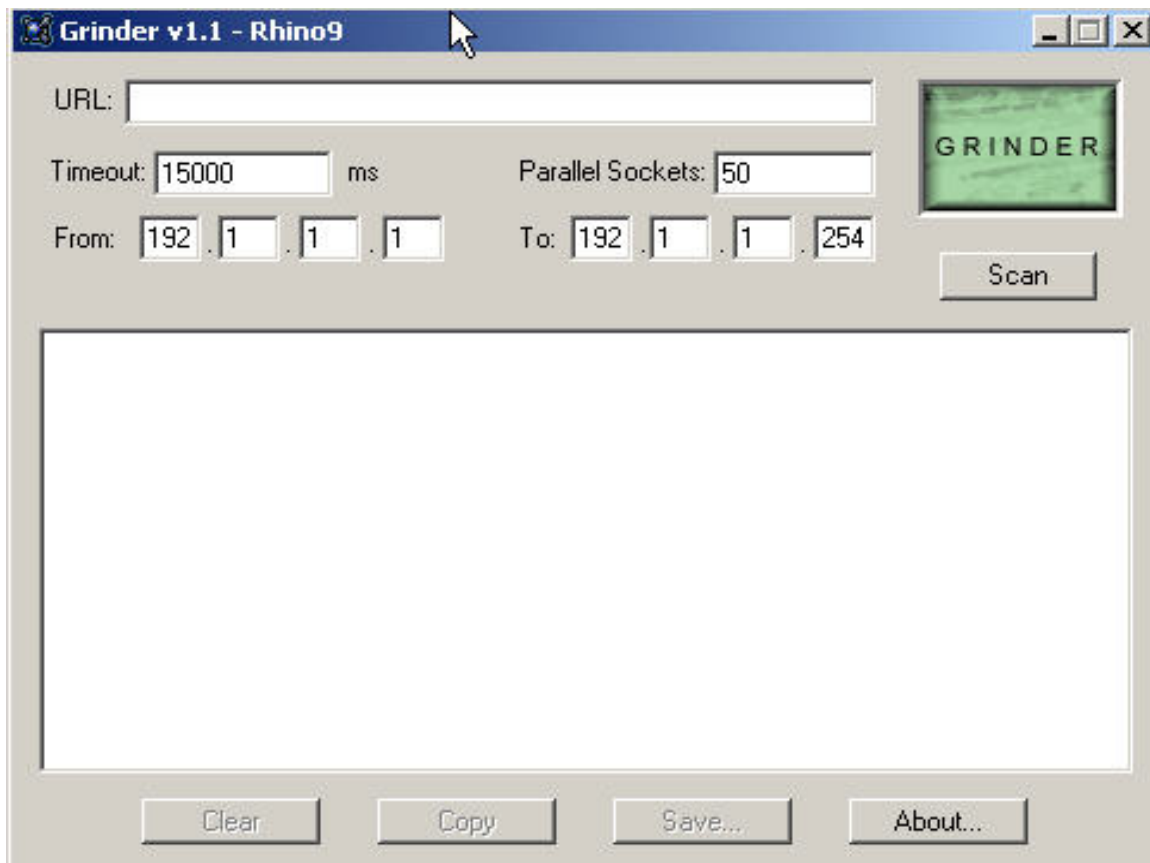


Figure 15 – *Grinder v1.1*

*Twwwscan v1.2* (figure 16) is a command line utility that can scan up to 400 known www/cgi vulnerabilities. A successful scan will display the HTTP header

and web server information. Twwwscan v1.2 can be downloaded from the following URL: <http://packetstormsecurity.nl/UNIX/cgi-scanners/indexsize.shtml>.

```

C:\WINNT\System32\command.com

Don't tell your web server free from attack      twwwscan 1.2  2001/02/19
                                                made by pilot
                                                http://search.iland.co.kr

usage      : twwwscan <server> <port> <display> <type> <pmode> <a_idsmode>
<display>  : -v(<0.6>) scan type<display status> or -n(no display)
<type>     : -t1(use GET),-t2(scan virtual host),-t3(virtual and GET) or -n
<pmode>    : passive mode scan -pw(windows) -pu(unix) -pa(ALL) or -n(no apply)
<a_idsmode>: -ids(Anti-IDS mode URL Encoding)

example 1  : twwwscan drill.hackerslab.org 80
example 2  : twwwscan 127.0.0.1 80 -v
example 3  : twwwscan target.com 80 -n -n -pw
example 4  : twwwscan virtual.yourhost.com 8080 -v -t3 -pu
example 5  : twwwscan idstest.yourhost.com 80 -v -t1 -pa -ids

contact    : search@iland.co.kr (<http://search.iland.co.kr>)

Tested On  : Windows 950SR2,98,98SE,NT4,2k,Me

thanks r0ar,korea security guys,kuol(he designed the twwwscan logo)
Dug Song(monkey.org),UNYUN(Shadow Penguin Security),Roelof(a author of pudding)

Powered by Borland C++ 5.5 (<http://www.borland.com>)
  
```

Figure 16 – Twwwscan v1.2

## Hacking with LINUX

(Source: Hacker's Manual. URL: <http://www.cleo-and-nacho.com/mainpages/hacking.htm>)

### Basic commands

DOS	LINUX (case sensitive)
DIR/W	ls (shows directory across the screen format)
DIR	ls -l (shows directory list format)
DIR/AH	ls -al AHY=(hidden) -al=(include hidden files) (shows directory)
RENAME	mv (rename)
ATTRIB	chmod (shows attributes)
MD	mkdir (make directory)
RD	rmdir (remove directory)
DEL	rm (delete)

COPY                    cp     (copy)(example: cp filename \$HOME)  
 CD                    cd     (takes you to home directory)  
                       (cd ~username)

## File Permissions

ls -l (shows files and directory, figure 17)

ls -al (shows hidden files and directory, figure 17)

```

[root@localhost gz32t2]# ls -l
total 16
drwxrwxr-x  4 gz32t2  gz32t2    4096 Apr 10 19:16 Desktop/
drwxr-xr-x  3 gz32t2  gz32t2    4096 Apr 12 07:59 Documents/
-rw-rw-r--  1 gz32t2  gz32t2      53 Apr  9 18:36 linux
drwx----- 2 gz32t2  gz32t2    4096 Apr  7 16:28 tmp/
[root@localhost gz32t2]# ls -al
total 160
drwxr-xr-x 15 gz32t2  gz32t2    4096 Apr 12 08:29 ./
drwxr-xr-x  3 root    root      4096 Apr  7 16:28 ../
-rw-----  1 gz32t2  gz32t2    438 Apr  7 19:45 .bash_history
-rw-r--r--  1 gz32t2  gz32t2     24 Apr  7 16:28 .bash_logout
-rw-r--r--  1 gz32t2  gz32t2    191 Apr  7 16:28 .bash_profile
-rw-r--r--  1 gz32t2  gz32t2    124 Apr  7 16:28 .bashrc
-rw-rw-r--  1 gz32t2  gz32t2     56 Apr 12 07:28 .DCOPserver_localhost__0
lrwxrwxrwx  1 gz32t2  gz32t2     37 Apr 12 07:28 .DCOPserver_localhost__0
-> /home/gz32t2/.DCOPserver_localhost__0
-rw-rw-r--  1 gz32t2  gz32t2     12 Apr  7 17:02 .desktop
drwxrwxr-x  4 gz32t2  gz32t2    4096 Apr 10 19:16 Desktop/
drwxr-xr-x  3 gz32t2  gz32t2    4096 Apr 12 07:59 Documents/
-rw-rw-r--  1 gz32t2  gz32t2      0 Apr  7 17:01 .drakfw
-rw-rw-r--  1 gz32t2  gz32t2   33580 Apr 12 08:29 .fonts.cache-1
drwx----- 2 gz32t2  gz32t2    4096 Apr  7 19:47 .gconf/
drwx----- 2 gz32t2  gz32t2    4096 Apr  7 19:47 .gconfd/
drwx----- 3 gz32t2  gz32t2    4096 Apr 10 19:36 .gnome/

```

Figure 17 - File permissions

Row #1 is the file permissions

Row #2 is who owns the file

Row #3 is the group owner of the file

File permissions are grouped together into three different groups.

If the line starts with a letter “d”, then it is a directory. If there is no d, then it is a file.

```

- - - - -
| | | |-----> Other = anyone on the machine can access
| | | |-----> Group = certain groups can access
| | | |-----> User = only the owner can access
|-----> Directory Mark

```

```

- rw- r-- r--
| | | |-----> Other can only read the file

```

```

| | |-----> Group can only read the file
| |-----> User can read or write to the file
|-----> It is not a directory

```

- rwx rwx r-x

```

| | |-----> Other can read and execute the file
| |-----> Group can read write and execute the file
| |-----> User can read write and execute the file
|-----> It is not a directory

```

Some commands to use if you own the file or have root access.

```

chmod o+rw filename    (all 3 groups permission with read)
chmod og-r filename    (makes file read to user that owns the file)
chmod +x filename      (makes file execute by all)
chown username filename (change file owner)
chgrp groupname filename (change file to own by another group)

```

## Footprinting

From a shell, the following command “finger @domainName.com” or “finger -l @domainname.com” can be used to find usernames that has logged on to that domain, shown in figure 18.

```

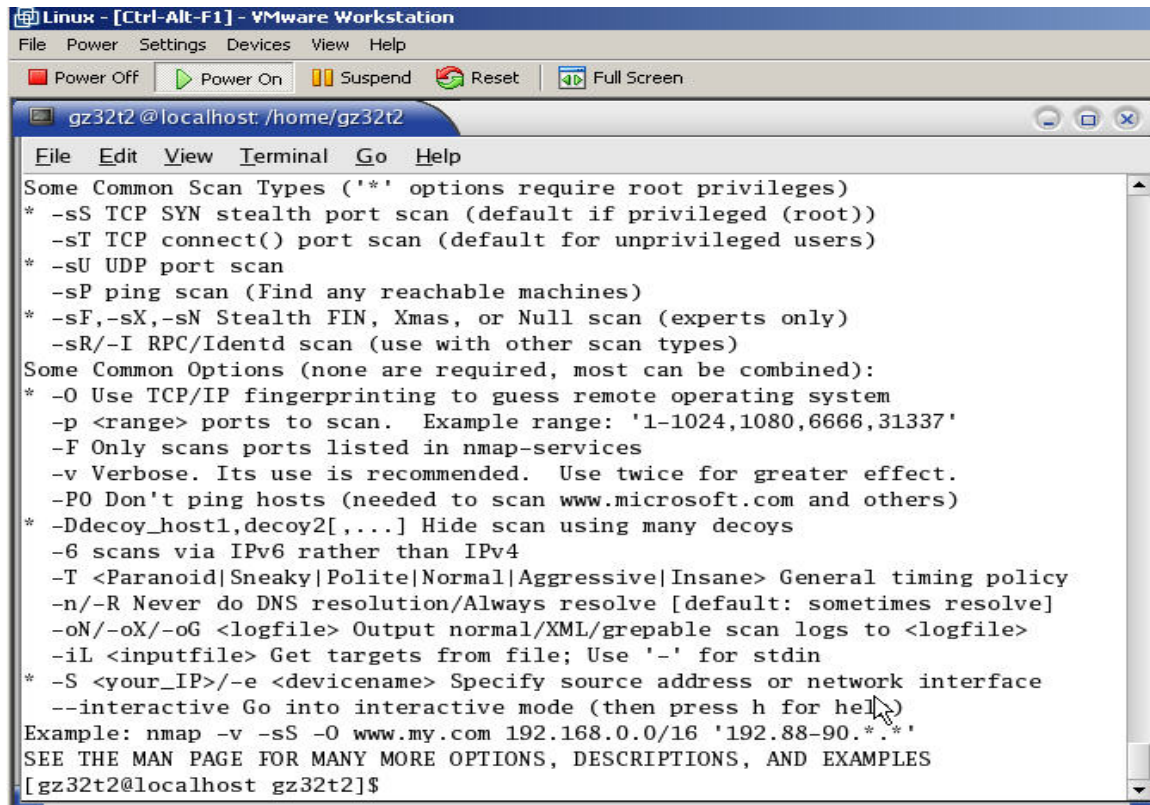
Linux (2) - [Ctrl-Alt-F1] - VMware Workstation
File Power Settings Devices View Help
Power Off Power On Suspend Reset Full Screen

[root@localhost root]# finger
Login   Name    Tty     Idle    Login Time   Office      Office Phone
root    root    tty1    Apr 15 20:58
[root@localhost root]#
[root@localhost root]#
[root@localhost root]# finger -l
Login: root                               Name: root
Directory: /root                         Shell: /bin/bash
On since Tue Apr 15 20:58 (PDT) on tty1
No mail.
No Plan.
[root@localhost root]# _

```

Figure 18 - finger  
Scanning

*Nmap* is a tool for TCP and UDP port scanning, figure 19 shows command usage and options. This tool can be downloaded from the following URL:  
[http://www.insecure.org/nmap/nmap\\_download.html](http://www.insecure.org/nmap/nmap_download.html).



The screenshot shows a Linux terminal window titled "Linux - [Ctrl-Alt-F1] - VMware Workstation". The terminal is running a command prompt for a user named "gz32t2" at "localhost". The prompt is "[gz32t2@localhost gz32t2]\$". The terminal output displays the following text:

```
File Edit View Terminal Go Help
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
  -sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan. Example range: '1-1024,1080,6666,31337'
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended. Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -6 scans via IPv6 rather than IPv4
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
[gz32t2@localhost gz32t2]$
```

Figure 19 – *nmap*

## Enumeration

*Telnet* can be used to connect to a host, example of the command are “telnet machine.com” or “telnet 206.146.43.56”. Its options are displayed by typing *help*, shown in figure 20.

Trying.....

Connected to machine.com

Linux 2.0.28 (mahine.com) (ttyp0)

Machine login:username

Password:#####



bash\$

Notice the O/S version “Linux 2.0.28” that was obtained from the host.

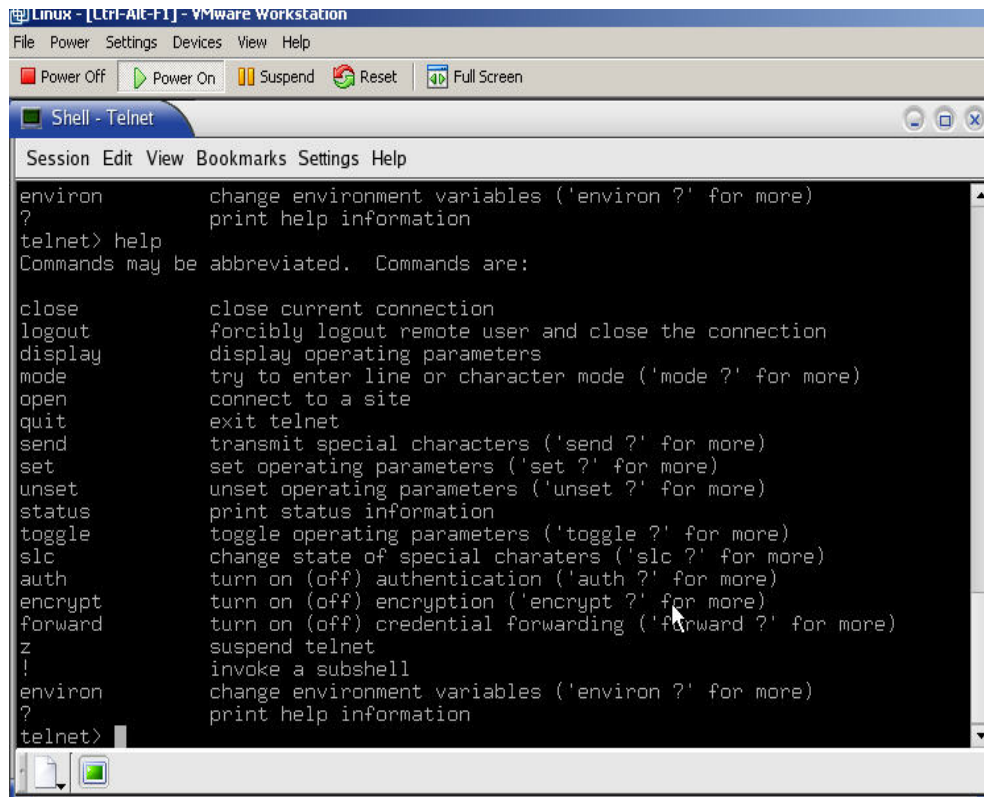


Figure 20 - telnet

### Gaining access

*John the Ripper* is a program that can crack password files and can be downloaded from the following URL: <http://www.openwall.com/john/>.

*Crackerjack* is a program that attempts to hash the password against a password file and a word file. By entering the password file in the Word file prompt, this will attempt to get the user ID information first. Hash will attempt adding numbers in front or at the end of words, like 1sally or sally1.

D:\jack

Crack Jack Ver 1.4 OS/2 and DOS  
Copyright © 1993

PWFile(s): domain.com.passwd

Wordfile : domain.com.passwd

### Escalating privilege

*Fake SU* (Trojan) can be used to get the administrator's root password. To do so, change the shell script so that a hidden directory is searched before all others. Then copy the *fake su* binary into the directory. When the administrator logs on with the *su* command, everything will look normal and the system will prompt for the password. At this time, the password will be automatically copied into the log file `/tmp/.elm69` and the program will delete the *su* Trojan. It will return a password wrong error and request it to be entered again. The administrator attempts to enter the password again and this time the real *su* executes and logs in successfully.

```
gcc su.c -o su
```

.bash\_profile might look like this:

```
# .bash_profile
```

```
# Get the aliases and functions
```

```
if [ -f ~/.bashrc ]; then
```

```
    . ~/.bashrc
```

```
fi
```

```
# User specific environment and startup programs
```

```
PATH=$PATH:$HOME/bin
```

```
ENV=$HOME/.bashrc
```

```
USERNAME=""
```

```
export USERNAME ENV PATH
```

You change the first line to: `PATH=$HOME/.term:$PATH:$HOME/bin`

## Pilfering

Rlogin requires a `.rhosts` file in the home directory that tells the system where to receive rlogin from. Adding `++` under their host name would allow users to rlogin without a password. The idea is to target systems without the `“rhosts”` file.

Figure 21 shows the usage of the command.

```
rlogin -l username hostname
```

```
connecting.....
```

```
password:
```

```
bash$
```

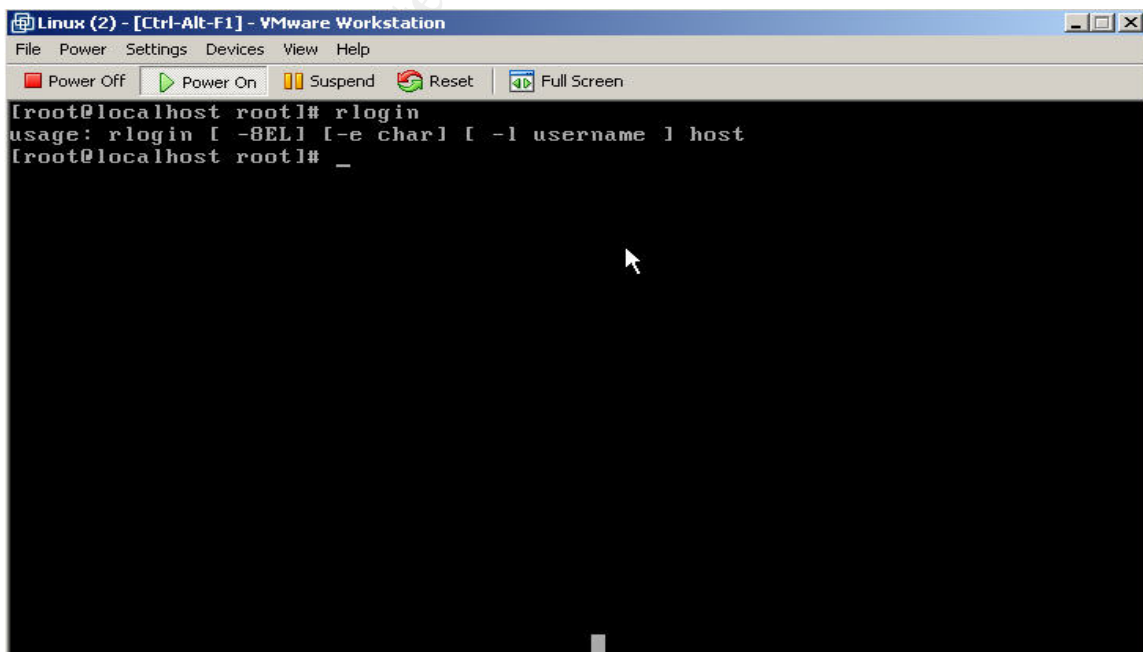


Figure 21 - *rlogin*



## Covering tracks

Making yourself invisible by cleaning up the traces from utmp, wtmp, xferlog and other logs are very important to maintaining access to the system. Have a routine to go in quietly, write down the activity when connected and cleanup before disconnecting. *Zap2* is a program for cleaning wtmp, lastlog and utmp files.

## **Useful Hacking links and resources**

Site with Unix hacking tools.

<http://www.thenewbiesarea.com/unix.shtml>

Download scanners and various hacking tools.

<http://www.siamstreet.com/kenny/www/warez.html>

Download sniffers, scanners, key loggers and network utilities.

<http://xstem.com/hdloads.htm>

Searches the links with your keywords, mostly hacking related sites.

<http://www.warezcrawler.net>

Links to other hacking sites.

<http://dmoz.org/Computers/Hacking/Cracking/>

Site has Trojans, such as Executor, Y3K Rat versions 1.5 and 1.6 for downloading.

<http://storm.prohosting.com/~0v3rrid3/morphmenu.html>

Send \$10 for a CD of various hacking files, tools and cracks.

[www.cleo-and-nacho.com/mainpages/hacking.htm](http://www.cleo-and-nacho.com/mainpages/hacking.htm)

Site has Trojans, key loggers and port scanners for downloading.

<http://storm.prohosting.com/~0v3rrid3/morphmenu.html>

Support documentation on how to hack, and some tools.

<http://www.accessorl.net/~cyberwar/codehacks.html>

Download Trojans, viruses, hack tools, nukes and mail bombs.

<http://www.geocities.com/robsnewbiehacking/openingpage.htm>

Online bookstore, 281 titles with the keyword *hacking*.

<http://search.barnesandnoble.com/booksearch/results.asp?WRD=hacking&userid=2V0755>

Step by step on how to deface web sites.

<http://www.volny.cz/rootshell/deface1.htm>

Published magazine, 2600 (figure 17) -The Hacker Quarterly.

<http://www.2600.com/>

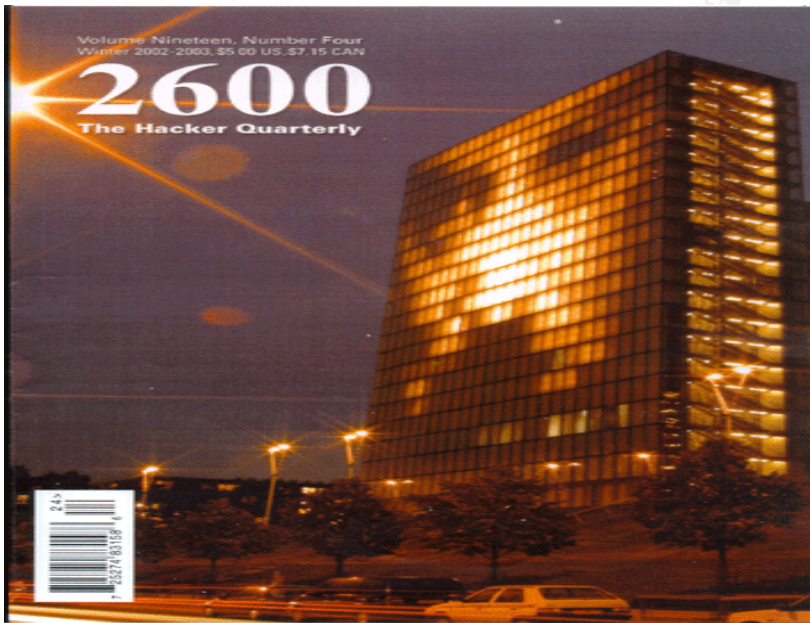


Figure 17 – 2600 The Hacker Quarterly

## Conclusion

Hackers can be of any age, from any country and with the ability ranging from beginner to expert. The increase in Internet attacks could be related to several factors, such as the growth in Internet users, increasing vulnerabilities in new software releases, ease of obtaining hacking tools and resources, and the increasing numbers of hackers.

As demonstrated, trojans, viruses, hacking tools and documentation are available for downloading through the Internet and provide a virtually endless amount of resources. These tools were downloaded and proven to be fully functional. As well, professional training and certification is now available through respected training institutions.

Hacking is increasingly emerging from the shadows whereby anyone with an Internet connected computer, spare time, and a little motivation can learn to hack.

## References

### Books:

Thomas, Douglas. Hacker Culture. University of Minnesota, 2002.

Freedman, David H and Mann, Charles C. @Large. Simon and Schuster, 1997.

McClure, Stuart; Scambray, Joel and Kurtz, George. Hacking Exposed. McGraw-Hill, 2001.

"Are you vulnerable?" Channel Business. February 26, 2003: 23-25.

Online:

"Hackoo search!" URL: <http://www.cleo-and-nacho.com/mainpages/hacking.htm> (Feb 2, 2003).

"Crackazoid" URL: <http://crackazoid.com/> (Feb 2, 2003).

"Rent A Hacker" URL: <http://www.rent-a-hacker.com/> (Feb 25, 2003).

"CERT/CC Statistics 1988-2002" URL: <http://www.cert.org/stats/> (Feb 25, 2003).

Delio, Michelle. "Attrition Offs Its Hacker Monitor." URL: <http://www.wired.com/news/culture/0%2C1284%2C43991-2%2C00.html> (March 2, 2003).

Kobes C, Jason. "Cyber Attacks." URL: <http://www.public.iastate.edu/~jkobes/Attacks/index.htm> (March 2, 2003).

"White Hat vs. Black Hat" URL: [http://www.infosecnews.com/opinion/2002/12/11\\_01.htm](http://www.infosecnews.com/opinion/2002/12/11_01.htm) (March 2, 2003).

"@stake" URL: <http://www.atstake.com/research/lc/download.html> (March 2, 2003).

"Anycrack" URL: <http://anycracks.com/?p=L1> (March 2, 2003).

"Warecrawler search" URL: [http://www.warezcrawler.net/cgi/sections.php4?bottom=0&section=hacking\\_phreaking](http://www.warezcrawler.net/cgi/sections.php4?bottom=0&section=hacking_phreaking) (march 2, 2003).

"Rob's game" <http://www.geocities.com/robsnewbiehacking/misc.htm> (March 2, 2003).

Carlson, David. "David Carlson's Online Timeline" URL: [http://iml.jou.ufl.edu/carlson/professional/new\\_media/90s.htm#00s](http://iml.jou.ufl.edu/carlson/professional/new_media/90s.htm#00s) (March 4, 2003).

"Life on the Internet" URL: <http://www.pbs.org/internet/timeline/index.html> (March 4, 2003).

"DumpSec download" URL: <http://www.somarsoft.com/> (March 4, 2003).

"2600 -The Hacker Quarterly" URL: <http://www.2600.com/> (March 4, 2003).

"Hackersmiling downloads" URL: <http://www.hackersmiling.com/utilities.html> (March 13, 2003).

"SANS/FBI top 20 list" URL: <http://www.sans.org/top20/#index> (March 13, 2003).

"Hacking Exposed" URL: <http://www.hackingexposed.com/tools/tools.html> (March 13, 2003).

Quittner, Jeremy. "Hacker Psych 101"  
URL: <http://tlc.discovery.com/convergence/hackers/articles/psych.html> (March 17, 2003).

Packet Storm Security. URL: <http://packetstormsecurity.nl/groups/rhino9/> (March 17, 2003).

Netscan tools download. URL: [http://www.answersthatwork.com/Downright\\_pages/downrights\\_internet.htm](http://www.answersthatwork.com/Downright_pages/downrights_internet.htm) (March 20, 2003).

"Microsoft Museum – Microsoft timeline" URL: <http://www.microsoft.com/museum/mustimeline.msp#> (March 21, 2003).

"UNIX timeline" URL: <http://trident.mcs.kent.edu/~bennett/class/kernel/sum99/notes/unixtimeline.html> (March 21, 2003).

Ritchie, Dennis and Thompson, Ken. June 1972

"History and timeline" URL: <http://www.caffeine.co.za/content/UnixHistory.html> (March 21, 2003).

"Stats and Graph" URL: <http://zone-h.org/en/stats> (March 24, 2003).

“The Inside story on cyber graffiti” URL:

[http://www.etest-associates.com/pressroom/pr\\_website\\_defacement\\_artcl.htm](http://www.etest-associates.com/pressroom/pr_website_defacement_artcl.htm)

(March 25, 2003)

Sieberg, Daniel and Bash, Dana. “Computer worm grounds flights, blocks ATMs”

URL: <http://www.cnn.com/2003/TECH/internet/01/25/internet.attack/> (April 1, 2003)

Alley, Byron. “SDMI Pays Hackers \$5000” URL:

<http://www.winplanet.com/winplanet/opinions/2717/1/> (April 03, 2003)

Hacking Unix download. URL:

<http://www.thenewbiesarea.com/unix.shtml> (April 3, 2003)

The Living Internet. URL: [http://livinginternet.com/?i/ia\\_hackers\\_draper.htm](http://livinginternet.com/?i/ia_hackers_draper.htm) (April 8, 2003)

“Featured games” URL: <http://www.strategyfirst.com/en/> (April 15, 2003)

© SANS Institute 2003, Author retains full rights.