Interested in learning
more about security?

# SANS Institute
# InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

## Battle for the Internet: The War is On!

There is a battle raging between security professionals and hackers. By placing people into the shoes of a hacker, and teaching them the skills to gain access to a system, one is better able to defend against them. As a hacker, we dig up information on companies/individuals by mirroring their websites, using search engines, whois databases and traceroute. Next, we move to "Scanning." We ping their computers, look at which ports are open, identify their operating system, map their networks, and see if they have any avai...

Copyright SANS Institute
Author Retains Full Rights

AD

CounterTack
Counter Tack Active Monitors
for In-Progress Attacks
GET THE
WHITE PAPER
NOW >>>

GIAC Security Essentials Certification (GSEC)
Practical assignment Version 1.4b – Option 1

**Battle for the Internet: The War is On!**

Kevin J. Owens
April 20, 2003


## ABTSRACT

There is a battle raging between security professionals and hackers. By placing people into the shoes of a hacker, and teaching them the skills to gain access to a system, one is better able to defend against them. The first step is "Foot Printing/Reconnaissance." As a hacker, we dig up information on companies/individuals by mirroring their websites, using search engines, *whois* databases and *traceroute*. Next, we move on to "Scanning." We *ping* their computers, look at which ports are open, identify their operating system, map their networks, and see if they have any available modem connections. Then we move on to "Enumeration," looking at valid user accounts and network shares. To "Gain Access" we search for vulnerabilities our opponent has, crack their passwords, and *sniff* the data on their network. "Escalating Privilege" is the next step to go from a low-level user account to having administrator equivalency. With these privileges, we manipulate files and directories to help us "Maintain Access" with the help of *backdoors*, *rootkits*, and *Trojans*. Lastly, we do not want to loose our accounts hence we "Cover Our Tracks" by modifying or deleting log files, hide files, and use protocols covertly to hide what we are doing. If computer security professionals stay on the cutting edge of hacker tools and methods of entry, they will be able to defeat hackers before they even get started on your systems.


## INTRODUCTION

There is a war going on, did you know that? Everyday there are people using the Internet to declare a war on both individuals and computers. There are two sides to this battle: on the one side is the security professional in the trenches trying to defend, and on the other side, there is the hacker (cracker).

Well over 2,000 years ago, a great Chinese warrior-philosopher, Sun Tzu, wrote "The Art of War" (Tzu). People have translated Master Sun Tzu's writings and related them to the business/corporate world. Now, let us relate them to Computer Security, since it is a battlefield! If you do not think so, then why were over 20,000 websites hacked in the first week of the war with Iraq (Warner)?

We are going to look at the side of the hacker, because if you know your enemy you will be better able to defend yourself or your clients. The steps you may take as a hacker against your opponent are (McClure):

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Foot Printing/Reconnaissance
  - This is the step where we want to get as much information about our opponent without being intrusive. Things like target address ranges, namespace acquisitions, and information that will be beneficial in deeper attacks.
- Scanning
  - This is where we want to assess our opponent's systems. What operating system do they use? What ports are they listening on? We are looking for vulnerable places to enter into their systems.
- Enumeration
  - Next, we go a little deeper in our attacks to attempt to identify valid user accounts or poorly protected network shares.
- Gaining Access
  - Now that we have some information, we begin to attempt to access our opponent's computers.
- Escalating Privilege
  - If we have gained a low-level user account, we will now escalate our privilege to that of an administrator equivalency.
- Creating Backdoors/Maintaining Access
  - We do not want to loose our access to our opponent's machines; hence, we create *backdoors* to come back in with privileged access.
- Covering Your Tracks
  - Not getting caught, or not having our "new" accounts be erased is important, so we need to hide our activities.

Let us look at these steps one at a time.

But first, no one wants to get caught scanning computers, so use an anonymizer or proxy. There are numerous ones available online, here are a few:

http://www.amegaproxy.com
http://www.anonymizer.com
http://www.proxys4all.com/web-based.shtml (Has several choices)

Alternatively, try the **MultiProxy** program, which you can download at:

http://www2.multiproxy.org/mproxy12.zip
http://www.multiproxy.org/anon_proxy.htm (Anonymous Proxy List)

For more information on being Anonymous, read this article (http://www.elitehackers.com/fi1/hacking/anonymity.txt), and some interesting links, are at the bottom of this page (http://www.uwasa.fi/~ts/http/anonpost.html).

***"Military action is important to the nation – it is the ground of death and life, the path of survival and destruction, so it is imperative to examine it (Tzu, p.41)."***

To follow Master Sun Tzu, we would want to examine everything about your enemy that you can discover.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

## FOOT PRINTING/RECONNAISSANCE

A great deal of information can be gleaned from your opponent's website. One can find addresses, phone numbers, fax lines, and especially contact names (Accounting, Sales, Engineering, IT). Press releases on the company website or other financial sites can tip off operating systems, applications, and databases that the company utilizes. The source code of the website can also reveal hidden information that can give you additional tips on areas to exploit. Hence, it would be helpful to have a complete copy/mirror of your opponent's website. There are several good tools that could accomplish this, a couple of them are:

**Wget** http://www.gnu.org/software/wget/wget.html (UNIX)
**Teleport Pro** http://www.tenmax.com/teleport/pro/home.htm (Windows)

Another great reconnaissance tool is "Sam Spade." It is written by Steve Atkins, and you can download it free at:

**Sam Spade** http://www.samspade.org/ssw/download.html

This works for Windows 95 through Windows XP. It has many great network tools: crawl a website, *whois*, *traceroute*, *ping*, reverse DNS queries…

You will also want to use popular web search engines to look up more information on your opponent:

**AltaVista** http://www.altavista.com
**DogPile** http://www.dogpile.com/index.gsp
**Google** http://www.google.com
**Hotbot** http://www.hotbot.com
**Yahoo** http://www.yahoo.com

"USENET" searches can also produce all sorts of good information. Administrators sometimes describe problems with a specific operating system or network device, and then include their company information in their signature line.

**Google** http://groups.google.com

Another great resource for reconnaissance is *whois* databases. These are Internet-based utilities to query information about a system. They provide a "white pages" directory for an organization. You can find things like contact names for administrative, billing, and technical service. Phone numbers, fax numbers, company addresses, and e-mail addresses are usually displayed along with Domain Name Servers and IP addresses. All of this is filled out when a company/individual registers a domain name.

Now, you might ask, why don't people complete these registration records with phony information? In case a company or individual is attacked from your organization, you need to provide real information to be duly notified (Skoudis).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Currently, there are four Regional Internet Registries/Databases:

| | |
|---|---|
| **America (ARIN)** | http://www.arin.net/whois/index.html |
| **Asia Pacific (APNIC)** | http://www.apnic.org/search/index.html |
| **Europe (RIPE NCC)** | http://www.ripe.net/perl/whois |
| **Latin America & Caribbean (LACNIC)** | http://lacnic.net/cgi-bin/lacnic/whois |

Some other useful *whois* databases are:

http://www.allwhois.com (Good for over 70 countries)
http://www-whois.internic.net/cgi/whois
http://www.networksolutions.com/cgi-bin/whois/whois

*Whois* databases were originally developed for the military before others followed through with their own *whois* databases. For those interested in looking up U.S. Military and Government sites, please note that this should only be done from U.S. Government computers, if not, it could be construed as violating the "Computer Fraud and Abuse Act of 1986 (18 USC 1030)":

http://www4.law.cornell.edu/uscode/18/1030.html

The Department of Defense has the following "Consent to Monitoring" (http://whois.nic.mil/consent_no.cgi):

> This is a Department of Defense computer system. This computer system, which includes all related equipment, networks and network devices (specifically including access to the internet), are provided only for official u.s. government business.
>
> DoD computer systems may be monitored by authorized personnel to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures. Monitoring includes "hacker" attacks to test or verify the security of this system against use by unauthorized persons. During these activities, information stored on this system may be examined, copied and used for authorized purposes, and data or programs may be placed into this system. Therefore, information you place on this system is not private.
>
> Use of this DoD computer system, authorized or unauthorized, constitutes consent to official monitoring of this system. Unauthorized use of a DoD computer system may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be provided to appropriate personnel for administrative, criminal or other action.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

NOTE: Viewing this page is a consent to monitoring. They will also be recording your IP address and other information if you visit the following pages. I am including these sites for completeness of *whois* databases.

**U.S. Military** http://whois.nic.mil
**U.S. Government** http://www.nic.gov

If this has not scared you enough, here is another great quote from "The Neophyte's Guide to Hacking":

> Stay away from government computers. You will find out very fast that attempting to hack a MilTac installation is next to impossible, and will get you arrested before you can say "oh sh*t". Big Brother has infinite resources to draw on, and has all the time it needs to hunt you down. They will spend literally years tracking you down. As tempting as it may be, do not rush into it, you will regret it in the end (Deicide).

Okay, now that I have made you paranoid about government machines, let us move on to the next step. From the *whois* queries, we have hopefully obtained the IP Address for the DNS server. We need to see if DNS has not been configured securely by our opponent. Can we perform a DNS zone transfer? Some tools that can help you perform this are:

**Axfr** in **DIG** http://nscan.hypermart.net/?index=dns
**Sam Spade** http://www.samspade.org/ssw/download.html

Alternatively, if you do not want to download anything and want to try a "Click Kiddies" **nslookup** tool that retrieves DNS information for a range of IP addresses, click on http://www.bankes.com/nslookup.htm (Rhoades).

"Click Kiddies?" Who are "Click Kiddies" you might ask? Well, you are all familiar with "Script Kiddies" and "Packet Monkeys," if not head over to Denis Dion's paper "Script Kiddies and Packet monkeys – The New Generation of 'Hackers'" at http://www.sans.org/rr/hackers/monkeys.php. Some websites have their hacker tools online where no downloading is required, just a simple click of the mouse, hence the term "Click Kiddies" (Rhoades). There are numerous online hacker tools for "Click Kiddies." A search engine for online tools can be found at http://www.attackportal.net.

Now, we can look for access points to attack our opponent by mapping their network perimeter. The many flavors of UNIX include *traceroute*, while Windows includes *tracert*. Some *traceroute* tools to help accomplish this are:

**Multiple Tracert** http://www.tracert.com/cgi-bin/trace.pl
**Opus One** http://www.opus1.com/www/traceroute.html

In addition, if you prefer the visual traces:

**Sarangworld** http://www.sarangworld.com/TRACEROUTE
**VisualRoute** http://www.visualware.com/download/index.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Now we have some ideas about our opponent and the layout of their networks. What is next? We return to Sun Tzu for further guidance.

***"Test them to find out where they are sufficient and where they are lacking (Tzu, p.111)."***

As Master Sun points out, we need to find out where the areas of weakness are in our enemy, to do this we enter the next step of our hack: Scanning.

## SCANNING

First, we need to check if our opponent's systems are alive. We can achieve this by *pinging* their systems to see if they respond. Some good tools to perform this are:

| | |
|---|---|
| **Fping** | http://packetstormsecurity.nl/Exploit_Code_Archive/fping.tar.gz |
| **Friendly Pinger** | http://www.kilievich.com/fpinger/download.htm |
| **Hping** | http://www.hping.org/download.html |
| **Multiple Ping** | http://www.tracert.com/cgi-bin/ping.pl |
| **Nmap** | http://www.insecure.org/nmap |
| **Ping War** | http://www.simtel.net/pub/dl/17874.html |

Next, we would want to see what services our opponent is running. There are 65,535 TCP ports and 65,535 UDP ports in each system (http://www.iana.org/assignments/port-numbers). Imagine having 65,535 doors and 65,535 windows in your company. How could someone make sure that all of them are secure and locked down? Many companies are not complete in closing their ports. Hence, we need to find out what ports are open. To accomplish this we would want to scan their ports.

TCP Port Scanners:

| | |
|---|---|
| **Strobe** | http://www.deter.com/unix/software/strobe103.tgz |
| **SuperScan** | http://www.foundstone.com/resources/termsofuse.htm?file=superscan.exe&warn=true |
| **WinScan** | http://www.prosolve.com/software/winscan.php |

UDP Port Scanners:

| | |
|---|---|
| **WUPS** | http://www.ntsecurity.nu/toolbox/wups/ |

Both TCP/UDP:

| | |
|---|---|
| **ScanLine** | http://www.foundstone.com/resources/termsofuse.htm?file=scanline.zip&warn=true |
| **Netcat** | http://www.atstake.com/research/tools/nc11nt.zip (Windows) |
| **Netcat** | http://www.atstake.com/research/tools/nc110.tgz (UNIX) |
| **Nmap** | http://www.insecure.org/nmap |
| **SATAN** | http://ciac.llnl.gov/ciac/ToolsUnixNetSec.html#Satan |

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

A nice online port scanner that uses "nmap," and only works for IP addresses in the Class C range from which you are coming is available at:
http://www.linux-sec.net/Audit/nmap.test.gwif.html

In addition, if you want to examine TCP source ports, SYN, FIN, and Xmas scans, all from the Windows command line then try this tool (McClure):
**IpEye** http://www.ntsecurity.nu/toolbox/ipeye/

Now that you have some IP addresses, what type of operating system is your opponent running? Tools can determine the operating system (with a good deal of certainty) by seeing the response of the target to its probes; it works best if your opponent has at least one *listening* port. This is referred to as "stack fingerprinting."
**Nmap** http://www.insecure.org/nmap
**Queso** http://ftp.snt.utwente.nl/pub/os/linux/debian/pool/main/q/queso/
**Traceping** http://wizard.ae.krakow.pl/~mike/traceping.cgi
For web servers, try http://www.netcraft.com.

You can also identify operating system types via SNMP:
**Active SNMP** http://www.cscare.com/ActiveSNMP/features.asp
**MIB Browser** http://www.ibr.cs.tu-bs.de/cgi-bin/sbrowser.cgi?ACTION=GETHOST&OID=&HOST

A good network-mapping tool that combines *ping*, *traceroute*, port scanning, and uses "queso" for detecting the operating system is:
**Cheops** ftp://ftp.marko.net/pub/cheops/

A host scanner compilation for Linux that combines nmap, snmpscan, NetBIOS auditing, and a vh shell script is:
**THC-Probe** http://www.thc.org/download.php?t=r&d=probe-4.1.tar.gz

War Dialing:
To scan for modems that your opponent may be using, try these tools:
**PhoneSweep** http://www.sandstorm.net/products/phonesweep/
**PhoneTag** http://www.geocities.com/g2007l2/phonetag.zip
**THC-Scan** http://www.thc.org/download.php?t=r&d=thc-ts20.zip
**ToneLoc** http://chroot.ath.cx/fade/miscdl/tlppv03.zip

Where is the enemy weak? Master Sun Tzu had this to say:

> ***So when the front is prepared, the rear is lacking, and when the rear is prepared the front is lacking. Preparedness on the left means lack on the right, preparedness on the right means***

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

***lack on the left. Preparedness everywhere means lack everywhere (Tzu, p.108).***

## ENUMERATION

If none of the above has provided much information, you will want to attempt to identify valid user accounts or poorly protected resources shares. These are places where our opponent may be weak. Enumeration attacks are more invasive and as such will be easier to be spotted. Information we hope to discover are: network resources and shares, users and groups, and applications and banners (McClure).

Windows NT/2000 Enumeration:
Do not forget one of the best Windows NT Hacking Kits (Windows NT Resource Kit). It contains utilities, some Perl, ports assignments for common UNIX utilities, and remote administration tools. Some of these tools can be downloaded free at:
http://download.microsoft.com/download/winntsrv40/rktools/1.0/NT4/EN-US/sp4rk_i386.Exe
Windows 2000 Server CD includes some great utilities in the Support\Tools folder. Windows includes some built-in enumeration tools (McClure):

- **Net view** – to list domains available
- **Nbtstat** – NetBIOS name table
  - Scan entire networks using **nbtscan** at:
    http://www.inetcat.org/software/nbtscan.html
- **Nltest** – identifies Primary and Backup Domain Controllers

A good multi-purpose site that has some hacker tools that can help at this phase is the "Ad hoc IPTools Page" at:
http://tatumweb.com/iptools.htm

Where is the target (in the physical world)?
http://cgi-www.ckdhr.com:81/perl/loc2maps

Somarsoft has a tool that will help you enumerate Windows NT shares, even over a null session.
**DumpSec** http://www.somarsoft.com/

"Nbtdump" is a utility that can dump NetBIOS information from Windows NT/2000 and UNIX/Linux Samba servers such as shares, user accounts with comments, and the password policy.
**Nbtdump** http://www.atstake.com/research/tools/nbtdump.exe

"NetBIOS Auditing Tool (NAT)" finds network shares and attempts entry using user-defined username and password lists (McClure).
**NAT** http://packetstorm.linuxsecurity.com/NT/scanners/nat10bin.zip

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

"Epdump" queries the endpoint mapper on NT target machines. This gives you some idea what is running on which dynamically assigned ports.

**Epdump** http://online.securityfocus.com/data/tools/ms-epdump.zip.

"NetViewX" is a tool to list the servers in a domain or workgroup. It is a bit like the NT "net view /domain" command, but it allows you to list only servers with specific services.

**NetViewX** http://www.ibt.ku.dk/jesper/NetViewX/default.htm

Two command-line tools to help you enumerate are **user2sid** – to look up usernames to security identifiers; and **sid2user** – to look up security identifiers to usernames. These are both available at:

http://www.chem.msu.su:8080/~rudnyi/NT/sid.txt

Enumerating banners and application information can tell you a lot by how your opponent's computers respond. Just as in UNIX, ***telnet*** connections can respond giving you information as to the type of server, what version… For more information, try the "TCP/IP Swiss Army Knife":

**Netcat** http://www.atstake.com/research/tools/nc11nt.zip (Windows)
**Netcat** http://www.atstake.com/research/tools/nc110.tgz (UNIX)

You can dump the contents of your opponent's registry using another of Somarsoft's tools.

**DumpReg** http://www.somarsoft.com/

<u>NetWare Enumeration</u>:
Novell has a tool that can see the status of all of the servers on your opponent's network. You may also be able to browse the NDS trees all the way to the end leaf using this product.

**On-Site Admin** http://www.lss.ksu.edu/download/novell/onsiteb8.exe

Another useful tool from Novell, to view any NDS object and its corresponding attribute values, is:

**NDSsnoop** http://www.novell.com/coolsolutions/tools/1005.html

To list the serial numbers of all servers in the network, try out another of Novell's tools called **Snlist**, available at:

http://www.novell.com/coolsolutions/tools/downloads/snlist.exe

To find out which users belong to which groups:

**Bindery** http://ftp.cerias.purdue.edu/pub/tools/novell/bindery.zip

To look at objects like servers, users and groups, try the **Bindin** tool at:

http://files.chatnfiles.com/Netware%20Super%20Library/BINDERY/BINDIN/BINDIN.EXE

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

More tools to help you enumerate user information are:

**Userdump** http://www.hammerofgod.com/download/userdump.zip
**Userinfo** http://userinfo.swrus.com/

UNIX Enumeration:
To find out what directories are being shared on a UNIX machine, try the command ***showmount***. However, one of the best tools for enumerating users and hosts is the ***finger*** command. You will be able to see each user's home directory, login time, idle times, office location, and the last time they both received or read mail. If your opponent's machine does not have a finger server, your opponent's machine will display the message: "Connection not made."

**Finger** http://www.ipswitch.com/Products/WS_Ping/finger.html

Some other useful UNIX commands are (McClure):

- **rwho** – displays users currently logged on to the remote host
- **ruser -l** – displays similar information but includes how long since the user typed at the keyboard
- **telnet** [IP address] **25** – to attempt to get information via SMTP
- **tftp** – for grabbing the passwd file:

```
[root$] tftp 192.168.10.123
tftp>  connect 192.168.10.123
tftp>  get /etc/passwd /tmp/passwd.crack
tftp>  quit
```

Remote Procedure Call (RPC) is a protocol that allows applications to talk to one another over the network. To enumerate RPC applications try the command ***rpcinfo***, which is the equivalent of the *finger* command, but for RPC. The program "rpcdump" does the same job as running rpcinfo -p remote_host from a shell prompt.

**Rpcdump** http://www.atstake.com/research/tools/rpcdump.exe

Another good RPC scanning tool that we have mentioned earlier is "nmap."

**Nmap** http://www.insecure.org/nmap

***"Attack when they are unprepared, make your move when they do not expect it (Tzu, p.54)."***

## GAINING ACCESS

Now that we have learned what operating system our opponent is running, we need to find out what vulnerabilities that it has. These are places where our opponent may be unprepared. The following sites provide information on vulnerabilities:

**Bugtraq** http://www.securityfocus.com/
**CERT** http://www.cert.org/

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

**CIAC** http://www.ciac.org/ciac/
**NTBugtraq** http://www.ntbugtraq.com/

In addition, **Church of the Swimming Elephant** takes the above and puts it into a list of bulletins released daily at:

http://www.cotse.com/mailing-lists/todays/subject.html

**NIST** has a nice searchable index on vulnerabilities at:

http://icat.nist.gov/icat.cfm

The **SANS/FBI Top 20 List** of vulnerabilities can be found at:

http://www.sans.org/top20/

For example, you may want to research the latest CGI/ASP bugs at any of the above websites and then use your favorite search engine to locate web sites that use CGI/ASP. For an interesting article on an example of this see the "The Google attack engine" from The Register back in the Fall of 2001 (Greene):

- "(Someone has been) abusing Google to attack Web servers, switches and routers in a novel way, by crafting search terms to include known exploits. Such a search will occasionally yield active Web pages used by administrators."
- "[Ryan Russell – SecurityFocus researcher] was using Google to check how common a particular string is on the Web, to gauge how often a [Snort] rule might cause a false-positive. Part of the process of deciding how often the rule might cause a false positive. So while searching Google for a vulnerability in Cisco IOS Web Server, Russell followed a link and found himself in a switch belonging to a US .gov site."

For those computers running Windows XP that have not downloaded the large Service Pack 1 (SP1) yet, there is a vulnerability that will allow someone to delete arbitrary files using Help and Support Center. It takes advantage of the file C:\WINDOWS\PCHEALTH\HELPCTR\System\DFS\uplddrvinfo.htm. To test your machine to see if you are susceptible to this attack, create a junk folder, filled with useless files on your c:\ drive. Then paste the following into your browser "hcp://system/DFS/uplddrvinfo.htm?file://c:\junk*" and you will see the Windows "Help and Support Center" open. In addition, if you do not have SP1 installed the files in that directory have just been deleted. Even using other browsers like Mozilla does not help. Deleting or renaming this file (uplddrvinfo.htm) can remove this vulnerability for those who do not have the time or bandwidth to download SP1. This vulnerability was fixed in SP1, but here is a website with more information about the vulnerability:

http://cert.uni-stuttgart.de/archive/bugtraq/2002/08/msg00224.html

For vulnerabilities in Windows Internet Explorer (IE), head over to Pivx Solutions' site at http://www.pivx.com/larholm/unpatched/, as of April 10, 2003 there are 13 unpatched vulnerabilities in Internet Explorer.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Here are some recent articles that show how hackers are still exploiting vulnerabilities everyday:

- "U.S. Army Web Server Attacked"
  http://www.eweek.com/article2/0,3959,938096,00.asp
- "Worms Wreak Havoc on the Net in '03"
  http://www.eweek.com/article2/0,3959,997877,00.asp
- "Databases Ripe for Attacks"
  http://www.eweek.com/article2/0,3959,1007007,00.asp

Vulnerability Scanners:
Many vulnerability-scanning tools go thru their databases of known vulnerabilities and look for potential holes. One of the best is "Nessus." A good introduction to Nessus is Tony Enriquez's article "Pocket Nessus," which is located at http://www.sans.org/rr/tools/pocket_nessus.php.

**Nessus** http://www.nessus.org/download.html

A URL scanner that can search for known vulnerable CGI's on websites is "Whisker." It scans the CGI's directly and crawls the website determining which CGI's are already in use.

**Whisker** http://www.wiretrip.net/rfp/p/doc.asp?id=21&iface=2

"Nikto" is a web scanner that can perform comprehensive tests against web servers, including looking for dangerous files/CGI's, versions on over 130 servers, and problems on over 200 servers.

**Nikto** http://www.cirt.net/code/nikto.shtml

Scan computers for patch management using:

**HFNetChk** http://www.shavlik.com/

The Hacker's Choice (THC) has the "Happy Browser," which checks Windows NT servers and webservers for known vulnerabilities.

**Happy Browser** http://www.thc.org/download.php?t=r&d=thc-hb09.zip

"SAINT" is a vulnerability scanner because it pinpoints security risks accurately and comprehensively. This tool is useful in detecting network vulnerabilities.

**SAINT** http://www.saintcorporation.com/products/saint_engine.html

Passwords:
Many systems administrators do not change the default passwords on software or network devices. Many lists on the Internet publish these lists:

http://www.phenoelit.de/dpl/dpl.html
http://www.cirt.net/cgi-bin/passwd.pl
http://www.governmentsecurity.org/articles/DefaultLoginsandPasswordsforNetworkedDevices.php
http://www.astalavista.com/library/auditing/password/lists/defaultpasswords.shtml

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The "Astalavista Group" also includes a list of "Default Password Paths" at:
http://www.astalavista.com/library/auditing/password/lists/passwordpath.shtml

For "wireless" network device passwords go to:

http://www.cirt.net/cgi-bin/ssids.pl
http://mediawhore.wi2600.org/nf0/wireless/ssid_defaults/

Now, you want to know how you can crack passwords. First, let us look at the world of Windows NT. The password hashes for accounts in Windows NT are stored in the SAM (Security Account Manager) database. The location of the SAM database is %systemroot%\system32\config\SAM, where %systemroot% is the Windows directory that Windows was installed into (usually \winnt). When NT is installed, the SAM database is copied into the %systemroot%\Repair directory. The LAN Manager hashing that NT uses breaks the password down into two 7-character words that do not have case sensitivity. Now, if a person used a 10 character password, LAN Manager breaks it down into a 7-character password and a 3-character password. This makes it much easier to "crack" the password (Cole). One great Windows Password Cracker over the years has been "L0phtCrack."

**L0phtCrack v3.0** http://www.securityfocus.com/data/tools/lc3setup.exe
**LC4** http://www.atstake.com/research/lc/download.html

A command-line program that cracks hashes is "NgHashCrack." It cracks SHA-1 and MD5 hashes using brute force incrementally or by using a word list.

**NgHashCrack** http://www.ngsec.com/downloads/misc/ngHashCrack-1.0.zip

You can access web-based accounts, anything that needs a username and password (or more), via the brute force method using Munga Bunga's "HTTP Brute Forcer."

**HTTP Brute Forcer** http://ns13.eb1.biz/~clickont/mungabunga.exe

We will cover UNIX passwords in our next section, "Escalating Privilege," since typically you will need to have "root" status to see the /etc/shadow file, where the passwords are stored in an encrypted state.

A HTTP authentication hacker tool, which tries combinations of user ID's and passwords is:

**YaHa** http://www.cirt.net/code/yaha.shtml

The Hacker's Choice (THC) has a number of good tools. One tool is a powerful script language that hacks terminal logins via dictionary- or brute force hacking called:

**THC login/telnet** http://www.pimmel.com/products/thc/thc-lh11.zip

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

"NetBIOS Auditing Tool (NAT)," that we discussed earlier, connects to your opponent's system and then attempts to guess passwords from a predefined array and user-supplied lists (McClure).

**NAT** http://packetstorm.linuxsecurity.com/NT/scanners/nat10bin.zip

Some utilities to crack Cisco passwords are:

http://www.alcrypto.co.uk/cisco/
http://gd.tuwien.ac.at/pc/winsite/win95/netutil/ciscopwd.zip

Applications are even susceptible, especially databases. You can search for applications and find websites like "Oracle Default Users, Passwords and Hashes" at http://www.pentest-limited.com/default-user.htm.

Buffer Overflow:

"Buffer overflows" allow the execution of arbitrary commands to take over your opponents system or escalate your privileges. "Nessus," discussed above, looks for numerous overflow vulnerabilities. A powerful paper was written about buffer overflows called "Smashing the Stack for Fun and Profit" (Aleph One). Buffer overflows are created by writing past the end of an array corrupting the execution stack. Code that does this is said to smash the stack, and causes the routing to jump to a random address upon return. Smashing the stack allows you to run programs such as a shell or a specific DLL (Skoudis).

Sniffing Data:

To collect data transmitted across a network, use a *sniffer*. *Sniffers* eavesdrop on the network. Use "TCP Dump" to monitor the network activities and acquire data. You can dump the traffic on the network and print out certain packet headers.

**TCP Dump** http://www.tcpdump.org/

A command line *sniffer* for Windows 2000/XP that does not require a packet driver is:

**NgSniff** http://www.ngsec.com/downloads/misc/ngSniff-1.1.zip

A free network protocol analyzer that works for both Windows and UNIX is "Ethereal." You can examine live data (packets) or download it to disk. There is also the ability to reconstruct a TCP session stream.

**Ethereal** http://www.ethereal.com/download.html

Some other good *sniffers* and network analyzers are:

**Sniffit** http://newdata.box.sk/neworder/a/sniffit.0.3.2.tar.gz
**Snort** http://www.snort.org/dl/
**Iris Network Traffic Analyzer 3.7**
http://download.com.com/3000-2092-8740584.html?tag=lst-0-1

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Sniffing in switched networks is more challenging. An attacker needs to inject packets into the network to redirect traffic, which is known as "ARP Cache Poisoning" (Skoudis). For switched networks, try the Linux multipurpose *sniffer*/interceptor/logger, "Ettercap." It supports both active and passive dissection of protocols, including ciphered ones.

**Ettercap** http://ettercap.sourceforge.net

To grab community names, SNMP requests and sets, try:

**SNMPsniff** http://www.cotse.com/sw/sniffers/snmpsniff-1_0.tgz

We can also go back to our "Swiss Army knife" of hacker tools, "Netcat." With "Netcat," we can use it to transfer files, scan ports, create *backdoors* and create relays (Skoudis).

**Netcat** http://www.atstake.com/research/tools/nc11nt.zip (Windows)
**Netcat** http://www.atstake.com/research/tools/nc110.tgz (UNIX)

Alternatively, try **Cryptcat** (Enhanced Netcat with Twofish encryption):

http://farm9.com/content/Free_Tools/cryptcat_nt.zip (Windows)
http://farm9.com/content/Free_Tools/cryptcat_linux2.tar (Linux)

In addition, there is even more information out there on the Internet. Just typing the words "Hacker" + "Source Code" into Google's search engine found over 132,000 sites with hacker information on them, and "Hacker" + "Tool" identifies over 436,000 sites.

***"In ancient times skillful warriors first made themselves invincible, and then watched for vulnerability in their opponents (Tzu, p.84)."***

## ESCALATING PRIVILEGE

As skillful warriors, we have now gained access to our opponent's domain, and need to make ourselves invincible. We can achieve this by escalating our privileges to that of an Administrator, Supervisor, or root account.

Windows:

Developed by Konstantin Sobolev in Russia, "GetAdmin" exploits a hole that gives an account membership in the *Local Administrators* group. No special permissions are needed to run this program, which can also be run through a *telnet* session.

**GetAdmin** http://cmp.phys.msu.su/ntclub/pub/code.htm

Microsoft released a patch to fix this vulnerability, but if you run "crash4.exe" on the server first, and then run "GetAdmin" the exploit should still work.

**crash4.exe** http://www.users.globalnet.co.uk/~mnemonix/crash4.exe

Keystroke recorders allow you to capture data your opponent types on his keyboard, even NT's "trusted path" – Alt+Ctrl+Delete logon.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

**Invisible Keystroke Logger** http://www.amecisco.com/iksnt.htm
**KLogger** http://www.ntsecurity.nu/toolbox/klogger/

If you have the "Restore files and directories" user right, you change the ownership of files by using the tool:

**SetOwner** http://www.ntsecurity.nu/toolbox/setowner/

Bryce Cogswell and Mark Russinovich wrote "NTFSDOS." This program allows access to NTFS partitions from operating systems that use FAT. Put this program on a system disk, and then boot the NT machine off it. You will now have full read access to the NTFS partitions. Now you can grab the SAM in the %systemroot%\system32\config directory.

**NTFSDOS** http://www.sysinternals.com/ntw2k/freeware/NTFSDOS.shtml

To manipulate and view file and directory access control lists, registry security, disk shares and network printers use "NTSEC." Using a command line interface, you will be able to export, change and view directory information. You could then change permissions, auditing settings, as well as users, groups, rights and policies on your opponent's machines.

**NTSEC** http://www.pedestalsoftware.com/products/ntsec/

Windows hides data in a space called *Windows Protected Storage*. Hidden information is in there that includes form auto-fill data offered by Internet Explorer every time you enter something into a form on a web page; passwords to websites; MS Outlook account and identity passwords, and dial-up passwords. To explore this space use:

**SecretExplorer** http://www.webdon.com/wse/default.asp

Another program that will let you explore protected storage, view .pwl files, and recover lost login passwords is:

**PwlTools** http://www.webdon.com/vitas/pwltool.asp

To reveal the shadowed (*****) Windows passwords use:

**Revelation** http://www.snadboy.com

Using the program, "Sechole," grant a non-admin user debug-level access on a system service. From this point, local Admin rights can be gained.

**Sechole** http://www.users.globalnet.co.uk/~mnemonix/sechole2.zip

Use "Pwdump2" to dump the password hashes in the SAM database. You can then input this data into L0phtCrack.

**Pwdump2** http://razor.bindview.com/tools/desc/pwdump2_readme.html

Create *Trojans* using the tool "eLiTeWrap." Extract files automatically into a temporary directory, and manipulate them by using the user's system or other

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

programs in the package. You can also start programs automatically, and hide these from the user.

**eLiTeWrap** http://packetstormsecurity.nl/trojans/elitewrap.zip

NetWare:

In NetWare, we can take account information from the NDS or Bindery files using "Imp." It includes various attack methods to compromise account passwords.

**Imp** http://www.wastelands.gen.nz/imp/imp211.zip

A nice suite of tools for hacking NetWare is "Pandora." There are both an "online" version for direct attacks against live servers, and an "offline" version for password cracking of the NDS.

**Pandora** http://www.nmrc.org/project/pandora/download.html

Copy the NDS files using:

**Jcmd** http://www.jrbsoftware.com

UNIX:

In UNIX, passwords used to be kept in the */etc/passwd* file. The password was encrypted as 13 characters. This file is world readable, which means everyone can read it. To solve this problem, later versions of UNIX moved the encrypted password to the */etc/shadow* file. Someone who is "root" can only read this file.

There are many UNIX password crackers one of which has been referred to as "Crack, the breakfast of addicts." Alex Muffett wrote "Crack," which has a configurable language that will allow the user to program in the types of guesses that will be attempted.

**Crack** ftp://ftp.cerias.purdue.edu/pub/tools/unix/pwdutils/crack/

Using a command-line tool, you can crack UNIX and NT LanMan passwords using a dictionary-only cracker:

**John the Ripper** http://www.openwall.com/john/

If you have a very large UNIX *passwd* file, you can filter out the important accounts using:

**THC-GetVIP** http://www.thc.org/download.php?t=r&d=thc-gv15.zip

Exploit well-known weaknesses in the TCP/IP protocol suite by using "HUNT." This tool allows you to spy on connections and look for information like passwords.

**Hunt** http://lin.fsid.cvut.cz/~kra/index.html#HUNT

There are a number of sites with exploits and tools on them for different Operating Systems, Routers/Switches, Services, Networks, and *Trojans*, one of which is the **Digital Information Society**:

http://www.phreak.org/html/exploits.shtml

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

***"So in the case of those who are skilled in attack, their opponents do not know where to defend (Tzu, p.104)."***

## CREATING BACKDOORS/MAINTAINING ACCESS

We have breached the defenses of our opponents, escalated our privileges to that of administrator status, and now we seek to maintain our access. This is where we use *backdoors* to guarantee future access. *Backdoors* are a way back into a system bypassing any existing security and perhaps defeating any additional security enhancements that are added onto a system later. We will discuss a number of *backdoor* programs that range in complexity, but there are also "legitimate" *backdoors* that could be placed. We could simply install a service such as *IIS* with known remote holes. "Hackers are using vastly more sophisticated techniques to secretly control the machines they've cracked, and experts say it's just the beginning (Poulsen)."

Windows:
To hide processes, files, directories and registry keys/values, use "Windows NT RootKit." This even includes execution redirection to hide *Trojans* from a user. If your opponent opens, hashes, CRC's, or even scans the file – they will see the original file, but if they execute the file, they get the *Trojan*. You can even *telnet* into "RootKit" from remote.

**RootKit v0.40** http://packetstormsecurity.nl/NT/_root_040.zip

A partial list of how you can use "SubSeven" on your opponents is:

- Monitor ALL of your opponent's online activity
- Watch them if they have a Web Cam
- Listen to them if they have a microphone
- Copy any of their files
- Delete ANY of their files
- Put ANY file on their computers
- Record their passwords
- Edit their Registry
- Redirect incoming connections
- Browse their network
- Update itself with a newer version
- Plus much, much more

**Sub7 2.2 Beta** http://www.hackemate.com.ar/sub7/files/Sub7%20v2.2.zip

**Sub7 2.15 Legends** http://www.hackemate.com.ar/sub7/files/Sub7%20v2.1.5%20Legends.zip

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

"NetBus" is the older version of "Back Orifice (BO)." It is still good since it works on both Windows NT and Windows 9x. This has many of the same functions as "Sub7," you can even schedule commands to run at predefined times.

**NetBus** http://home.t-online.de/home/husky_college/nbpro201.exe

We can use our old favorite "Netcat" again, or use a similar version that is a little stealthier. It is a small 3k *backdoor* coded in assembler, which lives up to its name:

**Tini** http://ntsecurity.nu/toolbox/tini/

A more complex program is "Back Orifice 2000." It has numerous features, some of which are:

- Keystroke logging
- HTTP file system browsing and transfer
- Manage the Microsoft Network file sharing
- Edit your opponents Registry
- Browse, transfer, and manage their files
- Redirect TCP/IP connections
- Access console programs, such as command shells through *Telnet*
- Grab NT registry passwords
- Process control, start, stop, list
- Remote reboot
- And much more

**Back Orifice 2000 (BO2K)** http://www.bo2k.com/software/index.html

"VNC" stands for Virtual Network Computing. Using this program, you can remotely hijack the NT GUI. It is a remote display system, which allows you to view a computer's desktop environment from anywhere on the Internet and from a wide variety of machine architectures.

**Virtual Network Computing (VNC)** http://www.uk.research.att.com/vnc

<u>NetWare</u>:

Why not leave a way back into your opponent's system with supervisor equivalency? You can using "Super," which lets you toggle on and off the supervisor equivalency.

**Super.exe** http://www.netwarefiles.com/utils/super.zip

There is a *backdoor* in NDS, which is completely hidden from everyone and everything. You need Administrator access to set it up. Here are the steps to do it (McClure, pp.308-309):

1) Log into the tree as Admin or equivalent.
2) Start the NetWare Administrator (nwadmn3x.exe).
3) Create a new container in a deep context within the tree. Right-click an existing OU, and create a new OU by selecting Create and choosing an Organizational Unit (OU).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

4) Create a user within this container. Right-click the new container, select Create, and choose User.
5) Give the user full Trustee Rights to his or her own object. Right-click the new user, and select Trustees Of This Object. Now make that user an explicit trustee.
6) Give this user full Trustee Rights to the new container. Right-click the new container, and select Trustee Of This Object. Make the user an explicit trustee of the new container by checking all of the available properties.
7) Modify the user to make his or her security equivalent to Admin. Right-click the user, select Details, select the Security Equivalent To tab, select add, and select Admin.
8) Modify the Inherited Rights Filter on the container to disallow Browse and Supervisor capabilities.
9) Now log in through the *backdoor*.

<u>UNIX</u>:
First, you want to *backdoor* service binaries to access your opponent's system later, like ***ps*** and ***netstat*** to hide any connections you may make. Examples of critical binaries that you would *backdoor* on Solaris 2.x machines are:

- /usr/bin/log
- /usr/sbin/in.rlogind
- /usr/sbin/in.rshd
- /usr/sbin/in.telnet.d
- /usr/sbin/ping

"Linux RootKit 5" contains backdoored versions of *chfn*, *chsh*, *crontab*, *du*, *find*, *ifconfig*, *inetd*, killall, *linsniffer*, *login*, *ls*, *netstat*, *passwd*, *pidof*, *ps*, *rshd*, *syslogd*, *tcpd*, *top*, *sshd*, and *su*. It also comes with *bindshell*, *fix*, *linsniffer*, *thesniff*, *sniffchk*, *wted*, and *z2*. **Lrk5** can be downloaded at:
http://packetstormsecurity.nl/UNIX/penetration/rootkits/lrk5.src.tar.gz

A set of nice hacking tools that includes *backdoors*, tunnels and cleaners written by THC members is:
**THC-UnixHackingTools** http://www.thc.org/download.php?t=r&d=thc-uht1.tgz

A great list of ***RootKits*** for UNIX can be found at:
http://packetstormsecurity.nl/UNIX/penetration/rootkits/

In addition, a list of ***Trojans*** for UNIX is at:
http://www.phreak.org/archives/exploits/unix/trojans/

One of the early commentators of Master Sun Tzu's work had this to say about vulnerability in your opponents:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

***Keeping your own military in order, always being prepared for opposition, erase your tracks and hide your form, making yourself inscrutable to opponents. When you see that an opponent can be taken advantage of, then you emerge to attack (Tzu, p.85).***

## COVERING TRACKS

As Master Sun Tzu has said, we need to cover our tracks now that we are in our opponent's systems. We need to disguise ourselves, making ourselves undetectable to our opponents. Some of this was already discussed in the last section when we discussed *RootKits*. We now need to erase or edit log files, hide files and directories, and create covert channels on the network.

Why should you care about auditing and logging? These files create a permanent or semi-permanent record of events on a system. Your intrusion activities might be recorded leading a nice trail back to yourself, or closing any potential holes that you have been exploiting. Just remember that if your opponent is sending the logging to a line printer, this is one of the most difficult items to deal with. For a great example of this read Cliff Stoll's "The Cuckoo's Egg," where a line printer led to the recording of a hacker's exploits in numerous computers (Stoll).

How much logging is being done varies greatly from opponent to opponent. This is dependant also, on how meticulous the opponent's administrator is, since log files pile onto their current workloads. We want to edit these log files to make them appear as normal as possible, or at the very least erase our presence.

Windows:
The common log files for Windows NT are found in the %systemroot%\system32\config directory. The .log files are the buffer files that keep the most recent events; these are periodically written to the .evt files which event viewer uses. The files used for logging are (Cole):

- system.log - basic events
- security.log - security events
- application.log - events involving the running of certain applications
- SysEvent.Evt
- SecEvent.Evt
- AppEvent.Evt

The Security and System Events are the two log files that you should be the most concerned with viewing to see if you have left a trace. You can wipe these logs or add data to them to camouflage your visit.

You can use tools to clear the system, application and security event logs:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

**ClearEventLog** http://duke.net/eventlog
**ClearLogs** http://www.ntsecurity.nu/toolbox/clearlogs/

Selectively erase event records from the Security log, instead of erasing everything, using:

**WinZapper** http://www.ntsecurity.nu/toolbox/winzapper/

Note: The public version of this utility is limited. When you modify the event log, the event viewer will stop working until the machine is rebooted. A file called "dummy.dat" is left behind that contains the original copy of the event log. There are modified versions of "WinZapper" without these limitations.

If all else fails in deleting log files and you have left evidence behind, there is one more option you can do, the radical destruction of data. A nasty program will destroy all data on any given DOS or Windows 3.x/9x/NT/2000 machine called "Hard Drive Killer Pro." Do not open this file on your own system since it would destroy all of your data! This file is a *Trojan*, and will be recognized by most anti-virus vendors' programs, such as McAfee, Norton, and Trend Micro as a malicious program and will not let you download it unless you turn off your protection.

**Hard Drive Killer Pro** http://www.hackology.com/programs/hdkp/ginfo.shtml

You also need to turn off auditing in Windows. While being Administrator, go the Audit policy and turn off the things you wish to turn off. For individual files and directories, you will have to edit these by right-clicking on them, selecting properties and then choosing the Security tab. Click on the Auditing button, and turn off what you want to turn off. Alternatively, you can use the **auditpol** tool in "Windows NT Resource Kit" to turn off auditing.

You can hide files using the *attrib +h* command, but there is a better solution. NTFS supports file streaming; you can use this to hide files. Using alternate data streams, you can store data under an original file. Streams are not displayed in Windows Explorer, or in a *dir* listing from a command prompt. You will need the POSIX utility ***cp*** from the "Windows NT Resource Kit" (Skoudis).

<u>NetWare</u>:
The common log files for NetWare are:

- Accounting - SYS:SYSTEM\NET$ACCT.DAT
- Auditing - SYS:_NETWARE*.CAF
- Console Monitor Log - SYS:SYSTEM\CONSOLE.LOG
- File Server Error Log - SYS:SYSTEM\SYS$ERR.LOG
- Transaction Tracking Error Log - SYS: TTS$LOG.ERR
- Volume Error Log - root of each volume is VOL$LOG.ERR

To turn off auditing, follow these steps (McClure, p.307):

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

1) Start up SYS:PUBLIC\auditcon.
2) Select Audit Directory Services.
3) Select the container you wish to work in and press F10.
4) Select Auditing Configuration.
5) Select disable Container Auditing.
6) You will now be able to add containers and users to the selected container without an administrator knowing.

After you have changed the above log files, you will want to change the file history. Follow these steps (McClure, p.307):

1) Start **filer** from SYS:PUBLIC.
2) Select Manage Files And Directories.
3) Find the directory where the file resides.
4) Select the file.
5) Select View/Set File Information.
6) Change Last Accessed Date and Last Modified Date.

UNIX:

Log files for UNIX vary from flavor to flavor. However, here are some general guidelines:

- System log files and accounting files, can be found in **/var/adm**, **/var/log** or **/usr/adm**
- Common log files including **messages**, **syslog** and even **sulog**.
- Check **/etc/defaults** and **/etc/syslog.conf**.
- **wtmp**, **utmp**, and **lastlog** will contain information relating to logins.

The main logging files on a Linux system are (Cole, p.283):

- **/var/run/utmp** - tracks who is logged into the system.
- **/var/log/wtmp** - tracks who has logged in and out of the system.
- **/var/log/btmp** - tracks failed logon attempts.
- **/var/log/messges** - keeps messages reported from the syslog facility.
- **/var/log/secure** - tracks access and authentication information.

Other processes might be logging this information to separate log files. Here are some potential files to look for:

- /**var/log/maillog** - logs inbound and outbound mail activity
- **/var/spool/cron/log**- cron log file
- **/var/spool/lp/log** - log file for printing

Editing these files should be easy since most of them are text files. Nevertheless, for some you may need a special tool to selectively remove entries from the list like:

**Remove** http://www.dsinet.org/tools/logutils/remove.c

Other tools to help you erase your tracks are:

**Wipe** http://www.phreak.org/archives/exploits/unix/log-tools/wipe-1.00.tgz

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

**Zap** http://www.phreak.org/archives/exploits/unix/log-tools/zap.c
http://www.phreak.org/archives/exploits/unix/log-tools/zap2.c

Search for unencrypted log files and modify them using:

**THC-ManipulateData** http://www.thc.org/download.php?t=r&d=manipulate_data-1.0.tar.gz

Overwriting files will not hide them; they can be recovered. Delete files securely by wiping out the inodes of the deleted files using:

**THC-SecureDelete** http://www.thc.org/download.php?t=r&d=secure_delete-2.3.tar.gz

For a nice list of utilities to securely wipe data, head to:

http://packetstormsecurity.nl/UNIX/secure_delete/

You can hide files in UNIX by creating a file or directory named ". " (dot-space) or ".. " (dot-dot-space). Most people will miss these files since the single dot represents the current directory and the double dot represents the parent directory when you list a directory. The added spaces will camouflage it in a normal listing of a directory, and will usually go unnoticed (Skoudis).

Protocol Tunneling:

We can hide data traversing a network by disguising it to look like normal web traffic. On UNIX system with a Perl interpreter, install **Reverse WWW Shell**, which can be downloaded at:

http://www.megasecurity.org/Sources/rwwwshell-1_6_perl.txt

Alternatively, try the **THC-RWWWShell** available at:

http://www.thc.org/download.php?t=r&d=rwwwshell-2.0.pl.gz

Covert Channels:

Instead of using one protocol to carry another (tunneling), hide data in the openings of a protocol. One can hide data in TCP and IP headers (Skoudis). You can do this using Craig Rowland's Linux program:

**Covert_TCP** http://www.firstmonday.dk/issues/issue2_5/rowland/

## CONCLUSION

Warning – Use at your own risk:

As for the tools and techniques that you have now been given, I would like to use the standard disclaimer to use moderation with this new knowledge, and always get permission in writing before scanning a system or network, or cracking passwords. Most businesses, including ones that you may work at (even as a security professional), may frown on scanning of their systems without permission. Some of these tools (written by unknown or questionable sources)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

may even have *Trojan horses* inside them, download them and try them on a "test" machine first. When in doubt, do not use it.

Note regarding URL's:
Locations of tools change on a regular basis. If a tool has moved, there are a number of things you can do to look for it. Sometimes the webmasters of the site has just moved the location of their tools when they revamp their site, going back to the home page of the URL and start from there. Otherwise, check Google (http://www.google.com) and search for the file's name. For instance, search for a tool like **wipe-1.00.tgz**, and if you get too many hits add the word **download** and perhaps **hacker** in there to limit the number of sites.

I hope that you now have some ideas of the methods and techniques that hackers use on systems everyday. Security professionals need to understand these concepts to better defend against hackers, and identify when they are on your systems. One cannot simply ignore computer security, because as Kevin Poulsen recently pointed out in "SecurityFocus," things will get worse before they get better (Poulsen). Security is changing on a daily basis, if security professionals stay on the cutting edge of hacker tools and methods of entry, they will be able to defeat hackers before they even get started on your systems, or as Master Sun Tzu said it:

> ***So it is said that if you know others and know yourself, you will not be imperiled in a hundred battles; if you do not know others but know yourself, you win one and lose one; if you do not know others and do not know yourself, you will be imperiled in every single battle (Tzu, p.82).***

I hope that with this information you can now win the battles against the intruders on your systems.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

**BIBLIOGRAPHY**

Aleph One. "Smashing the Stack for Fun and Profit." 9 Nov 1996. URL: http://www.phrack.org/show.php?p=60&a=6 (20 April 2003).

Current maintainers of the list are Rootkid, Nicolas Gregoire and Nexus. "Default Password List." 20 April 2003. URL: http://www.phenoelit.de/dpl/dpl.html (20 April 2003).

Cole, Eric. Hackers Beware. Reading: New Riders Publishing, 2002.

Deicide. "The Neophyte's Guide to Hacking." 23 October 1993. URL: http://hackez.narod.ru/hacking/hack_guide.htm (20 April 2003).

Dion, Denis. "Script Kiddies and Packet monkeys – The New Generation of 'Hackers'." 29 January 2001. URL: http://www.sans.org/rr/hackers/monkeys.php (20 April 2003).

Enriquez, Tony. "Pocket Nessus." 23 January 2002. URL: http://www.sans.org/rr/tools/pocket_nessus.php (20 April 2003).

Finnigan, Pete. "Oracle Default Users, Passwords and Hashes." 2001. URL: http://www.pentest-limited.com/default-user.htm (20 April 2003).

Fisher, Dennis, eWEEK. "U.S. Army Web Server Attacked." 18 March 2003. URL: http://www.eweek.com/article2/0,3959,938096,00.asp (20 April 2003).

Fischer, Dennis, eWEEK. "Worms Wreak Havoc on the Net in '03." 3 April 2003. URL: http://www.eweek.com/article2/0,3959,997877,00.asp (20 April 2003).

Greene, Thomas C. "The Google attack engine." 28 November 2001. URL: http://www.theregister.co.uk/content/6/23069.html (20 April 2003).

McClure, Stuart, Scambray, Joel, and Kurtz, George. Hacking Exposed: Network Security Secrets and Solutions, Third Edition. Reading: Osborne/McGraw-Hill, 2001.

Mitnick, Kevin D. The Art of Deception. Reading: Wiley Publishing, Inc., 2002.

Poulsen, Kevin, SecurityFocus. "Windows Root Kits a Stealthy Threat." 5 March 2003. URL: http://www.securityfocus.com/news/2879 (20 April 2003).

Rhoades, David. "Attack Portals: Point & Click Hacking (with Online Tools)." 26 February 2003. URL: http://www.mavensecurity.com/AttackPortals.zip (20 April 2003).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Skoudis, Ed. The Hack-Counter Hack Training Course Workbook. Reading: Prentice Hall PTR, 2002.

Stoll, Cliff. The Cuckoo's Egg. Reading: Pocket Books, 1990.

Tzu, Sun (translated by Cleary, Thomas). The Art of War. Reading: Shambhala Publications, Inc., 1988.

Vaas, Lisa, eWEEK. "Databases Ripe for Attacks." 7 April 2003. URL: http://www.eweek.com/article2/0,3959,1007007,00.asp (20 April 2003).

Warner, Bernhard. "Iraq War Sparks Tit-For-Tat Hacker Attacks." 28 Mar 2003. URL:http://www.reuters.com/newsArticle.jhtml;?type=topNews&storyID=2467068 (20 April 2003).

© SANS Institute 2003, Author retains full rights.

Last Updated: October 21st, 2014

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| **SANS Cyber Defense San Diego 2014** | **San Diego, CAUS** | **Nov 03, 2014 - Nov 08, 2014** | **Live Event** |
| **SANS DFIRCON East 2014** | **Fort Lauderdale, FLUS** | **Nov 03, 2014 - Nov 08, 2014** | **Live Event** |
| **SANS Sydney 2014** | **Sydney, AU** | **Nov 10, 2014 - Nov 22, 2014** | **Live Event** |
| **SANS Korea 2014** | **Seoul, KR** | **Nov 10, 2014 - Nov 15, 2014** | **Live Event** |
| **SANS Tokyo Autumn 2014** | **Tokyo, JP** | **Nov 10, 2014 - Nov 15, 2014** | **Live Event** |
| **Pen Test Hackfest** | **Washington, DCUS** | **Nov 13, 2014 - Nov 20, 2014** | **Live Event** |
| **SANS London 2014** | **London, GB** | **Nov 15, 2014 - Nov 24, 2014** | **Live Event** |
| **SANS Hyderabad 2014** | **Hyderabad, IN** | **Nov 24, 2014 - Nov 29, 2014** | **Live Event** |
| **Healthcare Cyber Security Summit** | **San Francisco, CAUS** | **Dec 03, 2014 - Dec 10, 2014** | **Live Event** |
| **SANS Cyber Defense Initiative 2014** | **Washington, DCUS** | **Dec 10, 2014 - Dec 19, 2014** | **Live Event** |
| **SANS Oman 2015** | **Muscat, OM** | **Jan 03, 2015 - Jan 08, 2015** | **Live Event** |
| **SANS Security East 2015** | **New Orleans, LAUS** | **Jan 16, 2015 - Jan 21, 2015** | **Live Event** |
| **SANS Gulf Region 2014** | **OnlineAE** | **Nov 01, 2014 - Nov 13, 2014** | **Live Event** |
| **SANS OnDemand** | **Books & MP3s OnlyUS** | **Anytime** | **Self Paced** |