

# STEAL THIS COMPUTER BOOK 4.0

What They Won't Tell You About the Internet

**WALLACE WANG**



**NO STARCH  
PRESS**

San Francisco

# 8

## STALKING A COMPUTER

Like car thieves, hackers usually target the first computer they find with weak defenses. If a computer is too hard to break into, hackers will usually go off in search of easier prey. The reason is simple. Unless hackers have a specific reason for breaking into a particular computer, they can accomplish their goals on any undefended machine and don't need to waste time trying to break into one that's well-protected.

On the other hand, if a hacker really wants to break into your computer because it contains files the hacker wants or because your computer provides the least well-guarded path into a more heavily protected computer network, you can't do anything to stop that hacker from trying. The only safe computer is one that's never turned on.

The streets are safe in Philadelphia. It's only the people who make them unsafe.

—FRANK RIZZO, ex-police chief and mayor of Philadelphia

### WHY HACKERS CHOOSE THEIR TARGETS

Sometimes hackers break into computers for fun, just to see if they can do it, or to practice their skills. Hackers often target corporate computers to gain access to their large storage space, which can be perfect for stashing pirated programs or movies. By storing large collections of illegal material on someone else's computer, hackers shift liability from themselves to an unsuspecting stranger.

Sometimes hackers target corporate computers for the information contained in them. In his book *Friendly Spies*, Peter Schweizer claims that Germany financed hackers in an effort called Project Rahab, which mapped out the structure and flaws of computer networks belonging to the governments of France, Japan, England, and the United States. Likewise, China has been accused of using hackers to probe for weaknesses in the computer networks of other countries, and it's likely that the United States and Russia have also developed this capability.

Even if your computer doesn't belong to a top-secret government network or a major corporation, hackers might still target your computer for fun, but increasingly, they're doing it for profit. Few hackers care to see which web pages someone visits, but many would be very interested in seeing the credit card numbers someone types into a particular web page. To snare this type of information, hackers will often install

remote-access Trojan horses (see Chapter 5 for more information about RATs) that can capture keystrokes or screen images and send them to the hacker later.

Hackers also break into computers owned by individuals in order to install programs called “bots,” which let them control that computer remotely. Unlike RATs, which allow a hacker to gain complete control over an infected computer, bots are much smaller programs that accept and perform a more limited range of commands. By linking bot-infected computers together, a hacker can create an army of “zombies” or “drones.” With a single command, they can be instructed to send a flood of data to another computer that will shut it down (a denial of service attack), or send out massive amounts of junk email (spam). (Individual computers connected to high-speed Internet connections, such as DSL or cable modems, are especially prized because they’re always available and can blast out information like spam at high speeds.)

There will always be some hacker with a reason to break into any particular system, including yours, whether you’re in charge of a corporate computer installation or just your own personal computer.

## FINDING A TARGET

When an army needs to find a target, they send out scouts who attempt to infiltrate enemy territory and report back on what they’ve found. Likewise, when hackers want to break into a computer, they need to scout out possible targets to determine which ones to attack. If hackers don’t have a specific computer they want to attack, they’ll often scout for targets of opportunity using war dialing, port scanning, and war driving.

### War dialing

Before the growth of the Internet, war dialing was the best way to find a computer to attack. Even with today’s heavy reliance on the Internet, many companies still use telephone modems to allow salespeople to remotely connect to and control an office computer using programs such as pcAnywhere or LapLink. If a computer happens to be connected to both a network and an outside telephone line, hackers can often sneak in through the telephone line, bypassing defenses deployed on the network. (If a computer is only accessible to the outside through a phone line, war dialing might be the only way to get in at all.) Phone lines typically don’t have firewalls or intrusion detection systems.

Many companies get a false sense of security from knowing that a modem’s phone number is not listed publicly. But just because a hacker doesn’t know the specific phone number to a computer doesn’t mean he can’t find it. That’s what war dialing is all about.

Most company phone numbers all use the same prefix. For example, internal phone lines for a company with the 239 prefix could all have numbers like 239-1029 or 239-8953. A hacker could spend all night dialing different telephone numbers until he reaches one with a modem on the other end, or simply let a computer do this tedious work by running a war dialer (see Chapter 2).

A war dialer can automatically dial a range of phone numbers, such as those from 239-1000 to 239-9999. For each number it tries, it listens for the telltale squeak of an answering modem and, if it hears it, records the telephone number. A hacker can let a war dialer run overnight and wake up the next morning with a list of phone numbers, both listed and unlisted, that are each connected to a modem.

He can then dial each telephone number individually. Before a computer will allow access through a telephone line, it usually asks for a password. All the hacker needs to do is guess the correct password and the computer will throw open its doors to let the hacker inside.

One of the simplest defenses against war dialing is a callback device. The moment someone (a valid user or an intruder) calls the computer, the callback device hangs up and dials a pre-arranged telephone number that only a valid user would answer. Of course, a really determined hacker could somehow find out the phone number used by the callback device and then use call forwarding on that number to reroute the call to the hacker's phone number.

## Port scanning

Port scanning works much like war dialing, but instead of dialing multiple phone numbers to find a way into a computer, scanners probe a range of Internet Protocol (IP) addresses, as shown in Figure 8-1.

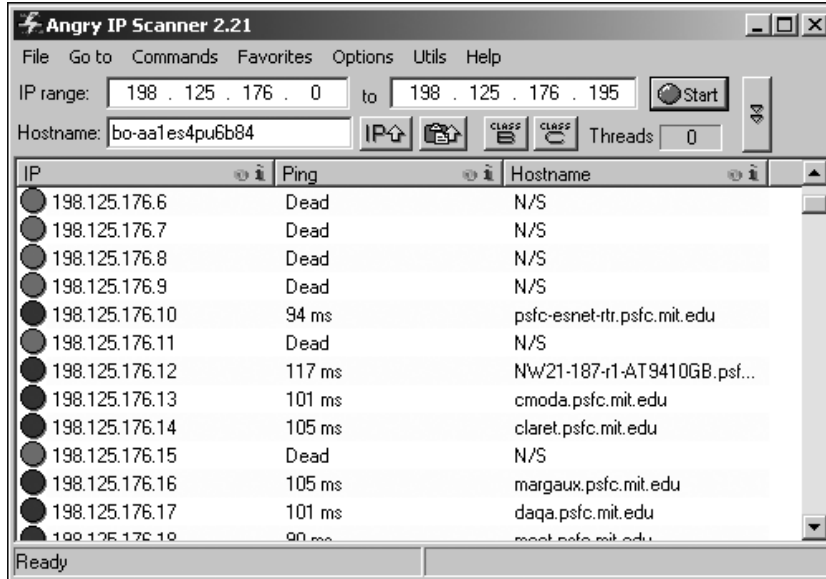


Figure 8-1: A port scanner can scan a range of IP addresses to find a computer to attack.

Every computer connected to the Internet uses ports, opening up countless doors that hackers can use to access a computer. Table 8-1 lists the more common ports, but keep in mind that a computer may have several hundred ports open at any given time.

Computers can communicate over the Internet using two protocols, TCP and UDP. Normally when one computer wants to communicate with another through a port using the TCP protocol, the first computer sends a synchronize (SYN) message to the second computer, which essentially tells it, "I'm ready to connect to your port." The type of communication the first computer wants to initiate determines which port number the computer uses, such as port 110 to send email or port 80 to send a web page. When the



target computer receives this message, it sends back a synchronize/acknowledgment (SYN/ACK) message, which says, "Okay, I'm ready too." Now the first computer can send data to this particular open port of the second computer.

**Table 8-1: Common types of ports available on servers accessible over the Internet**

SERVICE	PORT
File Transfer Protocol (FTP)	21
Telnet	23
Simple Mail Transfer Protocol (SMTP)	25
Gopher	70
Finger	79
Hypertext Transfer Protocol (HTTP)	80
Post Office Protocol, version 3 (POP3)	110

The TCP protocol is often used when reliability is more important than speed, since constantly acknowledging the other computer can slow down communication. That's why sending email or transferring files is usually done using TCP.

The UDP protocol is most often used for streaming video or Internet telephony where speed is more crucial. The UDP protocol saves time because it doesn't go through the "handshaking" process that the TCP protocol requires, but like TCP, UDP can still be exploited.

In legitimate interactions, receiving TCP synchronization messages on a port is no cause for alarm, but receiving them unexpectedly and abundantly can be a telltale sign of an attempt to probe a computer's defenses, like a burglar loudly jiggling the handle of every door on a building, trying to see which ones are locked.

So to mask their probing attempts, port scanners use a variety of evasive techniques. While none of these techniques will work all the time, the combination of these tactics can help identify different ways to get into a computer, such as the following:

**TCP connect scanning** Connects to a port by sending a synchronize (SYN) packet, waits for a return acknowledgment packet (SYN/ACK), and then sends another acknowledgment packet to connect (ACK). This type of scanning is what normally happens when two computers communicate through a port. This is easily recognized and often logged by target computers to alert system administrators of a possible hacker attack.

**TCP SYN scanning** Connects to a port by sending a SYN packet and waits for a return acknowledgment packet (SYN/ACK), which indicates that the port is listening, but never sends an acknowledging ACK packet back to the target computer. Known as half-scanning, this technique is less likely to be logged and detected than ordinary TCP connect scanning, although now many security programs specifically look for this type of scanning simply because it's more likely to be used by hackers hiding their probing attempts.

**TCP FIN scanning** Connects to a port by sending a “No more data from sender” (FIN) packet to a port. A closed port responds with a Reset (RST) message, while an open port simply ignores the FIN packet, thereby revealing its existence as an open port.

**Fragmentation scanning** Breaks up the initial SYN packet into smaller pieces to mask its existence from any packet filter or firewall protecting the target computer. Used in conjunction with other scanning techniques such as TCP connect, TCP SYN, or TCP FIN scanning.

**FTP bounce attack** Requests a file from an FTP server on the target system using the IP address and port number of another computer, thus masking the source of the attack (the hacker’s computer). A successful file transfer indicates an open port on the target computer without revealing the hacker’s IP address.

**UDP (User Datagram Protocol) scanning** Uses UDP instead of TCP. When a closed UDP port receives a probe, its send an ICMP\_PORT\_UNREACH error message. Ports that don’t send back an ICMP\_PORT\_UNREACH error message are open.

Once port scanning has determined that a computer on a specific IP address has ports open to attack, the next step is to determine what type of operating system and server software the target computer is using. To make this determination, hackers send data to different ports and analyze the way the computer responds, as shown in the port scanner screenshot in Figure 8-2.



Figure 8-2: The N-Stealth port scanner has identified that this particular target computer is running Microsoft IIS, version 6.0.

Port scanners use a variety of platform-probing techniques, including the following:

**FIN probing** Sends a FIN (“No more data from sender”) packet to a port and waits for a response. Windows responds to FIN packets with Reset (RST) messages, so if a RST message comes back, the computer is likely running Windows.

**FIN/SYN probing** Sends a FIN/SYN packet to a port and waits for a response. Linux systems respond with a FIN/SYN/ACK packet.

**TCP initial window checking** Checks the window size on packets returned from the target computer. The window size from the AIX operating system is 0x3F25 and the window size from OpenBSD or FreeBSD is 0x402E.

**ICMP message quoting** Sends data to a closed port and waits to receive an error message. All computers should send back the initial IP header of the data with an additional eight bytes tacked on. Solaris and Linux systems, however, return more than eight bytes.

Once a hacker knows the IP address of a target computer, the open ports available on that target computer, and the type of operating system used by the target computer, the hacker can plan his strategy for breaking in, much like a burglar might case a house before trying to break into it in order to determine the best route.

If you want to see how a port scanner works, you can try Angry IP Scanner ([www.angryziber.com/ipscan](http://www.angryziber.com/ipscan)); Nessus ([www.nessus.org](http://www.nessus.org)); iNetTools ([www.wildpackets.com](http://www.wildpackets.com)); N-Stealth ([www.nstalker.com/eng/products/nstealth](http://www.nstalker.com/eng/products/nstealth)); Nmap ([www.insecure.org/nmap](http://www.insecure.org/nmap)); SAINT ([www.saintcorporation.com](http://www.saintcorporation.com)); or SARA (<http://www-arc.com/sara>).

Nmap is considered the premier port scanning tool, which offers a variety of scanning and evasion techniques. Since most networks now use firewalls and intrusion detection systems (IDS) to detect port scanners, Nmap breaks its data packets into smaller fragments, which can fool a firewall or IDS from recognizing that a port scan is even taking place.

Nmap also lets you spoof where data is coming from. If a firewall or IDS detects a flood of data coming from one computer, it might rightly conclude a hacker is probing its defenses. But by using Nmap, a hacker can still probe a computer, but each probe appears to come from a different computer (when it’s really coming from a single computer). No matter how good a firewall or IDS may be, it can never be 100 percent reliable, and port scanners like Nmap constantly evolve to take advantage of the latest tricks.

## War driving

Rather than physically connecting computers with cables to form a network, many companies and individuals are turning to wireless networks instead. The idea is simple. You plug in a device known as a router or access point, which relays signals to and from any computer with a wireless network interface card (NIC). Those computers can then access the resulting wireless network as if they were physically connected to one another through cables.

Any computer with a wireless card within range of the wireless access point can access a wireless network. Unfortunately, it also means that a wireless card plugged into a hacker’s laptop across the street could access that same network too. When you set

up a wireless network, it's like having a normal wired network with cables sticking out of every window in the building, which anyone can plug into their computer and use to access your network, at any time, without you necessarily knowing about it.

With so many corporations and individuals going wireless these days, hackers can locate wireless networks simply by driving around a neighborhood with a laptop computer, a wireless network interface card, and a scanning program. Sometimes hackers also include a global positioning system (GPS) for mapping out the exact location of the wireless networks they find. The process of driving around and scanning for wireless networks is called *war driving*. (There is also war strolling, war flying, and war boating, but the main idea in each case is the same: cruise a neighborhood and search for wireless networks.)

Once you have a laptop or handheld computer with wireless capability, you can just saunter over near an unguarded wireless "hotspot" (an area where wireless access is available) and use it to connect directly to the Internet.

While coffeehouses and public libraries offer free wireless Internet access as an attractive service to their customers, many individuals and businesses unwittingly offer free wireless Internet access as well. When people set up a wireless network, they usually just plug their wireless router into their Internet connection (such as a cable or DSL modem) and right away, they have wireless access. Unfortunately, these people don't realize that the range of Internet access often extends beyond the physical boundaries of their home or office and spills out into the streets and sidewalks. Anyone can access the Internet through these unintentional wireless hotspots.

As mentioned, to find a wireless (WiFi) hotspot, you can drag your laptop or handheld computer around with you, or you can just use a handy WiFi locator device, such as the ones made by WiFi Seeker ([www.wifiseeker.com](http://www.wifiseeker.com)) or by Intego ([www.intego.com/wifiLocator](http://www.intego.com/wifiLocator)), shown in Figure 8-3.



Figure 8-3: A WiFi locator device lets you scan for WiFi hotspots without a computer.

In a surprising number of cases, people will set up a wireless network with no thought to security, which means you can access that WiFi network just by turning on your wireless-enabled computer. To prevent this, some people will turn on WiFi encryption, known as Wired Equivalent Privacy (WEP).

WEP encryption scrambles any data sent across a WiFi network, which essentially blocks strangers from accessing a WiFi network. The original WEP encryption standard only used 40-bit encryption keys, but newer, more secure WEP encryption uses 128-bit



keys. The longer the keys used to encrypt data, the harder the encryption is to crack. It's a bit like trying to guess a number between 1 and 10 versus guessing a number between 1 and 999,999,999.

To defeat WEP encryption, hackers use special sniffer programs that snare data from the WiFi network for cryptanalysis. The more data the sniffer program grabs, the better its chances of figuring out how the WiFi network is encrypting its data. Given enough time, most sniffer programs will eventually be able to crack WEP encryption, letting the hacker on to the network.

Newer wireless networks now use WiFi Protected Access (WPA), which is a stronger encryption standard. However, even this isn't invulnerable to attack, since hackers have developed a program dubbed coWPAtty, which snares enough data from the wireless network and then uses a dictionary attack (see Chapter 9 for more information about cracking passwords using a dictionary attack) to find the password needed to access the wireless network.

Hackers have developed sniffer programs for all types of computers and operating systems including Windows, Linux, Macintosh, and even Palm and PocketPC handheld computers. To find a sniffer program, visit WarDriving.com ([www.wardriving.com](http://www.wardriving.com)). For a specialized operating system designed just to sniff out WiFi networks, download and run a unique Linux distribution dubbed WarLinux (<http://sourceforge.net/projects/warlinux>).

To defeat sniffers, some corporate networks rely on client-side certificates, which verify that a particular computer is allowed access to a network. If a computer tries to access a network without the proper client-side certificate, the network cuts it off. Client-side certificates make accessing a wireless network harder, but if a hacker hijacks a computer that is allowed to access the network, the hacker can access the network through a "trusted" computer, which proves that there really is no such thing as a "trusted" computer.

### ***The steps to accessing a WiFi network***

The first step to accessing a WiFi network is to find a WiFi signal, either by using a WiFi locator device or by letting your WiFi-equipped computer scan the airwaves. Since two WiFi networks may overlap each other, each one identifies itself with a *service set identifier (SSID)*, which is a unique, descriptive name for a network. A computer must know the WiFi network's SSID to connect to it.

There are two ways hackers can retrieve this information. First, they can use a sniffer program to snare data packets out of the air and examine them to piece together the SSID. Second, they can anticipate that the network administrator will have left the WiFi network's default manufacturer settings in place including the default SSID, which is often just the name of the company that makes the WiFi router, such as *LinkSys* or *NetGear*. So when prowling the airwaves, hackers will first try all the various default passwords used by different WiFi manufacturers.

Some WiFi networks may require a user name and a password for access. As with SSID settings, however, nearly all WiFi equipment comes with a default user name and password, and few people bother to change this. So hackers first try feeding a WiFi network a known default password and user name for that particular WiFi manufacturer. If this doesn't work, the hacker can use the sniffer program to study data packets used by the WiFi network and steal a legitimate user's user name and password. In their quest to thwart intruders, some WiFi networks will only grant access to network interfaces

with specific (MAC) addresses, which uniquely identify computers on a WiFi network. However, to find a valid MAC address, hackers can do the same basic thing that they do to steal user names and passwords.

If you have a WiFi network, consider it vulnerable to attack. Someone can always attempt to access it from next door, down the street, or from a car parked outside your window. (Quick! Take a look now!)

### Finding a WiFi network

If you want to find a WiFi network that openly accepts users (for free or for a fee), visit a WiFi hotspot search engine such as HotSpot Haven ([www.hotspothaven.com](http://www.hotspothaven.com)) or WiFiMaps.com ([www.wifimaps.com](http://www.wifimaps.com)). By planning ahead, you can always be near a WiFi hotspot, whether you're in Pittsburgh or Pasadena.

However, if you want to find a WiFi network that *isn't* open to the public, you can visit the Wireless Geographic Logging Engine ([www.wigle.net](http://www.wigle.net)), which lists known WiFi hotspots in different parts of the world, as shown in Figure 8-4.

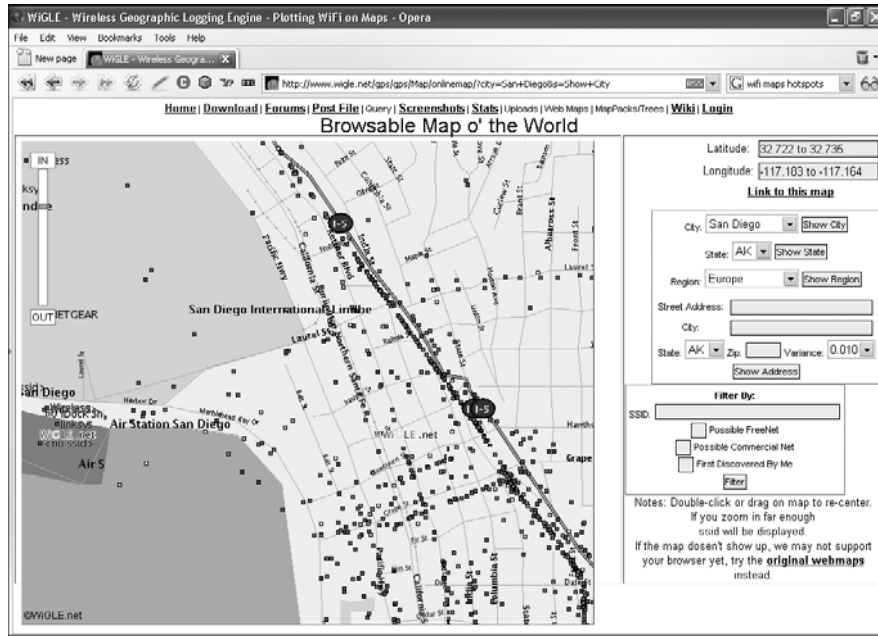


Figure 8-4: A WiFi map can show you possible hotspots near your hometown.

To make finding a WiFi network even easier, hackers have adopted the techniques of late 19th- and early 20th-century hobos who used to carve or draw marks on trees and buildings to warn other hobos of unfriendly towns, sympathetic households, or good places to hop on a passing train. Likewise, war chalking today (visit [www.warchalking.org](http://www.warchalking.org)) involves drawing marks around a neighborhood to identify the location and features of a particular wireless network, as shown in Figure 8-5.






let's warchalk..!	
KEY	SYMBOL
OPEN NODE	ssid  bandwidth
CLOSED NODE	ssid 
WEP NODE	ssid    access contact  bandwidth
blackbeltjones.com/warchalking	

Figure 8-5: War-chalking symbols to identify the location and status of a wireless network.

Once that first hacker discovers a WiFi network and leaves behind a war-chalking mark, other hackers will likely explore that wireless network. Although many companies make wireless equipment, many wireless hacking tools like Kismet ([www.kismetwireless.net](http://www.kismetwireless.net)), contain a database of default wireless configurations for each manufacturer. Since most people never change these default settings, a hacker using Kismet (or a similar wireless hacking tool) can often access a wireless network right away.

With so many unwanted intruders poking around a network, it's only a matter of time before one of them accidentally or purposely disrupts, deletes, or alters some important files.

### ***Protecting a WiFi network***

It's easy to protect a WiFi network from intruders: Just turn it off. Of course, it's not practical to turn it off when you're using it, so here are some simple tips to help protect your WiFi network from an unwanted intruder.

First, try lowering the signal strength from your wireless network's access point. By lowering the signal, you can limit its range from extending beyond the area in which you need it. Next, change all the default settings of your WiFi equipment, such as its SSID identifier and user name and password. Next, turn on MAC address filtering so that your WiFi network only allows computers with network interfaces with specific MAC addresses to access the network. Finally, turn on WEP encryption. While WEP encryption can't protect your network from a determined hacker, it can discourage the opportunistic hacker looking for an easy WiFi network to access. New WiFi equipment supports an improved encryption standard known as WiFi Protected Access (WPA). Given a choice, use WPA instead of WEP encryption.

For those who like to take a proactive stance in defending against hackers, try running a program called Fake AP, created by Black Alchemy ([www.blackalchemy.to](http://www.blackalchemy.to)). The Fake AP program floods the airwaves with phony SSIDs. Now if a hacker tries to find your WiFi network, he'll have to wade through this flood of bogus SSIDs, which decreases the chances that he'll actually find, let alone break into, your WiFi network.

## Probing sites by Google hacking

The key to breaking into any computer is to learn what type of software it runs. While it's possible to obtain this information by connecting directly to a target computer and running one of many hacker programs that probe a computer's security perimeter, this is much like a prowler peeking through the windows of a house that he plans to burglarize. It may work, but it risks alerting the target that it's being cased, and also leaves a trail that could potentially lead back to the intruder.

So rather than take this risk, hackers simply let Google find this information for them. Not only does this keep the hacker's identity hidden, but it also prevents the target from knowing it's being probed.

### Finding specific webserver software using Google

Hackers often specialize in breaking into specific webserver programs, and they can use Google to help them find more vulnerable computers to attack. To search for websites that run specific webserver programs, just type in the name of the server software you want to find, such as *Microsoft IIS 5.0* or *Red Hat Server 3.0*, using the following query format:

```
intitle:index.of "Software name"
```

<b>intitle</b>	Searches for web pages that contain a particular word or phrase in their titles
<b>index.of</b>	Specifies the directory listing of a website, which often has the title "Index of" near the top of the page
<b>"Software name"</b>	Specifies a particular webserver program name, such as <i>Microsoft IIS 6.0</i> or <i>Apache 2.2</i>

This type of Google query examines a website's directory listing to reveal both the way the website organizes its files and the name and version of the webserver software running it, as shown in Figure 8-6.

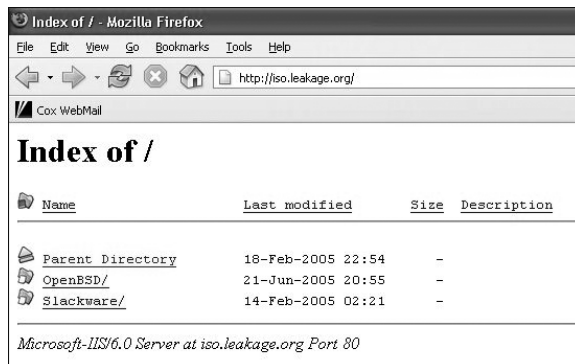


Figure 8-6: A website's directory listing exposes both the directories where crucial files are stored along with the name and version number of the webserver software.



### Searching specific websites

Another powerful Google search tool is the site operator, which narrows your search to a specific website domain. It has the following format:

site:"Domain name" "Search term"

- site Searches for web pages stored on sites in a specific domain
- "Domain name" Specifies the domain, such as .edu or army.mil
- "Search term" Specifies a search word or phrase

While this query can be useful to find specific types of information on specific types of websites, such as looking for information about "terrorism" on all ".gov" website domains, the real power of the site operator appears when it is combined with the intitle operator. This combination can search websites in specific domains running specific webserver programs.

So if you know how to break into an Apache webserver and you want to know which US Army websites might be running it, you could use the following query, which would display a listing as shown in Figure 8-7:

site:army.mil intitle:index.of apache

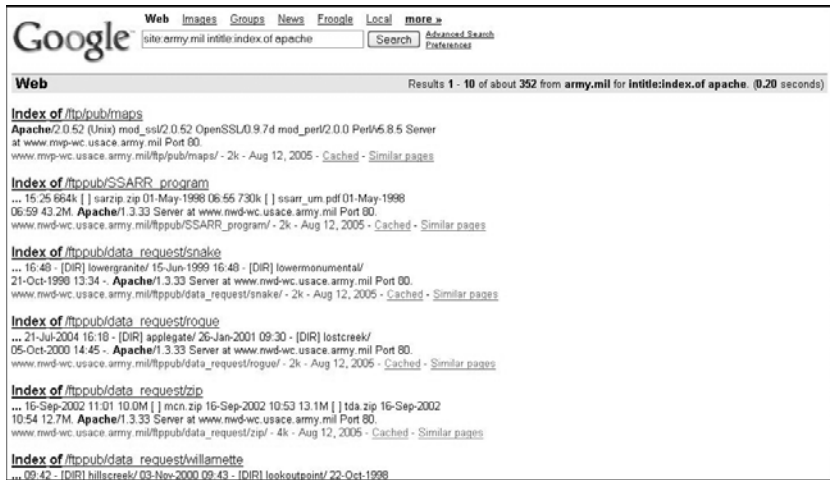


Figure 8-7: By using the intitle and site keywords, you can find a list of websites that run a particular webserver program.

Once you know which of your targeted websites run specific versions of a webserver program (such as Apache 1.3), you can use Google once more to search for *Apache vulnerabilities* or a similar string to view information about known flaws in that particular webserver program.

**NOTE:** Rather than use Google to search for software flaws, you can also browse through computer security sites such as [Packetstormsecurity.org](http://Packetstormsecurity.org) and [CERT.org](http://CERT.org) that list the latest software vulnerabilities found in webservers.

Security bulletins are meant to alert system administrators to flaws that they should patch immediately. However, many system administrators either never see these bulletins or don't implement them right away. As a result, hackers can also use security bulletins to find vulnerable websites (and many do).

For example, suppose you find a security bulletin that identifies a flaw in Apache and recommends that users upgrade to Apache version 1.3.27. Armed with this information, you just have to search for any website running an earlier version of Apache, and you'll know that it is likely to be vulnerable to the specific flaw described in the security bulletin. In many cases, security bulletins can be just as helpful to hackers as they are to system administrators.

### ***Probing a website's defenses***

Many system administrators run security scanners to probe for holes on their sites. This typically generates a report of its findings for the system administrators to study. Not surprisingly, many system administrators never delete these security scanner reports, and you can use a Google query using the `intitle` operator to look for them once you know the heading the security scanner always stores on its reports.

For example, one popular security scanner is Nessus ([www.nessus.org](http://www.nessus.org)), whose reports you can search for using the following query format:

```
intitle:"Scanner header"
```

To look for Nessus security scanner reports, the scanner header search string is "Nessus Scan Report":

```
intitle:"Nessus Scan Report" "This file was generated by Nessus"
```

This will help you find security scanner reports on other websites, as shown in Figure 8-8.

Even if the vulnerabilities reported by a security scanner report have been closed, a security scanner report can help hackers understand the defenses of a target computer better. Since security scanners can't detect every possible vulnerability, they can give lazy system administrators a false sense of security. If a knowledgeable hacker knows of a security flaw that a scanner doesn't detect, the system administrator may not have detected that flaw either, and there's a good chance that the hacker can exploit the flaw.

Besides security scanners, many system administrators rely on intrusion detection tools, such as the popular open-source Snort ([www.snort.org](http://www.snort.org)). To create reports, Snort users often run a program called SnortSnarf. Once again, if system administrators don't delete the SnortSnarf files from their systems, hackers can find them by simply searching with Google for "SnortSnarf alert page." Not only can this alert hackers that a particular website is running the Snort intrusion-detection system, but the retrieved SnortSnarf reports will also show the types of attacks that other hackers have tried (and that have, presumably, failed), as shown in Figure 8-9.

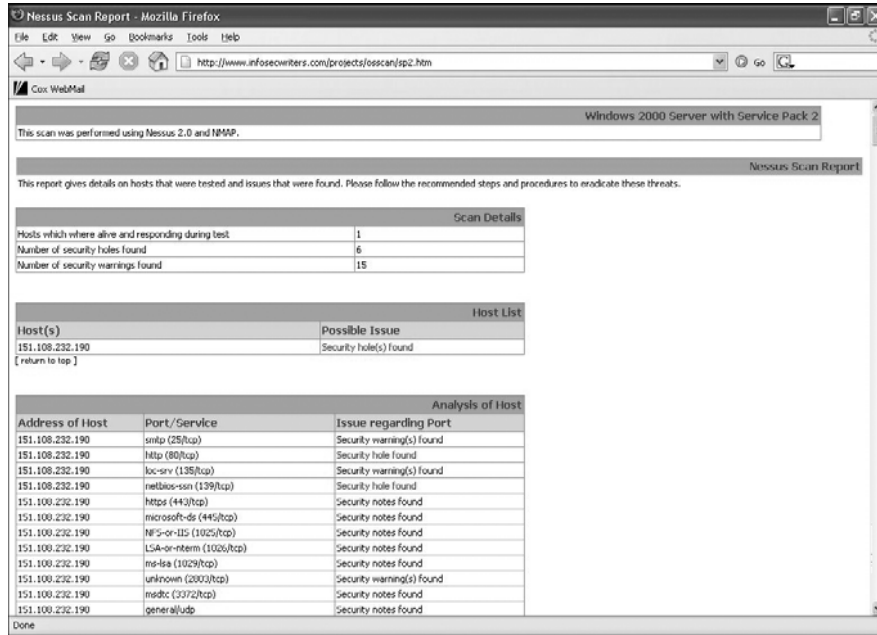


Figure 8-8: By searching for security scanner reports, you can learn what holes might still be open on a system.

Combine the “SnortSnarf alert page” query with the site operator, and you can find out which websites are running the Snort intrusion-detection program using a query such as this one:

```
site:edu snortsnarf alert page
```

The above query tells Google to search for all educational websites (.edu) that have used the SnortSnarf program to create a report.

### Finding and copying files using Google

Rather than break into a website (and risk getting caught), hackers can often retrieve the site files they want through Google. Many system administrators store user names, addresses, telephone numbers, and even Social Security numbers in a Microsoft Access database file, often called admin.mdb. To search for these types of files, you just need to use the allinurl operator. The format of this query is as follows:

```
allinurl:"Filename"
```

- allinurl** Searches for web pages that contain "Filename" in the web page locator string
- "Filename"** Specifies the file to find

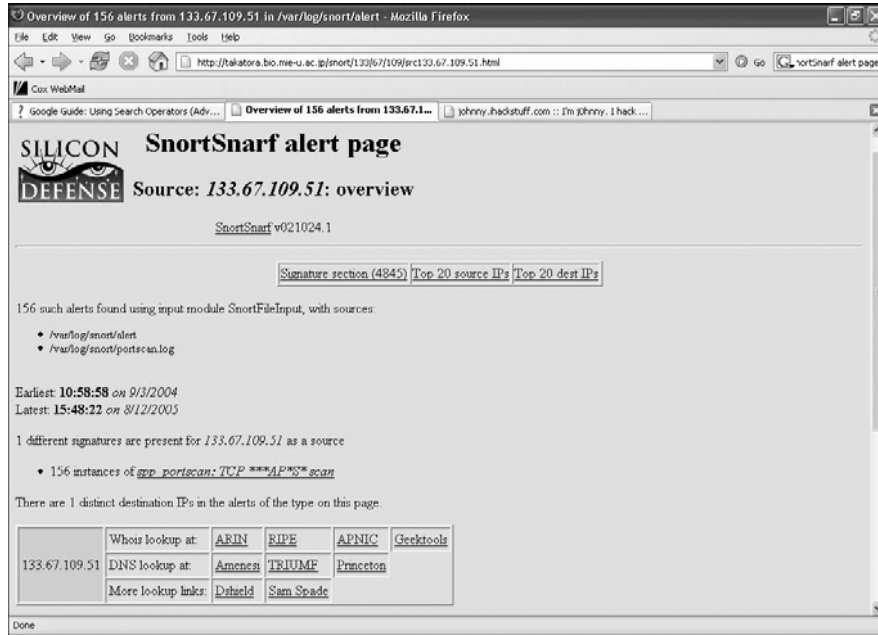


Figure 8-9: Viewing the report files of a website scanner can tell you in advance what types of attacks it is already protected against.

So to find the admin.mdb file, which often contains sensitive information, you would just use this query:

`allinurl:admin.mdb`

After finding this file using Google, you can download it through Google and view it, as shown in Figure 8-10, all in the privacy of your own computer.

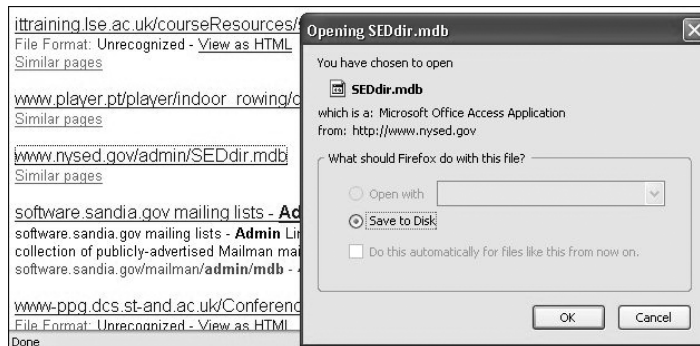


Figure 8-10: After finding a file with a Google query, you can download it from the website.





Another Google search operator that comes in handy for finding specific types of files is the filetype operator. Its format is as follows:

filetype:"*File extension*" "*Search term*"

<b>filetype</b>	Searches for files having the extension identified by " <i>File extension</i> "
<b>"<i>File extension</i>"</b>	Specifies the type of file to search for, such as PDF (Adobe Acrobat files) or DOC (Microsoft Word files)
<b>"<i>Search term</i>"</b>	Specifies a word or phrase to find in these files

So if you wanted to find Microsoft Word documents that contain the phrase *for internal use only*, you could use this query:

filetype:doc "for internal use only"

Combine the filetype operator with the site operator and you can search for all Microsoft Word documents that contain *for internal use only* in military websites, as shown below:

site:mil filetype:doc "for internal use only"

The filetype operator isn't likely to uncover any files containing top-secret documents or evidence of conspiracy, but it can be one more way to probe the inner workings of a website. In addition, the filetype operator demonstrates just how invasive Google is in indexing information that most website administrators don't even know have thereby been exposed to the world.

### ***Guarding against Google hackers***

To defend against Google hackers, keep any sensitive files off your webserver. Just because a file can't be accessed through your web pages doesn't mean that a hacker can't find that file anyway. Even if a sensitive file is only on your website temporarily, you are not safe.

Then try Google hacking your own webserver and see what you find. You may be surprised at how much information Google may already know about your server and how vulnerable your computer might really be.

Search engines like Google constantly troll different websites and store the files they find in a storage area called the cache. Once your website's files have been stored in Google's (or some other search engine's) cache, anyone can view them by using the cache operator. For example, if you want to view pages that were previously displayed by a website, you can use the cache operator followed by the website address, as shown below:

cache:cnn.com

This Google query will show you the web pages currently stored on Google for the CNN.com website. These pages will remain in Google's cache until the next time Google refreshes its cache by visiting the CNN.com website, even if CNN.com has removed or altered the pages in the meantime.

Google, like most search engines that regularly "crawl" the Internet to find websites to index, follows certain rules when visiting websites. One of those rules is that website administrators can create a special robots.txt file that specifies which parts of the website the search engine should not explore and store in its cache. So if there are sensitive files that on your computer that you don't want others to see, you can create a robots.txt file to tell Google not to index them. (Of course, it's much safer not to put sensitive files on your webserver computer in the first place.) To learn more about how the robots.txt file works, visit [www.robotstxt.org](http://www.robotstxt.org). Just be aware that hackers can also peek at your robots.txt file to see what type of information you want to protect, and then they'll know exactly what type of information to look for in your computer.

Another alternative is to request that search engines (for example, Google) ignore your website altogether. However, while this can prevent hackers from scanning your site using the search engine, it can also keep legitimate users from finding it that way too. To request that Google remove your site from its index, follow the steps listed at [www.google.com/remove.html](http://www.google.com/remove.html).

Finally, visit the Google Hacking Database (GHDB)—<http://johnny.ihackstuff.com>—to see how Google has exposed other websites to attack. You can (hopefully) thus learn how not to fall victim to the same tricks.

Every tool on the Internet can be used for good or for bad, and Google is no exception. If you run a website, you must learn about Google hacking in order to lock down your system's defenses. If you're just a curious and non-malicious individual, have fun experimenting with Google. You may find more than you ever imagined.

## THE NEXT STEP

With war dialing, port scanning, war driving, and Google hacking, hackers can locate nearly any computer connected to a phone line or the Internet. Unfortunately, once hackers find such a computer, they often can't resist the temptation to break in to it and explore it. And once a hacker has broken into a computer, the results could range from the hacker simply browsing around but altering nothing to his trashing the entire system and wrecking everything in sight. If you're in charge of a system's security, have fun trying to guard against the many ways someone can spy on your system. If you're a hacker, take your pick on which tactics to try first to peek past a computer's security defenses. No matter which method you use, there's a good chance one of them will work and help you circumvent even the most expensive computer security system in the world.