GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

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

PhoneSweep
The Corporate War Dialer

by Greg Hodes
SANS Security Essentials (GSEC) Practical
Version 1.2f

The saying, "a chain is only as strong as its weakest link," applies to the unsecured modem attached to a corporate workstation. Companies can spend millions of dollars on proxies, firewalls, and various other hardware/software solutions aimed at protecting their network. However, often times they over look the modems attached to computers on the network.

> Expensive and intimidating firewalls that guard your various public gateways can lead to a false sense of protection against outsider access to your computing resources. Almost no one contemplates the fact that firewalls are most easily circumvented by taking a back door -- a poorly secured dial-up server or an inadequately policed desktop modem -- to get into the network (McClure and Scambray).

The slogan on Sandstorm's (makers of PhoneSweep) website states, "One million dollars in firewalls and security can be defeated by one cheap modem" (Sandstorm.net). The unsecured modem provides a weak and often overlooked avenue into some of the most secure networks. Reports have been made that through unsecured modems, one was able to control a building's heating and lighting system. Other modems allowed access to the computers at a fire department's dispatch office (Shipley).

High speed digital internet access continues to grow and become more common place, in the United States. "The nation's major cable operators added 920,000 new high speed Internet cable modem subscribers … during the second quarter, bringing the number of cable modem customers in the U.S. to more than 5.5 million" (Beckwith and Chang). One would think that with the increase in the digital cable subscribers, the threat of an unsecured modem would diminish. However this isn't the case. Shipments of modems with new computers continue to grow. This has been attributed to the fact that a modem is practically standard equipment for computers sold today (PC World). Additionally, according to International Data Corp. (IDC) "more than 90 percent of all telecommuters use dial-up modems to log into their company's LAN. And IDC predicts that the majority will continue using dial-up modems until at least 2004" (Meinel).

In this paper we will look at the risk that an unsecured modem creates. Additionally we will briefly discuss how the hacker can take advantage of these exposures. Finally, we will look at the tool PhoneSweep and how it can help the Information Security Officer find and close these security holes.

© SANS Institute 2000 - 2005 Author retains full rights.

RISKS:

The risks associated with an unsecured modem depends on the gateway created by the systems connected to the modem. If the computer and modem aren't attached to a network, the risks are confined to the one workstation. Although this can be dangerous if the computer is in the CFO's office or the head of R/D for your corporation. If the modem is attached to the computer on the network the exposure is far greater. Imagine if the hacker got on the network through the modem on the network administrator's computer, the hacker would have the keys to the kingdom.

This threat to the confidentiality of the data also can cause compromises to the integrity of the information. If the hacker can see the data, he might also be able to modify the data. A hacker could decide to alter records on the network and cause all sorts of problems. The addition or removal of a simple decimal point could cause major problems for the entire company. Orders could be modified or deleted. Top Secret records could be read. The possibilities are endless with the right level of access and enough time.

An addition to the threat to the confidentiality and integrity of the data on the computer or the network, its availability is also at risk. Through the modem, the hacker could plant one or more DDoS zombies on the network. These zombies could then wake up and take down the entire network or any other target's network. The hacker could also gain access to the network's user database and, with enough time, lock out all the users. Imagine the ramifications of no one in the company being able to log on to the network.

An additional risk that an unsecured modem creates is for the hacker, or in this case phreaker, to make long distance calls for free. "A phreak is someone who breaks into the telephone network illegally, typically to make free long-distance phone calls or to tap phone lines" (searchSecurity.com). Some modems and phone systems allow you to activate a second dial tone when you enter a special code. Through these second phone lines, it is possible for the hacker/phreaker to make long distance calls for free (Sandstorm Enterprises PhoneSweep v3.01 User Manual). It is possible for the phreaker to call a local number, type in a special code to get a second dial tone, and then make international calls.

For a great list of the types of attacks made available by unsecured modems, look here: http://www.americasnetwork.com/issues/2000supplements/20001201nr/nr20001201_security.htm

TOOLS OF THE TRADE:

The practice of finding these unsecured modems is referred to as War Dialing. A war dialer is a software program, typically freeware, that is used to dial a predefined range of telephone numbers and report what it finds (searchSecurity.com). The popular choice for the hackers are ToneLoc and THC-Scan. ToneLoc, which stands for Tone Locator, is an old DOS based war dialer that has been around for a long time (Talisker's Network Security Tools). Another popular freeware war dialer is THC-Scan, which is short for The Hacker's Choice. THC-Scan is also a DOS based application. THC-Scan claims to be twice as good as ToneLoc (van Hauser). For a list of several other freeware war dialers, look here, at New Order's website: http://neworder.box.sk/box.php3?gfx=neworder&prj=neworder&key=wardil&txt=Wardialers

© SANS Institute 2000 - 2005 Author retains full rights.

Two popular commercial war dialers are PhoneSweep and TeleSweep Secure® Scanner 3.0. Both programs have a lot more features than their freeware counterparts and are aimed at the corporate world as a tool for vulnerability assessment. TeleSweep offers a Windows and Linux version and allows for distributed scanning (TeleSweep Secure® Dial-Up Vulnerability Scanner 3.0). PhoneSweep is only a Windows based application. We will now direct our focus on PhoneSweep.

PHONESWEEP:

PhoneSweep was introduced in September, 1998 as the first commercially available war dialer (Garfinkel). Sandstorm does not refer to PhoneSweep as a 'war dialer' as a way of separating itself from the illegal, poorly created hacker tools, such as ToneLoc and THC-Scan. "Sandstorm Enterprises refers to PhoneSweep as a **'Telephone Line Scanner'** to distinguish it from programs designed to commit illegal acts. It is legal, ethical and wise to use PhoneSweep to test your own phone systems for insecure modems" (Sandstorm Enterprises PhoneSweep v3.01 User Manual, 14).

PhoneSweep works by calling a predefined range of phone numbers and attempts to establish a connection with what is on the other end. It makes repeated calls to the same number in order to determine if the modem picking up is a fax machine, a data line, or both.

> PhoneSweep Plus, which works in a Windows environment, repeatedly calls all phone numbers maintained by a company, then searches for computers running remote access programs. The software does the job in three simple steps: connecting to a phone number, identifying the computer system to which the modem at the other end is attached, and attempting to log into that system by automatically trying common user name and password pairs (Gips).

FEATURES/ADVANTAGES:

PhoneSweep offers many advantages over its freeware brethren. PhoneSweep is expensive and with freeware war dialers like ToneLoc and THC-Scan available, it needs to offer something that the user can't find in the free software. In this section we will look at the features of PhoneSweep and show some of the benefits given to us by these features.

The freeware war dialers are made by hackers for hackers. Other than THC-Scan, with an official website of http://www.thehackerschoice.com, these programs have no official means of distribution or support. Having to resort to underground sources for this software can open up your network to additional problems. It is possible for these free war dialers to come with a virus or other type of "back door" (Sandstorm Enterprises PhoneSweep v3.01 User Manual, 12). Imagine if the freeware war dialer your company downloaded to test its network included a "phone home" feature that would send the hacker a list of your unsecured modems after it ran its scan. A hacker might claim to have a newer version of a certain war dialer, only to be distributing a virus or Trojan. To summarize a reputable, trusted source of downloading and support is an advantage had by using

© SANS Institute 2000 - 2005 Author retains full rights.

PhoneSweep.

PhoneSweep, having been created in 1998, is a Window's based application and does not really on the command line. "PhoneSweep has an easy-to-use graphical user interface that runs under Windows 95. The majority of the 'war dialers' that we reviewed run under DOS. A few of them would not work under the Windows 95 operating system" (Garfinkel). According to Sandstorm.net, PhoneSweep runs under all versions of Windows, including Win9x and NT/2000. Not having to go through a DOS command line to configure the program makes PhoneSweep a lot better than the older freeware, hacker tools. It is far easier for the average user to point and click to set up their scan than it is for them to memorize and use command switches. To reiterate, a benefit of PhoneSweep is that it is far easier to configure through a GUI than the freeware DOS versions, with their command line switches. However, for those so inclined, PhoneSweep can be run from a DOS prompt (Sandstorm Enterprises PhoneSweep v3.01 User Manual, 135).

One other feature that sets PhoneSweep apart from other war dialers is the fact that it requires a dongle to operate. War dialers all have the potential for abuse, and with the exception of the few corporate, white hat programs, that was their intent. Shortly after Sandstorm created PhoneSweep they realized the potential dangers of such a powerful program in the hands of the wrong people. To prevent this program from being used for abuse they developed a Hardware Licensing Device. "Each copy of PhoneSweep is distributed with a hardware license management device (also known as a dongle) that is required for proper operation" (Garfinkel). By requiring the use of a hardware licensing device it makes it harder for the program to be illegally distributed or shared. The dongle is branded with its own unique serial number, so "This traceability is designed to act as another deterrent to those thinking of 'sharing' or 'borrowing' the program" (Garfinkel). PhoneSweep will not make a call without the dongle present (Sandstorm Enterprises PhoneSweep v3.01 User Manual, 15).

Another advantage PhoneSweep has over the other products out there, especially the freeware, is that PhoneSweep evolves with changing technology. For example, the latest version of ToneLoc, version 1.10, has a last modified date of October 9, 1994 (Minor Threat and Mucho Maas). Surely in the last seven years, there have been advances in phone system technology. Similarly, THC-Scan is up to version 2, and it was last modified on December 25, 1998 (van Hauser). "Most of the current war dialers were written in the 1980s by high school students interested in committing toll fraud, said Garfinkel. The more recent ones, he added, were built by crackers who wanted to commit computer fraud" (Stutz). Outdated scanning software can lead to inaccurate results, and at the least make it more difficult to review what you've gotten.

Being able to identify the type of system on the other end of the modem is important to be able to eliminate and/or minimize the risks associated to unsecured modems. The freeware applications, being several years old, don't have the capability to determine the system answering the modem. PhoneSweep, on the other hand, has the ability to identify the type of system. As of Friday, Mar 9 2001 at 17:36:27 PhoneSweep can identify **303** systems (Sandstorm.net). Look here, on the Sandstorm website, for the complete and updated list of all identified systems: http://www.sandstorm.net/phonesweep/sysids.shtml So, another advantage of PhoneSweep is

© SANS Institute 2000 - 2005 Author retains full rights.

that it is still evolving and improving, thus providing faster scans, and more accurate results. Much of the freeware out there can be considered deadware since it is not being updated.

One key feature that PhoneSweep has over its competition is its ability to use single call detection. This feature is unique to PhoneSweep, and by being able to make some conclusions about a phone number in less calls, it will result in the completion of scans sooner (Sandstorm.net). In order to take advantage of single call detection, PhoneSweep requires that the modem meet certain standards. PhoneSweep will work with almost all modems, but special chipsets are required for faster scanning with single call detection.

Another distinct advantage PhoneSweep has over other programs is that it supports the use of multiple modems. PhoneSweep is scalable and thus can be configured to meet the needs of your company. At the present time Sandstorm offers a version of PhoneSweep that can support up to 16 modems and can make approximately 1000 calls an hour. Most all of the underground war dialers are only designed to use one phone line. As a result, large scans can take days, however, with PhoneSweep they can be completed in a fraction of the time. With its ability to provide detailed accurate results in less time, it is possible to make modem scanning a normal part of your company's security evaluation. Instead of doing this yearly, it is possible to do a scan on a quarterly or even monthly basis. Through the reports you can review a differential report and only concern yourself with what changed. The speed at which a scan can be completed as a result of multiple modem support is clearly an advantage PhoneSweep has over the competition. More on PhoneSweep's reporting capabilities later in this paper/

One important feature that puts PhoneSweep in a class by itself is its ability to do penetration testing as part of it scanning. Other war dialers, even some of the free ones, come with the ability to brute force penetrate systems, however the ease at which PhoneSweep operates make it better. The older programs, require scripts or manual entry of user names and passwords, PhoneSweep only requires that the Effort setting be set to PENETRATE (Sandstorm Enterprises PhoneSweep v3.01 User Manual, 22). The program lets you use a default list of user names and passwords or it allows you to customize your list. Another benefit that PhoneSweep has in this area is that since it can identify over 300 systems, it makes penetration testing a bit easier. If you know you are connecting to a Windows machine, user names like 'root' aren't likely to get you anywhere, where as 'administrator' is more likely going to be on the system. "Password guessing is only good if the program can automatically determine the kind of system it is running" (Stutz). To conclude, PhoneSweep allows for the user to, in one step, with one program, scan their system for modems and also attempt to penetrate them. There is no need to use a second program, exposing yourself to possibly a virus or another back door.

A war dialer is only as good as the results it generates. Most of the freeware programs out there provide very little reporting features. Generally speaking all you get out of them are simple logs of the number called and their results. PhoneSweep on the other hand provides detailed reports in the *.rtf format (Garfinkel). The template used to create the report is called reporttemplate.rtf and it can be customized to suit the needs of your company (Sandstorm Enterprises PhoneSweep v3.01 User Manual, 87). In addition to customizing the layout of the report template, you have the option to change what is displayed in the report. You

© SANS Institute 2000 - 2005 Author retains full rights.

can display different sections depending on your desires.

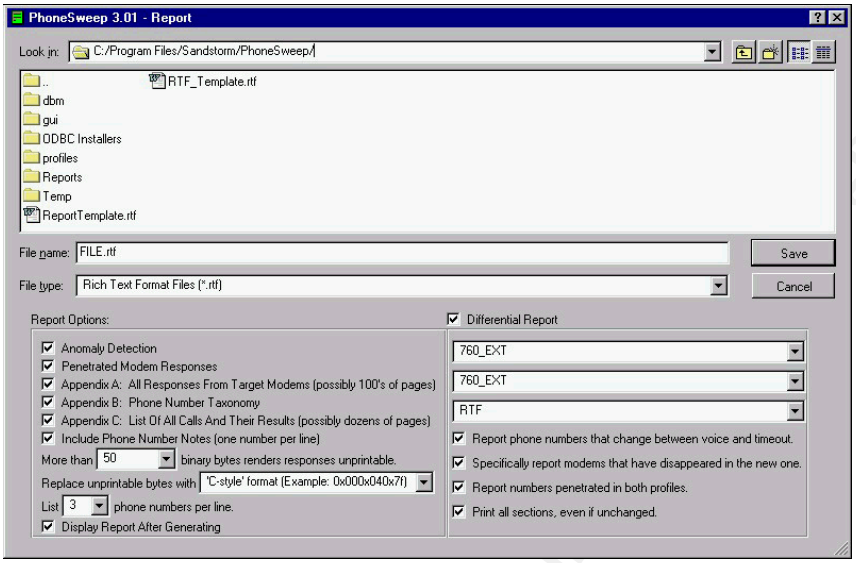
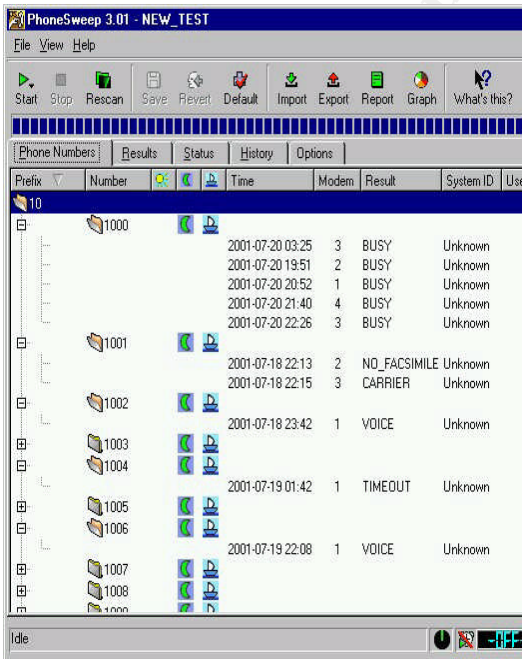


Figure 1 - Screenshot created 5 September 2001

In addition to the detailed reports generated by PhoneSweep, one can easily see the results of the scan in a couple of other ways. One way to see the results is by phone number called. It is possible to pick the phone number from the list and see the results of the scan. Another way to do it is by looking at the results by type. You can look through the results for all the Voice numbers for example. It is possible to check the Results tab in real time, so it is possible to see some of the results before the scan is complete (Sandstorm Enterprises PhoneSweep v3.01 User Manual, 77).



© SANS Institute 2000 - 2005 Author retains full rights.

Figure 2 - Screenshot created 5 September 2001

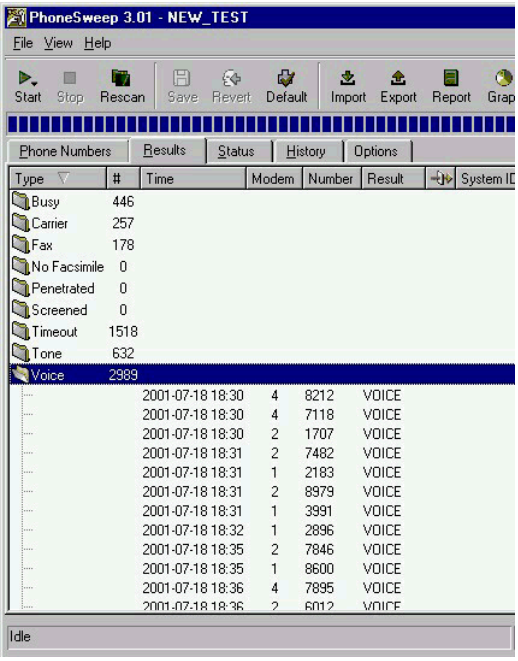


Figure 3 - Screenshot created 5 September 2001

Finally, new to PhoneSweep 3.0, is the ability to export the results to an Excel 2000 graph. PhoneSweep 3.0 includes "a 'graph' button that will create a Microsoft Excel 2000 graph of scanning results, ideal for executive presentations" (Sandstorm Announces PhoneSweep 3.0). This feature creates an easy to read and understand pie chart ideal for executives who don't want to read huge 100 page reports.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

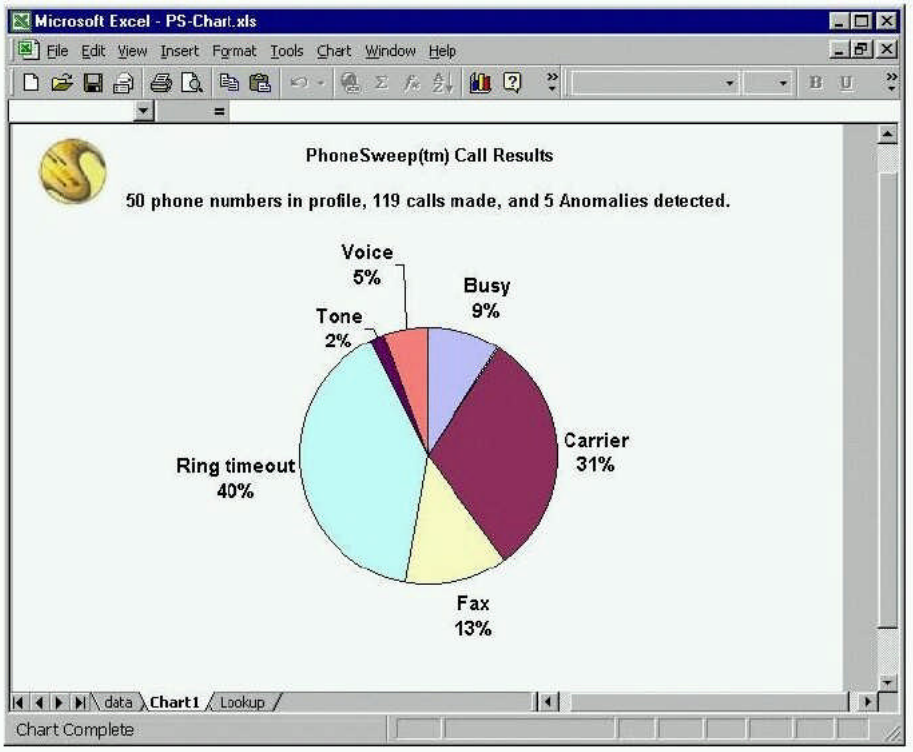


Figure 4 - Sandstorm Enterprises PhoneSweep v3.01 User Manual, 93

PhoneSweep also provides the ability to do a "Differential Report" (Sandstorm Enterprises PhoneSweep v3.01 User Manual, 91). These Differential Reports allows you to compare the results of two different scans and display what changed between them. See Figure 1 to see the options available for this type of report. The benefits of this report is to determine if the problem of unsecured modems has gotten better or worse. This type of report is valuable for creating a benchmark in order to test the effectiveness of your company's modem policy.

COSTS:

As it seems with most security software, if it is cheap, it isn't any good. Most computer, network security software seems to come at highly inflated prices, and PhoneSweep is no exception. PhoneSweep's high price is in part a method to keep it out of the hands of the hackers. Since PhoneSweep is so expensive, and they don't offer a demo version, the average hacker is going to go elsewhere for their phreaking needs (Garfinkel). PhoneSweep comes in five 'flavors' depending on your needs. The Basic version, which sells for under $1000, only allows for 1 modem and a limited number of calls per profile. The Plus version of PhoneSweep comes in 4 variations, allowing for 4, 8, 12, or 16 simultaneous modem connections. The Plus 4 and Plus 8 models only allow 10,000 phone numbers per profile, whereas the Plus 12 and Plus 16 allow for 20,000 numbers in each profile. The Plus 16 version costs $11,200, clearly out of the price range of the average hacker. Even with such high prices, the cost for PhoneSweep only goes up when you buy technical support or the recommended hardware through them. The price for one year of support increases the price approximately 15 to 20 percent. Through Sandstorm

© SANS Institute 2000 - 2005 Author retains full rights.

you can also buy the modems and the multi-port cards that take advantage of PhoneSweep's features (Sandstorm.net).

CONCLUSION:

An unsecured modem is like a screen door at the Pentagon. The door may or may not be locked, but the level of security is not nearly as strong as with the heavily armed, gun toting soldiers at the front door. No matter how strong the perimeter of your network is, an unsecured modem can create a hole exposing the entire network to danger. Tools designed to find and take advantage of these modems have been around for about twenty years (Garfinkel). Originally only hackers created and used war dialers, but eventually smart security administrators realized the value of a war dialer in vulnerability assessments. Corporations began using these underground war dialers to test their systems. Before long they realized that these tools just weren't good enough.

On September 1st, 1998, Sandstorm released PhoneSweep, the first of its kind corporate, telephone line scanner (Garfinkel). Armed with features unavailable in the freeware version, PhoneSweep set it sights on releasing a product for legitimate uses. With a hardware licensing dongle, high prices, and no demo versions, PhoneSweep did an excellent job to keep itself out of the hands of hackers and phreakers. The features available in PhoneSweep also make it a beneficial tool for vulnerability scanning. The new and improved graphic interface makes it easier to configure and use than the old, out dated, command line versions. Also, the ability to use multiple modems simultaneous and in single call detect mode allows the administrator to complete large scans in a fraction of the time, with far more accurate results. Finally, since PhoneSweep is only available through legitimate means of distribution, exposure to secret, hidden virus or backdoors are improbable. In order to get the free underground war dialers you have to download them from unknown sources, with no support. A hacker could disguise a virus as a new war dialer, and infect every computer it connects to.

To sum up, PhoneSweep is a fast, effect telephone line scanner, aimed at corporations interested in protecting their network from unsecured modems. It benefits and features justify paying for a program and not rely on a free war dialer found somewhere on the internet. The risks created by an unsecured modem are too great to ignore.

PhoneSweep version 3.01's homepage is http://www.sandstorm.net

© SANS Institute 2000 - 2005 Author retains full rights.

REFERENCES:

_____. Definition – Phreak. searchSecurity.com, 8 May 2001, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212783,00.html (5 September 2001).

_____. Definition – War Dialer. searchSecurity.com, 23 April 2001, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci546705,00.html (5 September 2001).

_____. "Sandstorm Announces PhoneSweep 3.0" Help Net Security, 28 June 2001, http://www.net-security.org/text/press/987516790,14570,.shtml (7 September 2001).

_____. "Is Dial Up a Dinosaur?" PC World, 21 March 2000, http://www.pcworld.com/news/article/0,aid,15864,00.asp (5 September 2001).

_____. "PhoneSweep" Idsec Limited, http://www.idsec.co.uk/phonesweep.html (6 September 2001).

_____. "Phreaking Tools" New Order, http://neworder.box.sk/box.php3?gfx=neworder&prj=neworder&key=phtls&txt=Phreaking%20tools (6 September 2001).

_____. "Sandstorm Enterprises PhoneSweep v3.01 User Manual" 12 April 2001.

_____. Sandstorm Enterprises, Inc. http://www.sandstorm.net/ (5 September 2001).

_____. "Talisker's Network Security Tools" http://www.networkintrusion.co.uk/wardial.htm (5 September 2001).

_____. "TeleSweep Secure® Dial-Up Vulnerability Scanner 3.0" SecureLogix Corp. http://telesweepsecure.securelogix.com/ (5 September 2001).

_____. "War Dialer" Whatis?com. 23 April 2001, http://whatis.techtarget.com/definition/0,289893,sid9_gci546705,00.html (6 September 2001).

_____. "War dialers" New Order, http://neworder.box.sk/box.php3?gfx=neworder&prj=neworder&key=wardil&txt=Wardialers (6 September 2001).

Beckwith, David and Lori Chang. "Cable Continues Rapid Deployment Of Broadband Services" National Cable & Telecommunications Association, 13 August 2001, http://www.ncta.com/press/press.cfm?PRid=169&showArticles=ok# (5 September 2001).

Davidson, Bob. "Telephone Network Security" America's Network, 1 December 2000, http://www.americasnetwork.com/issues/2000supplements/20001201nr/nr20001201_security.htm (6 September 2001).

© SANS Institute 2000 - 2005 Author retains full rights.

Garfinkel, Simon L. "Advanced Telephone Auditing with PhoneSweep: A Better Alternative to Underground 'War Dialers'" December, 1998, http://www.mids.org/mn/812/sim.html (5 September 2001).

Garfinkel, Simson L. "Comparison of THC-SCAN v2.0 with Sandstorm PhoneSweep 1.02" 29 Dec 1998. http://www.dataguard.no/bugtraq/1998_4/0770.html (5 September 2001).

Gips, Michael A. "Dial M for Modem" Security Management Online, September 1999, http://www.securitymanagement.com/library/000720.html (6 September 2001).

Gold, Steve. "Shipley Develops Commercial War-Dialer For Sandstorm Enterprises" Newsbytes ,14 December 1998, http://www.newsbytes.com/news/98/122999.html (5 September 2001).

King, Nathan A. "Penetration Testing" Information Security, June 2000, http://www.infosecuritymag.com/articles/june00/features1.shtml (6 September 2001).

McClure, Stuart and Joel Scambray. "Security Watch" InfoWorld, 11 January 1999, http://www.infoworld.com/cgi-bin/displayArchive.pl?/99/02/o08-02.77.htm (5 September 2001).

Meinel, Carolyn. "It's 2 a.m. Do You Know Where Your Modems—Both Unauthorized and Authorized—Are?" Messageq.com, August 2000, http://www.messageq.com/security/meinel_1.html (5 September 2001).

Minor Threat and Mucho Maas "ToneLoc v1.10 User Manual" SecurityFocus.com, 9 October 1994, http://www.securityfocus.com/tools/48 (5 September 2001). NOTE: Unable to get to the official homepage - http://www.paranoia.com/~mthreat

Shipley, Peter "Remote Access" NetworkCommand.com http://www.networkcommand.com/docs/ras2.html (6 September 2001).

Stutz, Michael "War Dialer Goes Corporate" Wired News, 7 October 1998, http://www.wired.com/news/print/0,1294,15483,00.html (5 September 2001).

van Hauser "THC-SCAN v2.00" The Hacker's Choice, http://www.thehackerschoice.com/releases.php (5 September 2001).

© SANS Institute 2000 - 2005 Author retains full rights.