

# War Dialing Your Company: A HowTo

## Overview

“Hello ... Hello?” It sure *seems* like there’s someone there. But there’s no response, and after a moment you hang up. Somewhere a log entry is made recording your phone number followed by the notation ‘Timeout’, meaning that there was no modem response within the specified waiting period. Your phone has just been scanned.

With firewall and related security software improving every day, users find their Internet activities are increasingly watched and sometimes blocked. Management may view such filtering as a way to increase productivity.(3) For those who want to circumvent these controls, it’s a simple matter to pick up a free or very inexpensive modem, let Windows recognize it and install the drivers, then plug the cable into an unused port in a nearby cubicle. Such unauthorized modems are not likely to be set up for outgoing calls only, or to require sufficient authentication on inbound calls. Though the main gateway to your network, the firewall, probably offers extensive logging of user activity, modems generally bypass the firewall and its logging and connect directly to the internal network.(3) For ‘outsiders’ that may wish to gain unauthorized entry into your network, these modems present an enticing target.

Though there are programs that scan for network vulnerabilities, they ignore a portal used in many attacks: the phone system. “War dialers”, so named because of the 1983 movie ‘War Games’ that brought them to the big screen, were originally developed by and for “phone phreaks” seeking free long-distance service.(1) They’re quite well suited to the task of finding modems. Someone’s going to be scanning your phone numbers for modems; if you scan first and close the holes, they are less likely to find an open door to your network.

There are two classes of phone scanning software: commercial products and freeware. Two well-known commercial products are Telesweep Secure from <http://www.securelogix.com> (4) and PhoneSweep from <http://www.sandstorm.net> (5). For large companies and those with the most stringent security requirements, there’s no question that commercial phone scanning software provides the most robust feature set, along with wider hardware compatibility and vendor support.

One prominent advantage of commercial products is the ability to place multiple calls in parallel on multiple phone lines, making 50-100 calls per modem per hour while storing the result in one database.(1) The SecureLogix product is able to use the existing modems dedicated for RAS to create a high-density dialing system.(5) TeleSweep Secure can identify 48 dial-up/remote control systems by name, while PhoneSweep can identify over 250. Other important features include advanced reporting, documentation, support, and even automatic penetration attempts when modems are detected.(2)

If you’re unfamiliar with phone scanning, freeware products can move you up the learning curve and help you determine which features mean the most to you. And, for

those with limited budgets, you'll be using the same software that's likely to be used in an unauthorized scan. The current freeware product of choice is THC-Scan (The Hackers Choice) available from <http://thc.pimmel.com> (6) and various other locations on the 'net.

## Installation

THC-Scan is a DOS program that I've run on Windows 95 and 98. The main web site says it will also run on NT, and on DOS emulators (UNIX) on 80x86 processors. Some 'hacker' sites have been known to offer versions of this type of product with hidden virus or Trojan software, so a safe approach is to set up a Windows 9x machine with a network connection outside of your firewall, or simply as a standalone PC with dial-up networking. Requirements are minimal, so an old Pentium 100 is more than adequate for the job. An old 14.4 modem, preferably one with jumpers that allow you to select the COM port, is much more likely to be recognized by THC-Scan than a new one. The software looks for the modem on COM 1 through COM 4 only, so a Winmodem on COM 5 simply isn't going to work.

Plan to BOTH download *and* install THC-Scan using the isolated PC, just to be on the safe side. If the machine does become infected, the damage will be contained. The zip file is only 541 KB, which doesn't take long to retrieve even with an older modem.

- Unzip THC-TS20.ZIP to a clean folder, e.g. C:\Temp.
- Unzip the resulting TS-BIN.ZIP to that folder, creating a BIN subdirectory.
- Unzip TS-DOC.ZIP to that folder, creating a DOC subdirectory.
- Run C:\Temp\bin\MOD-DET.EXE to detect the modem and capture settings for the configuration. Note that that MOD-DET.EXE only searches COM1 - COM4, and typically fails to find a compatible modem on the first attempt, but does find it on the second attempt. The COM Port, IRQ, and Base address information displayed in this step should be recorded for the next step.
- Run C:\Temp\bin\TS-CFG.EXE and choose MODEM CONFIG. Replace the default values for COM Port, IRQ, and Base Address with those found by MOD-DET.EXE.
- Note that the modem speaker may be turned off by changing the 2<sup>nd</sup> Init String from 'ATS11=64 S10=50' to 'ATS11=64 S10=50 M=0'. This allows the scan to be conducted silently.
- A Timeout value of 30 seconds under SCANNING OPTIONS seems to work well.

There's loads of information in the DOCS folder, and many options that can be tweaked, but these steps should be sufficient to get you started.

In a DOS Window, run "DOSKEY" if you're planning to scan a block of numbers at a time, then enter "C:\Temp\bin\thc-scan.exe 123-123x" to scan 123-1230 thru 123-1239. That's literally the first part of the phone number followed by an 'x'. The program does not use the normal modem setup, so if you need to dial a number like '9' to reach an outside line, you'll have to specify it here - e.g. 9,123-123x. By first running DOSKEY you can use the Up arrow to retrieve the last command and change one or more digits of the scan target. Larger blocks of numbers could be scanned by using 9,123-12xx, or

9,123-1xxx, etc. I didn't find an option for dialing a single phone number, and if you don't include at least one 'x' the program will err.

Output is placed in the installation BIN folder and includes a carrier.log or tone.log containing the 'interesting' numbers, and when doing a CARRIER scan includes a carriers.log that captures responses such as banner pages and login prompts.

## Approach

A few decisions must now be made. Of course you've already informed your supervisor of your intention to scan for modems, and obtained a signed statement to that effect if appropriate. But should you 'go public' with your plans? While it may be difficult to hide the fact that you're conducting a scan, savvy users will avoid detection by disconnecting their modems. Should you conduct your scan during business hours? PC's with rogue modems used for Internet access may be shut down after hours, while those used with remote-control applications may answer only after hours. How will you approach users found to have unauthorized modems or inadequate authentication?

A big advantage you'll have over an outsider is access to your phone administrator. They can provide you with the complete range of numbers handled by your phone switch, a description and jack location for each, numbers assigned to RAS servers, and maybe even a list of 'known' modems and FAX machines. This can save you loads of time that you might otherwise spend trying to use Telnet or remote-control software to connect to a modem that turns out to be a FAX. And, you want to make sure the numbers you're scanning are your own!

Plan to scan all of the numbers handled by your phone switch. The log files generated will tell you which numbers produced "interesting" results – those that you'll want to visit manually. Once the scan is complete you should save the log files generated by the scan to a floppy, and format the drive on the PC used for the scan before putting it on your network. With a list of possible modems in hand, you're free to use any PC/modem that you wish. You'll be using this PC to attempt connections to the modems you've found, so it should have any software you wish to try. Common applications to try include remote-control software, telnet, and Windows dial-up networking.

On my first scan, I was surprised to find several modems that answered a call placed by the remote control software that we use, but didn't prompt for a password. One was an administrator, logged in to the network with the Administrator account. Imagine the potential damage if someone else had found it first! My choice during this first scan was to protect the identities of those users, but to immediately implement authentication and verify that it was working properly. So I approached the offenders one by one to explain my findings and the changes that were required, and found everyone to be cooperative.

## Recommendations

**Define strict policy with associated punishment.** Not a solution, but at least a deterrent, and an important first step.(3)

**Consider modem registration.** A policy of registering all modems with the security staff will help to ensure that modems are set up properly the first time, instead of only when they are found by your scans.

**Verify the need for every modem.** As an 'insider' you have some advantages, and you should use them. After you've completed your scan and closed the obvious holes, take the report provided by your phone administrator and contact everyone that has a modem, even if they didn't show up in the scan. In my experience, a large percentage of users had either inherited the PC from someone else and didn't use the modem, or no longer performed the functions that had required it. After removing the modems, make sure to have the phone administrator disconnect the phone line at the switch.

**Put dial-in servers on a separate 'zone'.** Many companies now have a dial-in NT server running RAS (Remote Access Services) or something similar. Once dialed in and authenticated, dial-up users have all of the same privileges as an internal user. Since many firewalls now support multiple 'zones', consider putting the dial-in server on a zone by itself rather than on the internal side of the firewall. Not on the DMZ with your web servers, but in an isolated zone where you can specify exactly what services are and are not allowed between that zone and any other zone. That way, an unauthorized user that gains access to your dial-in server still has the firewall to contend with.

**Use phone extensions.** If your company has a phone switch, your phone administrator may be able to assign extensions to the dial-in modems rather than direct numbers. So, instead of dialing 123-1234 to reach a modem, you might dial 123-1234, then a 1 because you know the extension you wish to reach, then that extension e.g. 2345. Your dial-up networking in Windows would now be set to dial 123-1234,,1,2345. Your phone administrator can assign extensions that are only reachable through a central number and an extension, and not through a normal 7-digit number. One big advantage is that such numbers are considerably less likely to be found by scanning software.

**Change the access numbers periodically.** One reason for this is that former employees may still be dialing in, using the credentials of another employee or a customer, with or without their knowledge.

**Understand that not all modems can be eliminated.** For many common processes, there's simply no good alternative. Concentrate on eliminating unnecessary modems and properly securing the rest. Security is vital, but users must be able to perform their job functions.

**Schedule phone scans periodically.** Hopefully your subsequent scans will be less exciting than the first. As more companies offer web interfaces to their business systems, the number of necessary modems should drop.

**Consider Intrusion Detection.**(3) The article referenced describes two low-cost intrusion detection techniques.

(1) 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>

(2) King, Nathan A. "Sweeping Changes for Modem Security". June 2000.

<http://www.infosecuritymag.com/jun2000/junpentesting.htm>

(3) Powell, Dan; Schuster, Steve; Amoroso, Ed. "Local Area Detection of Incoming War Dial Activity".

[http://www.att.com/isc/docs/war\\_dial\\_detection.pdf](http://www.att.com/isc/docs/war_dial_detection.pdf)

(4) SecureLogix Corporation, <http://www.securelogix.com>

(5) Sandstorm Enterprises, Inc. <http://www.sandstorm.com>

(6) The Hackers Choice. <http://thc.pimmel.com>