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

War Dialing and War Driving: An Overview

Ruth Cowell
GSEC Practical Assignment
Version 1.2e

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

Table of Contents

Table of Figures……..……..3

War Dialing and War Driving: An Overview……..……4

Abstract……4

Introduction……4

War Dialing……..4

What is War Dialing?……..4
War Dialing Example……..5
War Dialing Products……..5
Using PhoneSweep™ on the Raw Data from Peter Shipley's Scans……..7

War Driving……7

What is War Driving?…….…7
War Driving Example…….….8
War Driving Tools……8
Mapping of War Driving Data……9

Recommendations……..10

Conclusions……11

References……12

Appendix A……14

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Figures

Figure 1. PhoneSweep's Phone Number Tab ……..6

Figure 2. A Map of Corporate Wireless Network Names and Locations in a Section of San Francisco……...9

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

War Dialing and War Driving: An Overview

Abstract

This paper begins with an introduction to the concepts of war dialing and war driving. This is followed by several sections on war dialing. These include a brief explanation of war dialing and an example. A discussion of some of the war dialing (or phone scanning) products that are available will follow. The sections on war dialing conclude with a brief look at the raw phone scanning data gathered in the example study, after it has been run through a commercial phone scanning product's identification engine. This will help the reader to become more familiar with both the type of information that can be gathered using war dialing, as well as some of the capabilities available in commercial phone scanning products.

The sections on war driving follow a similar approach. They begin with an explanation of war driving, followed by an example. This is followed by an introduction to some of the war driving tools that are currently available. The section on war driving concludes with a look at a mapping of some of the war driving data gathered in the example study. The paper itself will wrap up with recommendations on how to avoid becoming a victim of these attacks, followed by the conclusion.

Introduction

War dialing is a method used to hack into computers by exploiting features of the traditional phone system. It was first brought to the public's attention in 1983, when Matthew Broderick engaged in it in the movie "War Games".[1] Corporations are particularly vulnerable to war dialing due to the manner in which phone numbers are typically assigned within corporate locations.

War driving applies the basic principles of war dialing in order to target security vulnerabilities presented by wireless networks. These vulnerabilities are caused in large part by weaknesses in the WEP (Wired Equivalent Privacy), which is an algorithm that is part of the IEEE 802.11, the standard for wireless LANs. Again, corporations are particularly vulnerable as increasing numbers of them go wireless.

War Dialing

What is War Dialing?

War dialing uses a software program to automatically call large numbers of telephone numbers in

© SANS Institute 2000 - 2005 Author retains full rights.

a defined range to search for ones that have a modem attached.[2] The hacker simply enters an area code and the three digit exchange of a phone number. The war dialer will then call all numbers having that area code and starting with that exchange. Corporations are particularly vulnerable to this type of attack because each of their locations is typically assigned phone

[1] Owens, p.1.
[2] McFedries.

numbers having the same area code and exchange. Armed with a log of phone numbers of the modems that answered, the hacker may then attempt to gain unauthorized access to the computer system attached to the modems. Some of these programs can also determine which operating system is running on the computer and perform automated penetration testing. To do the latter, the war dialer runs through a list of common user names and passwords in order to gain access to the computer. [3]

War Dialing Example

The following is an example of war dialing, albeit benign. Peter Shipley is a computer consultant in the San Francisco Bay area. In the late nineties he spent several years completing a study in which he dialed every telephone number in the 508, 415, 510, 650, and 708 exchanges. His goal was to find the number of modems that represented a security risk to their owners. He wanted to use this number to make the public more aware of the threat that unprotected modems present.[4] Shipley found dial-ups to many vulnerable personal computers, as well as to hotels and even banks. He had potential access to such sensitive information as medical records and fire department dispatch computers.[5] His work did help to bring media attention to the issue, and his results will be discussed later in the paper.

War Dialing Products

It is likely that eventually someone will scan a given company's phone numbers looking for unprotected modems. It is therefore a good idea for the company to scan themselves first. This will bring to light any unprotected modems, and the door can then be closed before an unauthorized scanner is able to walk through. Unfortunately, network vulnerability scanners overlook the threat presented by unprotected modems, so phone scanning software must be used.

Phone scanning software falls into two types: freeware and commercial. Starting with the freeware type can help the novice to become more familiar with the features of a phone scanner and to determine which features are important to him or her. Another advantage of using the freeware type of scanner is that this type of software is more likely to be used by an unauthorized scanner. [6] THC-Scan (with THC standing for The Hacker's Choice) is one of the more popular freeware scanners, and available at **http://www.thehackerschoice.com/releases.php**.[7]

In contrast, commercial phone scanners are more appropriate for large companies having strict

© SANS Institute 2000 - 2005 Author retains full rights.

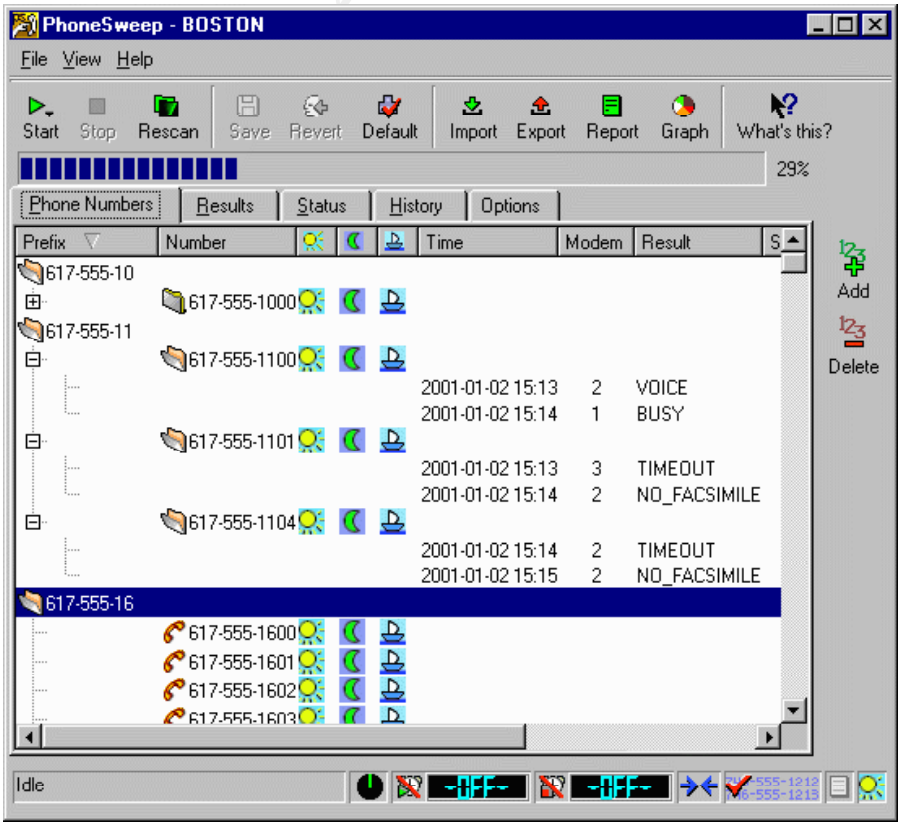
security requirements. Commercial software provides more robust feature sets, as well as wider vendor support and hardware capabilities. One of the big advantages that commercial phone scanners have over freeware scanners is that they can make multiple calls in parallel, on multiple

[3] whatis?com
[4] Poulsen, p.3.
[5] Johnson, p.1.
[6] Owens, p.1.
[7] The Hacker's Choice.

phone lines. They can make up to 100 calls per modem per hour, and send all the results to one database. (In order to perform multiple-modem scanning with THC-Scan, the user must run multiple copies of THC-Scan.)[8] Other commercial software features include documentation, reporting, and automatic penetration testing. Two of the better-known commercial phone scanners available are Telesweep Secure from SecureLogix and PhoneSweep, put out by Sandstorm Enterprise, Inc.[9]

PhoneSweep™ was the first commercial telephone scanner, and was introduced in 1998. According to its web site, it is the number one commercial phone scanner in the world.[10] It supports up to 8 modems and can identify over 200 different dial-up systems. These include "AUDIX Voice Mail, Carbon Copy™, Cisco RAS, Citrix ICA WinFrame, NetWare CONNECT, pcANYWHERE™, PPP, Shiva LanRover, Windows NT RAS, and XyLogics Annex."[11] *Figure 1.* illustrates the use of the Phone Numbers tab in the PhoneSweep GUI. [12]

Figure 1. PhoneSweep's Phone Number Tab



© SANS Institute 2000 - 2005 Author retains full rights.

[8] Johnson, p.1.
[9] Owens, p.1.
[10]Sandstorm Enterprises, Inc.(a), p.1.
[11] Johnson, p.3.
[12]Sandstorm Enterprises, Inc.(c), p.1.

UsingPhoneSweep™ on the Raw Data from Peter Shipley's Scans

Sandstorm Enterprises, Inc., the creator of PhoneSweep, was given access to the raw data that Peter Shipley collected during the war dialing study discussed above. It used this data to test the PhoneSweep identification engine. Of the 17725 total modems detected, there were 5783 systems identified by the engine (or 33.32%). [13]

Appendix A contains a list of the types of systems that were identified. (Information that would identify specific companies, etc. has not been included). The total number of each system type that was identified and the percentage of the total modems detected that each type represented is also listed. After looking at the data, it is easy to see why the results of Shipley's study drew a lot of media attention. The fact that a full third of the systems associated with specific phone numbers were identified should illustrate to the reader both the strength of current phone scanning software as well as the threat that unprotected modems represent to the public.

War Driving

What is War Driving?

War driving is one of the latest hacker fads, and is closely related to war dialing. Both involve scanning, in order to gain unauthorized access to computers and networks. War dialing, however, involves using software and a stationary computer to scan for unprotected modems. War driving, on the other hand, involves driving around and scanning in search of unprotected 802.11 wireless networks.[14]

The 802.11 access points and cards currently on the market use WEP (Wired Equivalent Protocol) for security. WEP is supposed to make it hard to eavesdrop on a wireless network or gain access to one without authorization.[15] Researchers at University of California at Berkeley, however, have recently discovered a number of problems with the WEP algorithm. Although an in-depth description is beyond the scope of this overview, the following is a list of the types of attacks they discovered:

- Passive attacks to decrypt traffic based on statistical analysis.
- Active attack to inject new traffic from unauthorized mobile stations, based on

© SANS Institute 2000 - 2005 Author retains full rights.

known plaintext.
- Active attacks to decrypt traffic, based on tricking the access point.
- Dictionary-building attack that, after analysis of about a day's worth of traffic, allows real-time automated decryption of all traffic.[16]

[13]Sandstorm Enterprises, Inc.(b), p.1.
[14]Zurko, p.1.
[15]Poulsen, p.2.
[16]Borisov, et al., p.1.

Despite its reported flaws, using WEP should still be better than using nothing for security, yet many wireless installations don't even use WEP. Those that do may still be open to attack if they have the encryption key set to one of the commonly known defaults.[17]

The authors of the Berkeley study point out that the listed attacks can be mounted using inexpensive off-the-shelf equipment, and they do recommend that anyone using an 802.11 wireless network employ other means along with WEP to protect that network.[18]

War Driving Example

The following example of benign war driving involves another study by Peter Shipley. It follows the formula: "laptop + wireless + GPS + car = war driving."[19] Using a special monitoring software on a laptop that is connected to a GPS receiver and a Lucent antenna on the roof of his car, Peter Shipley is "war driving" the streets of Oakland, San Francisco and parts of Silicon Valley, scanning for unprotected 802.11 wireless networks. His goal is to create a database that maps the location of open 802.11 wireless networks. His intent is not to help bad guys, and he won't be publishing the raw data. Instead, just as his intent with his war dialing study was to use the results to make the public more aware of the threat that unprotected modems present, his intent with the war driving study is to alert the public to the dangers presented by unprotected 802.11 wireless networks.[20]

War Driving Tools

Tools to aid in war driving are starting to become available. The following is a partial list of such tools:

A perl script by Peter Shipley to pull stat's from FreeBsd's wicontrol and lat/long from a GPS unit.
http://lists.bawug.org/pipermail/wireless/2001-April/000679.html

Two perl scripts by frisco@blackant.net, which he used to map around Ann Arbor, MI (supposedly there are some bugs in this so beware).
http://blackant.net/other/wireless.php

© SANS Institute 2000 - 2005 Author retains full rights.

A Windows application by Marius Milner <mariusm@pacbell.net> called NetStumbler. He hasn't released it yet, but you can get a copy for evaluation by emailing him. You can see his announce message on BAWUG and see a screenshot of it in action

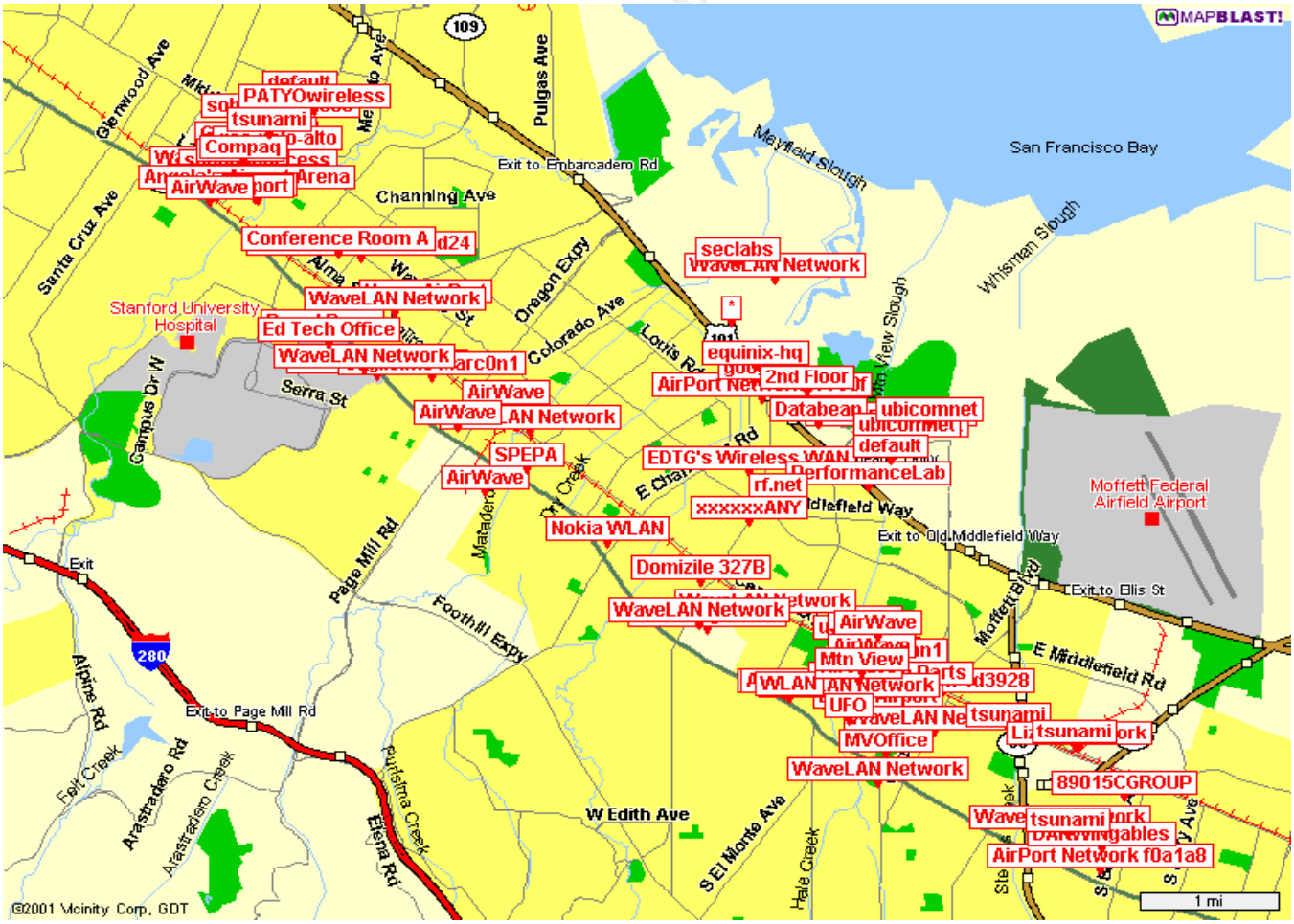
http://lists.bawug.org/pipermail/wireless/2001-May/000999.html
http://home.pacbell.net/mariusm/netstumbler.jpg [21]

[17] Zurko, p. 1
[18] Borisov, et al., p.1.
[19] vortex, p.1.
[20]Poulsen, p.3.
[21]Personal Telco Project, p.1.

Mapping of War Driving Data

Figure 2. is a map of the some of locations of wireless networks Shipley was able to identify in his study. This is one of seven such maps available at http://www.dis.org/wl/maps.[22]

Figure 2. A Map of Corporate Wireless Network Names and Locations in a Section of San Francisco



© SANS Institute 2000 - 2005 Author retains full rights.

As this and the other six maps illustrate, Shipley was able to identify the names of wireless networks as well as their latitude and longitude. He was also able to log signal strength and other vital stats.[23] Due to the vulnerabilities of WEP mentioned earlier, it is often a relatively easy matter to then gain unauthorized access to the wireless network from this point.

When Shipley locates an unprotected wireless network he only looks at the type of data that is

[22]Shipley, p.1.
[23]Poulsen, p.1.

being passed around, not the actual contents of files and e-mails (since that is a felony). There are, however, many programs currently available that can read such files and messages, should a bad guy choose to explore that option.[24]

Shipley recently sat with a friend in his car in the Silicon Valley parking lot of Sun Microsystems Inc. They were using laptops loaded with special monitoring software to observe lots of Sun's traffic, most of it coming from Windows machines. They were able to observe as someone transferred a file and someone else turned on an NT machine and received e-mail.

In a recent 90-minute drive in Silicon Valley, the two located more than 40 corporate wireless networks that appeared to be totally unsecured. They say they can find more than ten in just one block in downtown San Francisco. As frightening as this is, some security experts aren't surprised. As a matter of fact, one of them estimates that more than half of the wireless networks currently being operated now have no security at all. [25] For such networks, the potential is that laptop + wireless + GPS + car = disaster.

Recommendations

Recommendations to reduce exposure to war dialing and mitigate the effects of an attack include:

1. Use phone scanners to locate unprotected, unauthorized and unnecessary modems within your corporation, then protect or remove them.
2. Define a strict policy regarding use of such modems, and then stick to it.
3. Consider using one or more of the following:
   - Dial-up access authentication software for remote users
   - Use modem pools, so all modems are together and easier to restrict access to
   - Intrusion Detection[26]
4. Consider putting the dial-up server in a separate zone, where the administrator can define precisely which services are allowed between it and other zones.
5. Change access numbers at designated intervals, to prevent former employees from dialing in.
6. Assign extensions instead of phone numbers to dial-in modems, as it s harder

© SANS Institute 2000 - 2005 Author retains full rights.

for phone scanners to find them. [27]

Recommendations to reduce exposure to war driving and mitigate the effects of an attack include:

1. Use WEP, and avoid having the encryption key set to one of the commonly known defaults.

[24]Gomes, p.2.
[25]Gomes, p.2-3.
[26]Powell, p.5-6.
[27]Owens, p.3.

2. Anyone using an 802.11 wireless network should employ other means along with WEP to protect that network.[28]
3. Consider deploying a VPN (virtual private network), which would allow your communications to tunnel securely over the Internet.
4. "War drive" past your own corporation, and see what you find, before a bad guy does it for you.
5. Be aware that your transmissions extend beyond the perimeter of your building.
6. Be aware that your network name or "SSID" doesn't serve as your secret password. [29]

Conclusions

Despite the fact that war dialing has been around for almost two decades, it still presents a very serious security threat, particularly to corporate networks. This is because there are still plenty of unprotected modems out there, authorized or not. Corporations make particularly good targets for war dialers because phones and modems within a corporate location tend to share the same area code and three-digit exchange, so inputting that particular area code and exchange into phone scanning software is a promising method of locating modems.

Even more frightening than the threat presented by war dialing is the application of war dialing concepts in the search for unprotected wireless networks. Yes, the method has changed somewhat in that it has taken to the road, but it is still based on the concept of scanning, with the ultimate goal of locating unsecured portals into networks. The target in war driving, however, is the wireless LAN. As the cost of wireless technology continues to fall, the use of wireless networks is growing tremendously. So, therefore, is the threat.

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

[28]Borisov, et al.,p.1.
[29]Poulsen, p.2.

References

Borisov, Nikita; Goldberg, Ian; and Wagner, David.. "Security of the WEP algorithm." May 23, 2001. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (June 10, 2001).

Gomes, Lee. "Many wireless networks open to attack." April 27, 2001. http://www.zdnet.com/filters/printerfriendly/0,6061,2713009-2,00.html (June 9, 2001).

Johnson, Scott. "War-dialing: A Necessary Auditing Tool." September 20, 2000. http://www/sans.org/infosecFAQ/audit/war_dialing.htm (June 9, 2001).

McFedries, Paul. "The Word Spy." February 17, 1997. **http://www.logophilia.com/WordSpy/war-dialing.html** (June 9, 2001).

Owens, Dave. "War Dialing Your Company: A How To." December 10, 2000. http://www/sans.org/infosecFAQ/audit/war_dialing2.htm (June 9, 2001).

Personal Telco Project. "War Driving." May 17, 2001. http://www.personaltelco.net/index.cgi/WarDriving (June 9, 2001).

Poulsen, Kevin. "War driving by the Bay." The Register. April 13, 2001. http://www.theregister.co.uk/content/8/18285.html (June 9, 2001).

Powell, Dan; Schuster, Steve; and Amoroso, Ed. "Local Area Detection of Incoming War Dial Activity." **http://www.att.com/isc/docs/war_dial_detection.pdf** (June10, 2001).

Sandstorm Enterprises, Inc.(a) "Introducing PhoneSweep™." http://www.sandstorm.net/phonesweep (June 9, 2001).

Sandstorm Enterprises, Inc. (b) "PhoneSweep Identification: Peter Shipley Scans."

© SANS Institute 2000 - 2005 Author retains full rights.

http://www.sandstorm.net/phonesweep/ident.shtml (June 9, 2001).

Sandstorm Enterprises, Inc. (c) "PhoneSweep - Boston." **http://www.sandstorm.net/phonesweep/ps-numbr.shtml** (June 10, 2001).

Shipley, Peter. "maps of Pete's LanJacking." May 5, 2001. **http://www.dis.org/wl/maps/0417.gif** (June 10, 2001).

The Hacker's Choice. "Releases." 2001. **http://www.thehackerschoice.com/releases.php** (June 9, 2001).

vortex. "laptop + wireless + GPS + car = War Driving." April 17, 2001. http://www.free2air.org (June 9, 2001).

Whatis?com. "War Dialer." April 23, 2001. **http://whatis.techtarget.com/definition/0,289893,sid9_gci546705,00.html** (June 9, 2001).

Zurko, Mary Ellen. "LISTWATCH: items from security-related mailing lists." April 17, 2001. http://www.ieee-security.org/Cipher/Newsbriefs/2001/050101.ListWatch.html (June 10, 2001).

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

Appendix A

System Identification		#	%
>> unidentified binary protocol<<		10797	62.21%
>> unidentified text protocol <<		781	4.50%
ACCULINK Access Controller	6	0.03%	
AT&T 386 UNIX	6	0.03%	
AccessBuilder 4000	29	0.17%	
Advanced PICK O/S		2	0.01%
Annex Remote Access Server		28	0.16%
Ascend MAX Terminal Server		8	0.05%
Ascend MAX200 Terminal Server	9	0.05%	
Ascend Pipeline Terminal Server		47	0.27%
BLAST		2	0.01%
BSD/OS (UNIX)	11	0.06%	
Bay Networks System		40	0.23%
CRC Netpath 64 Frame Relay		3	0.02%
Carbon Copy		9	0.05%
Cisco	715	4.12%	
Citrix ICA WinFrame		168	0.97%
Cognitronics Announcer		2	0.01%
Convergent Technologies CTIX (UNIX)		1	0.01%
Cubix WorldDesk	5	0.03%	
DECserver 200 Terminal Server		8	0.05%
DECserver System	1	0.01%	
Data General AOS/VS System		6	0.03%

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

© SANS Institute 2000 - 2005 Author retains full rights.

Data General System MV/5500		**5**	**0.03%**
DataSMART T3 SMDSU		**2**	**0.01%**
Defender 5000		**18**	**0.10%**
Defender Security Server		**3**	**0.02%**
Dell UNIX System V		**2**	**0.01%**
Digital OpenVMS Alpha		**3**	**0.02%**
Digital OpenVMS System		**4**	**0.02%**
Digital OpenVMS VAX		**1**	**0.01%**
Digital VAX/VMS	**14**	**0.08%**	
Digital VaxCluster (VMS)		**1**	**0.01%**
Emulex ConnectPlus LT Remote Access Server		**1**	**0.01%**
FirstClass		**22**	**0.13%**
FreeBSD (Unix)		**4**	**0.02%**
HP Remote Assistant		**11**	**0.06%**
HP-UX (UNIX)		**8**	**0.05%**
Hermes II Macintosh BBS		**1**	**0.01%**
IBM 3708		**1**	**0.01%**
IBM 5251 Terminal		**4**	**0.02%**
IBM AIX (UNIX)	**79**	**0.46%**	
IBM PhoneMail		**2**	**0.01%**
IBM System/32		**8**	**0.05%**
IBM System/88		**5**	**0.03%**
InterLynx/400		**3**	**0.02%**
InterSystems MSM-PC/PLUS	**2**	**0.01%**	
Lansource WINport		**2**	**0.01%**
Lantronix		**4**	**0.02%**
Lighthouse Power Switch		**1**	**.01%**
Linux System (UNIX)		**23**	**0.13%**
MANAKON Telemanagement Console		**4**	**0.02%**
MediaGate EdgeCommander	**1**	**0.01%**	
Mentor PRO integrated database environment		**3**	**0.02%**
MichTron BBS		**1**	**0.01%**
Microware OS-9		**11**	**0.06%**
NCR 386/486 UNIX		**6**	**0.03%**
NetWare CONNECT Service Selector		**215**	**1.24%**
Netlink OmniLinx Switch		**73**	**0.42%**
Network Access SW (Digital VAX cluster terminal server)		**6**	**0.03%**
Octel System		**1**	**0.01%**
Octel Voice Processing System		**28**	**0.16%**
Open M for MS-DOS		**1**	**0.01%**
PC Anywhere		**494**	**2.85%**
PCBoard BBS		**21**	**0.12%**
PPP	**141**	**0.81%**	
PROMIS II System		**1**	**0.01%**

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

© SANS Institute 2000 - 2005 Author retains full rights.

Perle Model 3i PC Dial-up Server		**5**	**0.03%**
ProBoard BBS		**1**	**0.01%**
Procomm		**1**	**0.01%**
Procomm Plus		**7**	**0.04%**
Procomm Plus for Windows		**1**	**0.01%**
Procomm System	**33**	**0.19%**	
QNX Realtime OS	**20**	**0.12%**	
QuickMail		**5**	**0.03%**
ROLM CBX		**11**	**0.06%**
ROLM PhoneMail		**12**	**0.07%**
Red Hat Linux		**18**	**0.10%**
Remote2 Host		**13**	**0.07%**
Renex TMS-3		**1**	**0.01%**
SAGE System		**2**	**0.01%**
SCO Open Desktop (UNIX)		**6**	**0.03%**
SCO Open Server Enterprise (UNIX)		**6**	**0.03%**
SCO OpenServer (UNIX)		**61**	**0.35%**
SCO System (UNIX)		**84**	**0.48%**
SCO UNIX System V/386		**49**	**0.28%**
SOTAS Circuitsentry		**1**	**0.01%**
Schendler Elevator Corp. Lobby Monitor		**1**	**0.01%**
Searchlight BBS		**1**	**0.01%**
SecurID Prompt		**106**	**0.61%**
Secure Sentinel		**26**	**0.15%**
Shiva LanRover		**642**	**3.70%**
Sun Solaris (UNIX)	**3**	**0.02%**	
SunOS (UNIX)		**4**	**0.02%**
Sunsoft INTERACTIVE UNIX		**4**	**0.02%**
System V.4 (UNIX)	**4**	**0.02%**	
Telco Systems Inc. Route-24		**2**	**0.01%**
Telco Systems Inc. System		**4**	**0.02%**
TeleFinder BBS		**6**	**0.03%**
Telebit ACS		**17**	**0.10%**
Telebit NetBlazer		**54**	**0.31%**
TimePlex SYNCHRONY Enterprise Router		**1**	**0.01%**
TriBBS		**1**	**0.01%**
UNIX System		**73**	**0.42%**
US Robotics Courier Fax Dial Security Session		**1**	**0.01%**
US Robotics V.Everything Dial Security Session		**6**	**0.03%**
USL Unix System V		**37**	**0.21%**
Ultimate PLUS		**9**	**0.05%**
UnixWare		**1**	**0.01%**
Unknown with login: prompt		**2030**	**11.70%**
Unknown with username: prompt		**10**	**0.06%**
Virtual Advanced BBS		**1**	**0.01%**

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

WESCOM II Branch System		**4**	**0.02%**
WESCOM Phone System		**1**	**0.01%**
WILDCAT! BBS		**15**	**0.09%**
Wang VS		**5**	**0.03%**
WebFlow System	**3**	**0.02%**	
Wildcat! BBS for Win95/NT		**12**	**0.07%**
Worldgroup BBS	**6**	**0.03%**	
XETA System		**2**	**0.01%**
Xyplex System		**1**	**0.01%**
Xyplex Terminal Server		**1**	**0.01%**

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