Wardialing Brief

Kingpin

@Stake, Inc.
196 Broadway, Cambridge, MA 02139, USA.
http://www.atstake.com
E-mail: kingpin@atstake.com

Abstract. Wardialing consists of using a computer to dial a given set of telephone numbers with a modem. Each phone number that answers with modem handshake tones and is successfully connected to is stored in a log. By searching a range of phone numbers for computers, one can find entry points into unprotected systems and backdoors into seemingly secure systems. This brief introduces the wardialing concept, examines concerns with today's network setups, and lists free and commercial software products, whitepapers, news reports, and Internet resources.

Keywords: wardialing, telephony, security, modem

1 Introduction to Wardialing

Wardialing, or scanning, has been a common activity in the computer underground and computer serucity industry for decades. Hollywood made wardialing popular with the 1983 movie, *WarGames*, in which a teenager searching for a videogame company ultimately uncovers a government nuclear war warning system [1].

Seventeen years after the mainstream was made aware of wardialing activity, the problem of unprotected dial-up systems still exists in the majority of corporations.

The act of wardialing is extremely simple – a host computer dials a given range of telephone numbers using a modem. Every telephone number that answers with a modem and successfully connects to the host is stored in a log. At the conclusion of the scan, the log is reviewed and the phone numbers are individually dialed with a computer. The user then attempts to identify the systems, and, depending on the goals of the wardial, attempts system access. Many wardialing tools, depending on the modem used by the host, can also detect fax machines, private branch exchange (PBX) access points, and human voice.

Generally, an attacker would determine the range of phone numbers to wardial by finding a company's main number, fax number, or accessing company directories. This is often accomplished with publicly available information or retrieved from the company's dumpster.

"Unauthorized modems are one of the most overlooked security flaws in corporations today. Companies often have modem lines they don't even know are there." [2]

2 Concerns with Today's Network Setups

Many network infrastructures overlook the importance of securing the modems connected to dial-up telephone lines. Unprotected modems are often connected to an internal company network. Even if the target computer successfully prevents attacks coming from the Internet, the unprotected modem attached to the target computer can allow unauthorized access directly into the system. This could allow the intruder to connect to other systems inside and outside the corporate network.

"The best way into an organization's network may not be the front door, but via a modem into some desktop PC…" [3]

A typical corporate network setup will properly protect systems from unauthorized access coming from the Internet by putting in place firewalls, intrusion detection systems, and other security mechanisms. Unfortunately, the user-connected modems are left unprotected and insecure, thus allowing an attacker to come in through the "back door" and possibly gain system access and critical privileges (Figure 1).

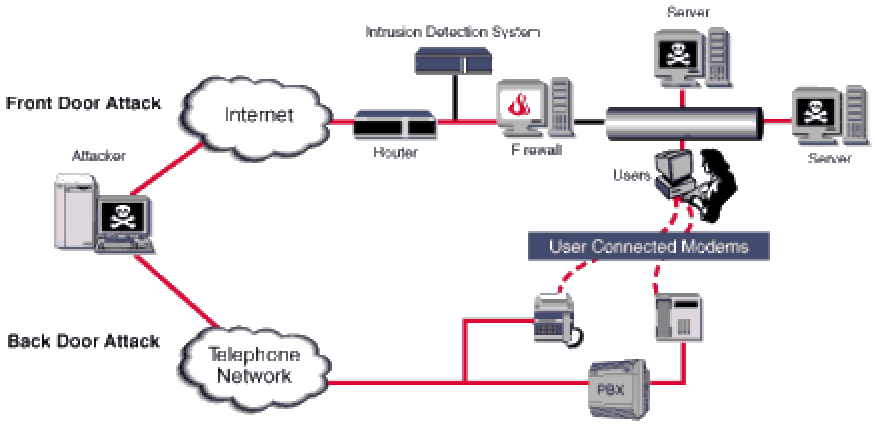

Figure 1: Typical corporate network with security focus on the Internet. [4]

Often, users will attach modems to their desktop PCs without alerting the system administrator. Network and system administrators need to be aware of the entire network topology and devices attached to users' machines.

Deregulation in the critical infrastructure areas, such as electricity and banking, also contributes to the security issues related to dial-up computer systems. Remote administration tools, specifically modems attached to telephone lines, are being installed at many sites to replace human control. This will allow a single administrator or group to control all the systems, regardless of location. However, if the security implications are not immediately addressed at installation time, the systems could be open to attack from an unauthorized user.

"Dial-up connections also let intruders access internal network resources without having to pass through any firewall or proxy, posing a threat that network administrators have very limited control over." [5]

Aside from user-connected modems, many other devices are connected to telephone lines and left unprotected, such as network routers, environmental control systems, elevator control systems, alarm systems, and PBX and telephone systems. Caution must be taken when configuring systems connected to any user-accessible telephone lines.

3 Whitepapers and Books

1. S. McClure, J. Scambray, and G. Kurtz, *Hacking Exposed*, Osborne/McGraw-Hill, 1999, ISBN 0-07-212127-0, Chapter 8: Dial-up and VPN Hacking pp. 266-288.
2. D. Powell, S. Schuster, and E. Amoroso, "Local Area Detection of Incoming War Dial Activity", http://www.att.com/isc.
3. G. White, "A Common Weak-Link in the Security Chain", http://www.securelogix.com.
4. G. White, "Protecting data networks by securing telephone networks", June 1999, http://www.securelogix.com.
5. Kingpin, "Handbook for BootyCall", March 2000, http://www.atstake.com.

4 News Reports

1. J. Littman, "Hacker Shocker: Research Project Reveals Breaches Galore", *ZDNet*, September 1997, http://www.zdnet.com/pcweek/news/0915/19awar.html.
2. S. Ranger, "Sun Sacks Employees For Modem Security Breaches", *Network* Week, May 1998, http://www.techweb.com/wire/story/TWB19980318S0012.
3. M. Stutz, "Wardialer Goes Corporate", *Wired News*, October 1998, http://www.wired.com/news/news/technology/story/15483.html.
4. J. Glave, "Crackers: We Control Your TV's", *Wired News*, July 1998, http://www.wired.com/news/news/technology/story/13838.html.
5. M. Nelson, "SecureLogix Builds Firewall to Fight Phone-Line Intrusion", *InfoWorld Electric*, November 1999, http://www.infoworld.com/articles/hn/xml/99/11/08/991108hnsecure.xml.
6. SecureLogix Corporation, "War Stories", http://www.securelogix.com/telesweepsecure/war.htm.

5 Commercial Products

1. Sandstorm Enterprises, Inc., "PhoneSweep™ Basic", US $980, http://www.sandstorm.net/phonesweep/index.shtml.
2. Sandstorm Enterprises, Inc., "PhoneSweep™ Plus", US $2800, http://www.sandstorm.net/phonesweep/index.shtml.
3. SecureLogix Corporation, "TeleSweep Secure™", http://www.securelogix.com/telesweepsecure/index.htm.
4. SecureLogix Corporation, "TeleWall™", US $29,000, http://www.securelogix.com/telewall/index.htm.
5. VerTTex Software, "ModemScan", US $389, http://www.verttex.com.

6 PC Resources

1. L0pht Heavy Industries, "Telephony Files Index", *Black Crawling Systems Archives*, http://www.L0pht.com/~oblivion/blkcrwl/telecom.html.
2. The Hacker's Choice, "THC-Scan 2.0", http://www.infowar.co.uk/thc/files/thc/thc-ts20.zip.

7 Macintosh Resources

1. L0pht Heavy Industries, "War Dialers", *Whacked Mac Archives*, http://www.L0pht.com/~spacerog/filelists/war.html.
2. H@ppy H@ck, "War Dialers", *H@ppy H@ck's Mac Site*, http://www.happyhack.com/pages/wardialers.htm.

8 Unix Resources

1. w00w00 Security Development, "ShokDial", http://www.w00w00.org/w00w00/ShokDial/.

9 PalmOS® Resources

1. Kingpin, "BootyCall", http://www.atstake.com.

References

1. The Internet Movie Database, Ltd., "WarGames (1983)", http://us.imdb.com/Title?0086567.
2. Information Week, August 1999.
3. CSI/FBI Computer Crime and Security Survey, Winter 1999.
4. SecureLogix, "Problem", http://www.securelogix.com/problem.htm.
5. PC Magazine, October 1999.