

Top 10 Dial-In Security Mistakes

Heather Smartt

INTRODUCTION

A constant barrage of information about hackers bombards companies. There are hundreds, if not thousands of books about computer security, network security, and operating system security. There are a number of security products on the market — some keep people out, some keep people in, some track people down. All of the Big Five accounting firms and many small, boutique firms are offering security consulting services. It is fair to say that computer security is a hot topic in society.

As an information security consultant for one of the Big Five accounting firms, the author has participated in many penetration projects. Although every client is different, certain findings are uncovered in nearly all dial-in reviews. If an organization would take some time to fix the most common mistakes, it would go a long way toward preventing hackers. Here are the most common security risks that are found during a dial-in review.

TOP TEN

1. Data lines are found in same prefix as voice lines
2. Enticement information — “Welcome to ...”
3. Direct dial-in systems (i.e., no authentication at all)
4. Lack of controls on default accounts

5. Accounts with easily guessed passwords
6. Help files
7. pcANYWHERE
8. Lack of monitoring
9. Trust
10. Unlimited access attempts

TOP TEN EXPLAINED

1. Data Lines In Same Prefix As Voice Lines

In a dial-in attack, the first thing the hacker has to do is find the modem lines. How does a hacker decide which numbers to dial? First, the hacker looks up the company's main number in the *Yellow Pages* (on the Internet, of course), along with information on the company's other main locations. Next, a hacker may call the various branches to get the voice numbers. The final step is to set up a war-dialer, such as Toneloc and to dial these numbers. If the company's data lines are in the same prefix as the voice lines, the hacker has hit paydirt. After all the numbers in the range are dialed, the hacker has a list of every number that responded with a carrier tone (i.e., modem lines) and a whole list of targets to attack.

Recommendation. Modem lines should not share the same prefix as voice or fax lines. In addition, these numbers should

HEATHER SMARTT is a Manager in a Big Five accounting firm's security consulting group and is based out of Dallas, Texas.

Periodically review the systems to ensure that these defaults still are secure, especially after operating system upgrades and application installations.

be unpublished and distributed only as necessary.

2. Enticement Information — “Welcome To ...”

What could be more reassuring to a hacker (or industrial spy) than a banner that says, “Welcome to the Company under Attack!” This banner not only assures the hacker that the system just dialed actually belongs to the targeted company, but also it says, “Welcome.” Legally, this could be interpreted as an invitation to enter and use the system, and the company under attack could be held liable for any further damages a hacker causes to interconnected networks.

Recommendation. System banners should never include enticement information, such as company name, operating system type, and version. Instead, banners prominently should display a warning such as “Unauthorized use strictly prohibited and will be prosecuted to the fullest extent of the law.”

3. Direct Dial-In Systems (i.e., No Authentication At All)

One of the most serious security mistakes encountered is that of systems that allow one to access the system directly, with no authentication whatsoever. The author has accessed numerous pcANYWHERE connections, DEC terminal servers, Cisco routers, PBX systems, environmental control systems, and a Tandem mainframe in this manner. This access has allowed her to run applications, steal password files, map out the network, perform denial-of-service attacks, launch additional attacks, and actually physically damage heat-sensitive systems. Although she did not actually turn up the heat, she could have and caused great physical damage to these sys-

tems as several of these environmental control systems controlled the heating and cooling of the mainframes. By accessing many of these direct dial-in systems, the outside hacker becomes an insider.

Recommendation. Ensure that systems are password-protected and that controls are in place to terminate the connection when a user hangs up the modem line. For additional insurance, regularly scan the network with a war-dialer and perform a mock penetration on each modem line dialed to test password controls.

4. Lack Of Controls On Default Accounts

With all the publicity surrounding hacking and hackers, an alarming number of default accounts still have no passwords or only default passwords. There are sites all over the Internet that contain lists of well-known accounts and the corresponding default password. When conducting a penetration study, the author dials each number once to look for direct dial-in systems and to obtain system identification information. This allows her to identify and hack into the most vulnerable systems first and to classify the modem lines by their underlying operating systems. Next she attempts to break into well-known operating systems (i.e., UNIX, NT, VAX/VMS, Cisco routers) with a list of default user IDs and passwords. She is able to break into a least one system in this manner at least 90 percent of the time. With the exception of the direct dial-in systems, this is the fastest way into a company’s network.

Recommendation. Remove, rename, or lock all unused default accounts. If the account must be used, change the password. Periodically review the systems to ensure that these defaults still are secure,

especially after operating system upgrades and application installations.

5. Accounts With Easily Guessed Passwords

After trying the list of all known default accounts, the author starts doing some educated guessing. If lucky enough to obtain a password file, she runs it through a password cracker. Normally, once she has the password file, she has access to systems across the entire network.

Even without the password file, there is still a pretty strong chance of getting in. The author can use the enticement information that she has gathered along the way. She tries the account name as the password and the account name with no password. If she has a list of system names, she tries each of these as an ID and password. A list of potential passwords is compiled based on the company and location. For example, she tries the company's name, the company's nickname, the month, major sports teams, and so forth. She also tries common account and passwords such as training/training and demo/demo. Invariably, she guessed correctly and obtains access to the internal network. With the need for so many passwords today, users generally have passwords that are easy for them to compose and remember. This makes the hacker's job an easy one.

Recommendation. Users need to be educated on what is and is not a good password and why it is important to be creative. In addition, system administrators should routinely run password crackers. They should notify and counsel any user whose password was cracked.

6. Help Files

Online help is a wonderful thing — especially on unfamiliar systems. For a hacker, it is even better when the system helps one gain access before authenticating.

VAX/VMS systems generally provide a help feature for users when they reach the

LOCAL> prompt. Generally, a user does not have to authenticate to reach this level. That means the user may have full access to the help function and can discover all sorts of interesting commands to try. Because of this user-friendly help feature, the LOCAL> prompt often provides an excellent jump-off point for further penetration. Targets can be obtained from the Show node and Show hosts commands and connections can be attempted through the connect command.

Recommendation. Restrict help files to authenticated users only. If users are fairly proficient in the use of the system, completely disable the help feature. In this case, ignorance may be bliss.

7. pcANYWHERE

pcANYWHERE is a nice application that can be fairly secure. In the author's experience though, it is often unprotected. She has nicknamed it pcEVERYWHERE and estimates that three out of five pcANYWHERE prompts are unprotected (i.e., no user ID and no password). Often, users do not even ask permission to use remote access software — they just buy it and load it. They reason that no one would ever find their modem number. If it is an unlisted number, why should they use a password? Fortunately for the hackers, and the author, Toneloc (a freely available wardialer) finds the number quite easily in the range of telephone numbers it dials.

When accessing an unprotected pcANYWHERE host, the author becomes an internal user. Screen savers with passwords that might stop or slow her down rarely are used. So when she dials in, she has full access to the user's desktop. Even worse are the users who do not log out of the network before going home and leave the applications they have been working on totally accessible. She has been able to send and read e-mail, copy confidential data, obtain passwords, download corporate phone directories, and launch further network attacks from these user's desktops.

Recommendation. Implement strict policy on and enforcement of remote access software use, such as pcANYWHERE. Ensure that users are aware of the potential security risks and ensure that IDs and strong passwords protect all accounts.

8. Lack of Monitoring

Monitoring is an important part of information security, yet it often is overlooked. Many administrators say they are just too busy to review stacks of logs that probably contain nothing extraordinary. However, regular review of the logs could alert a system administrator that an attack is in progress or that a penetration has occurred. During a dial-in review, the author is generally quite noticeable because she normally does not try to hide her tracks. She will make repeated attempts to guess passwords and trigger several auditable events. The purpose is to test the administrator to find out if she is being watched. She rarely gets caught! Imagine what could happen if a hacker did take care to hide their tracks — they could have unauthorized access for years before being caught accidentally.

Recommendation. Review logs regularly — at least once a week and preferably every day. Commercially available security auditing tools help make the logs more manageable. A security auditing tool will log high-risk events such as failed log in attempts and generate reports listing all questionable activities. Finally, be certain to log all superuser log ins and log outs.

9. Trust

Several operating systems, most notably UNIX, have an inherent remote trust feature. This feature allows an authenticated user to log on remotely, without further authentication, to any system that trusts their current system. The ramifications of this feature are staggering. Once the author broke into a UNIX system through

the use of a default user ID and password. Due to the trust relationships between the UNIX systems on the network, she was able to access remotely 936 UNIX hosts! To make matters worse, her initial account was a superuser-equivalent account, so she had in effect root access to 936 hosts.

Recommendation. Trust relationships generally are configured for convenience. It is best to remove all trust relationships and force users to authenticate themselves each time they log into a host. There are justifiable business needs for trust. If this is the case, security controls should be tightened wherever possible. In UNIX, for example, `.rhost` files should be readable only to the user and the `hosts.equiv` file should be readable only by root.

10. Unlimited Access Attempts

Allowing unlimited access attempts on a system is begging for an automated password guesser to be set up. The author has a program that will dial a number and then guess passwords until the remote system hangs up the connection. The program then will redial the number and continue guessing. By not limiting the number of access attempts per account, the chances of guessing the correct password is increased greatly.

Recommendation. Limit the number of chances a user has to correctly input their password. After this number has been exceeded, lock the account until the system administrator can intervene.

CONCLUSION

A security program is like a dam. Once there is a leak, the hole just gets bigger and bigger. Each security administrator must do his best to ensure that there are no leaks. It is a daunting job. These recommendations may not stop a dedicated hacker from breaking into a network, but they will deter the casual hacker. ■