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

The Default Password Threat

Hackers often do not use complex and technically intricate methods to penetrate most systems. A common technique used in system break-ins is the default password provided with built-in accounts. The built in passwords your vendor designed into your system, if not controlled and managed, can defeat any system. These built in passwords are not secret. Books, magazines, the Internet, vendor handbooks, and auditor guides all have data or tips on default passwords. This easy to fix, but difficult to maintain, vulnerability is a serious problem on all platforms, from personal computers to large mainframes.

The SANS Institute has recognized default passwords has one of its "Ten Most Critical Internet Security Threats.[1]" The document states that "some systems come with "demo" or "guest" accounts with no passwords or with widely-known default passwords. Service workers often leave maintenance accounts with no passwords, and some database management systems install administration accounts with default passwords.[2]"

A basic computer security commandment is to keep all passwords secret. Good computer security practices require that passwords be safeguarded. Computer security officers take this duty seriously. For example, users may receive initial passwords in sealed envelopes. Initial passwords may expire after the first use. Also, computer companies take steps to shield passwords. Most security systems, for instance, store passwords in an encrypted format and have settings to expire passwords after a set amount of time. Computer security experts worry about problems such as passwords being sent unencrypted through networks or of complex techniques used to steal passwords.

Do hackers always use complex techniques to "break into" a system? In many cases, no. Often, they use the easiest cracking technique available, default passwords. Default, or built-in, passwords are the hack you purchase along with a new operating system or software package.

What Are Default Passwords

Default passwords are those userid/password pairs that are built into an operating system, database or software. The usually come preinstalled with a standard, known userid and password. This userid and password is the same for all copies of a version of software. The userid has a standard name and the password is initially set to the same word or character string.

Default userids and passwords are everywhere. Probably the most common default userid/password is the Unix userid root. All Unix versions use the root userid as the initial userid during setup. However, all platforms, from including mainframes, midrange systems, desktop computers, network operating systems, and specialized devices such as routers have built-in userids and default passwords. IBM's Resource Access Control Facility (RACF) mainframe security software, the midrange Vax and AS-400 platforms, Windows NT, Novell, and Cisco routers all use built-in userids. Database systems are big

© SANS Institute 2000 - 2005 Author retains full rights.

users of default passwords. Database management systems on all platforms, including IDMS, Oracle, and Microsoft SQL, use "native" defaults. Software packages, such as games, use default passwords. Finally, the BIOS computer chips in many PCs have built in passwords.

Uses of Default Passwords

Built-in userids and passwords have a number of uses. Operating systems, databases and applications software use built-in userids and passwords for initial installations or for upgrades. Defaults are often essential to the installation process. Vendors use built-in accounts for customer support. These logonids may be customized for specialized uses. Vendors maintain and troubleshoot problems with pre-configured default accounts. Sometimes, vendor support personnel will resist any suggestion to take the defaults away. A properly configured demonstration default account will permit a potential customer to try out software before purchase or permit a user to learn the software at his own pace using planned lessons. Defaults are used for Internet communications of file retrieval. The ANONYMOUS account is often used to allow users to retrieve documents or files on the Internet. Many vendors design defaults to segregate users from other parts of the application. Some ERP systems isolate the user from the database by having a default perform system accesses. Finally, default accounts and passwords are used by applications programs to communicate with their databases. Enterprise Resource Planning (ERP) software packages commonly use built-in accounts and passwords to "talk" to their databases. This simplifies managing access to the database in these complex systems. Finally, defaults simplify programming by allowing userids and passwords to be "hardcoded" into the programs

A Security Problem

If built-in userids and passwords are so useful, why are they a serious security problem? Default userids and passwords pose a serious security problem because they:

- Are found on many widely used operating systems and databases used commercially
- May carry high level system or Database Administrator (DBA) privileges
- Often are tightly integrated into operations or present on mission critical systems
- Frequently are left unsecured by being set at the default
- Mask the audit trail, making monitoring difficult
- Have passwords that are widely known to many "users."
- "Hardcoded " defaults can be easily identified
- Can be easily exploited; even by a novice.

The most important risk with default passwords is that the information can easily be discovered by just about anyone. This information is available in vendor publications, books, on the Internet. This, coupled with ease of use, is what makes this a serious security problem.

© SANS Institute 2000 - 2005 Author retains full rights.

Sources of Default Password Information

Despite of the serious security risk that this security loophole poses, this intelligence is easy to acquire. The most useful sources are vendor manuals, computer books, a number of Internet sources, and on-line vendor documentation.

Vendor Manuals

Vendor sometimes publish default passwords in their documentation. For example, default password for a common highly privileged account for the VMS operating system was published in older Digital Equipment Corporation (DEC) documentation.[3] Although DEC removed this reference from its manuals, the password for this account remained the same and was valid for years later.

Vendors still publish default passwords, but now on the Internet. On-line system documentation is the latest iteration of vendor published default password information. Many manufacturers, systems integrators, and other vendors post documentation on their Internet web pages to support customers. The IBM Corporation, for example, publishes the default password to its all powerful IBMUSER account in for its RACF security software[4].

Computer Books

Computer books published to supplement vendor documentation are a second source of default information. These books can be found in any large bookstore, libraries, and on Internet bookseller sites. These books are particularly useful for uncovering defaults for personal computers, client server systems and databases, and network operating systems. The best sections to read are those on installation and security. Books were my source for default userids passwords on SAP R/3[5] and the Sybase database system[6].

The Internet

A rich source of intelligence of default password information is the Internet. Internet default password information can be found not only in online documentation, but also on the World Wide Web, in newsgroup discussions, and on hacker sites. One thing to remember about a World Wide Web posting, is that it is "world wide." A web site shares its information with about 150 million of its closest confidants. Anything posted on the Internet must be assumed to be known by your worst adversaries.

A large number of web pages contain default password data. A simple search on the Google search engine turned up 822 references on "default passwords.[7]" As with many Internet searches, many pages contained worthless information. However, this simple search turned up default passwords for Cisco routers and switches,[8] PC Bios[9], and the Netscape Enterprise Server[10].

© SANS Institute 2000 - 2005 Author retains full rights.

A more focused approach uses newsgroups to uncover defaults. Newsgroups exist for all widely used operating systems and security packages Newsgroups assist subscribers in solving problems. Sometimes users need to know the default password of a built-in userid. These people then post a query on a newsgroup, hoping for a response. Usually, they receive it. Newsgroups are productive. From newsgroups, I learned the default passwords for powerful accounts for the commonly used Oracle database[11] and the AS-400 operating system[12].

Any research on default passwords would not be complete without a visit to hacker sites. Many of these sites are open to all with the information openly available. One of the most common guides found on the Internet is A Novice's Guide to Hacking[13]. This handbook has good, but dated, information. Another is the newsgroup alt.2600 FAQ (Frequently Asked Questions). This is posted on the newsgroup alt.2600 and is updated frequently. The FAQ has good information on built-in accounts and default passwords and is updated frequently. Updated compilations of the alt.2600 FAQ can be found the World Wide Web (WWW)[14]. Both provide an excellent overview of hacking and its philosophy.

Information Systems Training

A lesser known, but important, source of information on built-in accounts and default passwords are publications and training courses for Information Systems (IS) auditors. A current trend in IS auditing is to perform "penetration testing." Penetration testing is a surreptitious attempt to access computer resources, often without the auditee's knowledge. One of the easiest ways to penetrate a computer system is to try default accounts and passwords to attempt access. In my experience as an IS auditor, many times default passwords work.

Because of this audit requirement, classes and publications designed for the IS auditor cover this topic extensively. Books written for IS auditors often cover platforms used by large organizations that are not in vogue with hackers. A good example is the Integrated Data Management System or IDMS. An IS auditing manual published default data for a powerful logonid in IDMS[15], a database still used by large organizations for production and financial data.

Default Passwords - Easily Exploited

Default passwords pose a major security risk. Hundreds of millions of users have access to this information on the Internet, in computer books and vendor manuals, and other areas. Default passwords are easy to use. Once a user identifies a computer platform (The alt.2600 FAQ will help you), all an unauthorized user must do is enter the userid and its default password. Many, like the Unix root account, are extremely powerful. Unauthorized accesses are difficult to audit, because they obscure the audit trail. If defaults are not specifically assigned to a user, accountability is lost. It would be impossible to determine who is actually using them. Finally, most platforms have some

© SANS Institute 2000 - 2005 Author retains full rights.

defaults. Default passwords are a security threat no information systems manager can ignore.

---

[1]The SANS Institute, "How To Eliminate The Ten Most Critical Internet Security Threats, The Experts' Consensus," Version 1.30, November 17, 2000, URL: http://www.sans.org/topten.htm (November 29, 2000).
[2] Ibid.
[3] Digital Equipment Co. VAX 11/780 Software Installation Guide, (December 1982), p. 3-1
[4] IBM Corporation. "Logging On as IBMUSER and Checking Initial Conditions." Resource Access Control Facility, Security Administrator's Guide, Version 2 Release 2. Second Edition, September 1995. URL: http://publibfp.boulder.ibm.com:80/cgi-bin/bookmgr/BOOKS/ICHMSA01/10.3.1 (November 30, 2000).
[5] Will, Lianne, SAP R/3 System Administration, (Berkeley, CA 1999), p. 12.
[6] Anderson, G. and Berson, A., Sybase and Client Server Computing, 2nd ed. (New York, 1997), p. 573.
[7] Search conducted at http://www.google.com on November 30, 2000.
[8] Jenkins, Joe, "Default Login / Pass Listing." Nerdnet. URL: http://www.nerdnet.com/security/index.php (November 30, 2000).
[9] Knight Eric, "Default Password List." Version 3.06. September 15, 2000. URL: http://www.securityparadigm.com/dad.htm (November 30, 2000).
[10] Howard, James, "Recovering a Lost Admin Password on Netscape Enterprise Server and FastTrack Server." URL: http://developer.iplanet.com/viewsource/howard_lostpwd/howard_lostpwd.html (November 30, 2000).
[11] Buttà, Mario, "Windows NT Oracle - default login & password." Comp.databases.oracle.misc. April 12, 2000. URL: http://x65.deja.com/[ST_rn=ps]/getdoc.xp?AN=610206477&CONTEXT=975596244.1997406214&hitnum=21. November 29, 2000.
[12] prog@linux.org (WHiTEy), "Re: Need help crackin routers password!!!!!!." Alt.hacker, January 17, 2000. URL: http://www.deja.com/getdoc.xp?AN=573710758&fmt=text, November 29, 2000.
[13] The Mentor, Legion of Doom/Legion of Hackers, "A Novice's Guide to Hacking." 1989 edition. December, 1988. URL: http://www.undergroundnews.com/kbase/underground/hacking/guide.htm (November 30,2000).
[14] Voyager, "alt.2600/#Hack FAQ" Revision .014, May, 29,2000 URL: http://www.landfield.com/faqs/alt-2600/faq/ (November 30,2000).
[15] Hutchinson, Sydney, A Guide to the Audit/Review of CA-IDMS/R Security, (Carol Stream, IL, 1990), p. 19.

Walter P. Opaska

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

© SANS Institute 2000 - 2005 Author retains full rights.