Network Working Group
Request for Comments: 2179
Category: Informational

A. Gwinn
Networld+Interop NOC Team

July 1997

Network Security For Trade Shows

Status of this Memo

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract

This document is designed to assist vendors and other participants in trade shows, such as Networld+Interop, in designing effective protection against network and system attacks by unauthorized individuals. Generally, it has been observed that many system administrators and trade show coordinators tend to overlook the importance of system security at trade shows. In fact, systems at trade shows are at least as prone to attack as office-based platforms. Trade show systems should be treated as seriously as an office computer. A breach of security of a trade show system can render -- and has rendered -- an exhibitor’s demonstrations inoperable -- sometimes for the entire event!

This document is not intended to replace the multitudes of comprehensive books on the subject of Internet security. Rather, its purpose is to provide a checklist-style collection of frequently overlooked, simple ways to minimize the chance of a costly attack. We encourage exhibitors to pay special attention to this document and share it with all associated representatives.

Physical Security

Before addressing technical security issues, one of the most frequently underrated and overlooked security breaches is the simple low-tech attack. The common victim is the one who leaves a console logged in, perhaps as root, and leaves the system. Other times, an anonymous "helpful soul" might ask for a password in order to assist the user in "identifying a problem." This type of method allows an intruder, especially one logged in as "root", access to system files.

Tips:

* Educate sales and support staff regarding system logins, especially "root" or other privileged accounts.
* Identify individuals who are not using exhibit systems for their intended purpose, especially non-booth personnel.
* Request identification from anyone wishing to access systems for maintenance purposes unless their identities are known.

System Security

This section discusses technical security procedures for workstations on the vendor network. Although specifics tend to be for Unix systems, general procedures apply to all platforms.

Password Security

Lack of passwords or easy to guess passwords are a relatively low-tech door into systems, but are responsible for a significant number of breakins. Good passwords are a cornerstone of system security.

By default, PC operating systems like Windows 95 and MacOS do not provide adequate password security. The Windows login password provides no security (hitting the "ESC" key allows the user to bypass password entry). Password security for these machines is possible, but is beyond the scope of this document.

Tips:

* Check /etc/passwd on Unix systems and the user administration application on other systems for lack of passwords. Some vendors ship systems with null passwords, in some cases even for privileged accounts.
* Change passwords, especially system and root passwords.
* Mix case, numbers and punctuation, especially on privileged accounts.
* Change system passwords on a regular basis.
* Do not use passwords relating to the event, the company, or products being displayed. Systems personnel at Networld+Interop, when asked to assist booth personnel, often guess even root passwords!

Extra Privileged Accounts

Some system vendors have been known to ship systems with multiple privileged accounts (for example, Unix systems with accounts that have root privileges [UID=0]). Some vendors may include a separate system administration account that places a user in a specific administrative program. Each additional privileged account presents yet another opportunity for abuse.

Generally, if a Unix system does not need additional root accounts, these can be disabled by placing "*" in the password field of /etc/passwd, or by using the administrative tool when a system employees enhanced security. Verify all systems for extra privileged accounts and either disable them or change their password as appropriate.

Make certain that privileged accounts are inaccessible from anywhere other than the system console. Frequently systems rely on files such as /etc/securettys for a list of "secure" terminals. As a general rule, unless a terminal is in this file, a root login is not possible. Specific use of this feature should be covered in the system's documentation files.

Tips:

* Check /etc/passwd on Unix systems and the user administration application on other systems for additional privileged accounts.
* Disable remote login for privileged accounts.
* Disable any unnecessary privileged accounts.
* Limit logins from root accounts to "secure" terminals or the system console.

Use of Authentication Tokens

Authentication tokens such as SecureID, Cryptocard, DES Gold and others, provide a method of producing "one-time" passwords. The principle advantage in a trade-show environment is to render worthless, packets captured by sniffers on the network. It should be treated as fact, that there are many packet sniffers and other administration tools constantly (legitimately) watching the network--especially at a large network-oriented trade show. Typed passwords, by default, are sent clear text across the network, allowing others to view them. Authentication tokens provide a password that is only valid for that one instance, and are useless after that. A logical extension of the use of authentication tokens would be to use them for "trips home" (from the show network to a home site) to minimize the chance of off-site security problems.

An alternative to these tokens is the secure shell ("ssh") protocol which provides an encrypted connection between clients and servers. This connection can carry both login traffic and arbitrary port-to-port communication, and is a powerful tool for securing an in-booth network and communications to and from remote systems.

Tips:

* Contact vendors of authentication tokens/cards for further information as to how to integrate into specific environments, or on to specific platforms.
* The public-domain utility "cryptosu" (csu), when used with a Cryptocard, provides a replacement for Unix's "su" command, employing a challenge/response style of authentication for root access.
* Explore the use of ssh clients and servers.

Anonymous FTP

Anonymous FTP accounts can easily turn into a security hole. Disable this service if not specifically needed. In the event that anonymous FTP is to be used, the following tips may help secure it.

* When a user logs in as "anonymous", they should be locked into a specific directory tree. Be sure that FTPd properly chroots to the appropriate directory. A "cd /" should put an anonymous user at the top of the "public" tree, and not the system's root directory.
* Some systems may allow symbolic links (or "shortcuts") to take a user outside the allowed tree. Verify all links inside the anonymous FTP hierarchy.
* Make sure that ftp's root directory is "owned" by someone other than the 'ftp' account. Typically, it should be owned by "root".
* Do not use a world-writable incoming directory unless absolutely necessary. Many sites use these as a way for users to transfer files into the site. This can, and frequently does, turn into an archive for stolen software (referred to by the pirate community as "warez").
* Removing read permissions from the directory permissions (chmod 733 on Unix systems) prohibits an anonymous user from being able to list the contents of a directory. Files can be deposited as usual, but not retrieved unless the user knows the exact name of the file.

Network File Sharing

Writable file shares without some form of security are invitations to destruction of information and demonstrations. Whether using NFS on Unix systems, or PC sharing facilities like CIFS, AppleShare, or NetWare, close attention should be paid to security of the files

exported. Keep in mind that one's competition frequently shares the same network at a trade show! Security for both read and write access should be employed and each access point examined.

Exporting a writable NFS filesystem to the world grants anyone the ability to read and write any file in the exported mount point. If this is done, for example, with a system directory such as "/" or "/etc", it is a simple matter to edit password files to create one-self access to a system. Therefore, /etc/exports should be closely examined to be certain that nothing of a sensitive nature is exported to anyone but another trusted host. Anything exported to the general public should be exported "read-only", and verified for the information that is available via the file shares.

Tips:

* Do not provide file sharing space unless needed.
* Verify where exported information will be "visible".
* Do not maintain any writable shares unless absolutely necessary!

Trusted Hosts

Trusted host entries are a method for allowing other hosts "equivalent" security access to another host computer. Some vendors ship systems with open trusted host files. Make certain that this issue is addressed.

Tips:

* On Unix systems, check for a '+' entry (all systems trusted) in /etc/hosts.equiv and all ".rhosts" files (there may be multiple .rhosts files) and remove it.
* Check for an "xhost +" entry in the "...X11/xdm/Xsession" file. Most often, an "xhost" entry will appear with a pathname such as "/usr/local/lib/xhost +". Remove this.

SetUID and SetGID binaries (Unix systems)

On Unix systems, the "suid" bit on a system executable program allows the program to execute as the owner. A program that is setUID to "root" will allow the program to execute with root privileges. There are multiple legitimate reasons for a program to have root privileges, and many do. However, it may be unusual to have suid programs in individual user directories or other non-system places. A scan of the filesystems can turn up any program with its suid or sgid bit set. Before disabling any programs, check the legitimacy of the files.

Tips:

* "find / -user root -perm -4000 -print" will find any occurrence of a setuid file anywhere in the system, including those on NFS mounted partitions.
* "find / -group kmem -perm -2000 -print" will do the same for kmem group permissions.

System Directory Ownership and Write Permissions

Check ownership of all system directories and permissions needed to write or modify files. There is no simple way to do this on PC operating systems like Windows NT without simply checking all files and directories or using a version of "ls" that will list ACLs.

On Unix systems, a directory with permissions such as "drwxrwxrwx" (such as /tmp) is world-writable and anyone can create or modify files in such area. Pay special attention to "/" and "/etc". These should be owned by some system account-not by an individual user. When in doubt, contact the vendor of the system software for confirmation of the appropriate directory or file permissions.

Network Services

Any servers not needed should be disabled. The notorious "R services" (rexec, rsh, and rlogin) are particularly prone to security problems and should be disabled unless specifically needed. Pay particular attention to trusted hosts files, and be aware of the risk of IP spoofing attacks from machines "pretending" to be trusted hosts.

Tips:

* On Unix systems, comment out "R services" (rexec, rsh, rlogin) in /etc/inetd.conf.
* Check for other unknown or unneeded services.

Trivial File Transfer Protocol (TFTP)

TFTP can be an easy way for an intruder to access system files. It is good general practice to disable TFTP. If TFTP is needed, verify that only files targeted for export are accessible. A simple way to check security is to attempt to tftp files such as /etc/passwd or /etc/motd to check accessiblity of system files.

TCP Connection Monitoring

Public domain software (TCP Wrappers or "tcpd" for Unix systems) allow restriction and monitoring of TCP connections on a host by host basis. Systems can be configured to notify an administrator and syslog when any unauthorized party attempts to access the host. This software is available from:

* ftp://info.cert.org/pub/tools/tcp_wrappers/

BIND (Berkeley Internet Name Daemon)

Earlier versions of BIND have been prone to various attacks. If a host is going to be acting as DNS, use the latest version of BIND. It is available at:

* ftp://ftp.isc.org/isc/bind

Sendmail and Mailer Security

A great number of previous versions of Sendmail have known security holes. Check installed sendmail for the most recent version. Alternatively, consult the operating system vendor to get the most recent release for the platform.

Web Server Scripting Security

All Web server scripts and binaries should be checked (especially the "...httpd/cgi-bin" directory) for those that allow shell commands to be executed. Many attacks in recent months have focused on the use of utilities such as "phf" for accessing /etc/passwd on a target system. Remove any script that is not needed in the course of operation of a web server.

Other Suggestions

* Check with the vendor of the operating system for known security issues. Make certain that all systems have the latest version of software--especially security patches to fix specific problems.

* Examine log files on the host frequently. On Unix systems, the "last" command will furnish information on recent logins and where they came from. The "syslogs" or "Event Viewer" will contain more specific information on system events.

* Web server logfiles (...httpd/log/access_log and ...httpd/log/error_log) will contain information on who has been accessing a WWW server, what has been accessed, and what has failed.

* Good backups are the best defense against system damage. Perform backups before placing a system on the trade show network then continue backups throughout the show and again following the event. A final backup set is useful to examine for possible attempts at (or successful) penetrations of system security.

General Network Security

As would be expected at network trade shows (large or otherwise), there are many entities running packet sniffers. Most are exhibitors who have a legitimate need to run them during the course of product demonstrations. However, be aware that there are many "listening ears" on network segments--any of whom can "hear" or "see" information as it crosses the net. Particularly prone to eavesdropping are telnet sessions. A good rule of thumb is to assume that "when you type your password, the only one that doesn't see it is you!"

It is a good practice to not log in (or "su") to an account with privileges across the network if at all possible. As mentioned previously, authentication tokens and ssh are a simple way to add security to system account access.

Packet Filtering

Many routers support basic packet filtering. If a router can be deployed between the local network and the show's network, general basic packet filtering should be employed. Below is a good "general" packet filter approach. The approach itself is ordered into categories:

* General global denials/acceptance.
* Specific global service denials.
* Specific service acceptance.
* Final denial of all other TCP/UDP services.

Based on the theory of denying everything that you don't know is acceptable traffic, a good approach to a filter ruleset, in order of execution priority, might be:

General Global Denials/Acceptance

1 Filter spoofed source addresses by interface. Match source addresses to routing information available for the interface. Discard packets with source addresses arriving on one interface (from the "outside" for example) claiming a source address on another interface (the "inside").
2 Filter all source routed packets unless source routing is specifically needed.
3 Allow outbound connections from "inside" hosts.
4 Allow established TCP connections (protocol field contains 6 and the TCP flags field either contains ACK or does NOT contain SYN bit). Only filter requests for 'new' connections.
5 Filter 'new' connections with source port of 25. Prevents people from pretending to be a remote mail server.
6 Filter loopback address (source address 127.0.0.1). Prevents packets from a misconfigured DNS resolver.

Specific Global Service Denials

1 Specifically block all "R-command" ports (destination ports 512-515).
2 Block telnet (destination port 23) from any host not requiring telnet access from the outside. (If you use ssh, you can block it from all hosts!)
3 Add specific filters to deny other specific protocols to the network, as needed.

Specific Host/Service Acceptance

1 Add specific access to specific "public" hosts' services (unsecure FTP or WWW servers).
2 Allow SMTP (source and destination port 25) for electronic mail to the mail server(s).
3 Allow inbound FTP connections (source port 20) to the FTP server(s).
4 Allow DNS (source and destination port 53, UDP & TCP) to name servers. If zone transfers are not needed, block the TCP ports.
5 Allow RIP packets in (source and destination port 520, UDP), if appropriate.
6 Add specific filters to allow other desired specific protocols or to open certain ports to specific machines.

Final Service Denial

1 Deny all other UDP and TCP services not allowed by the previous filters.

Author's Address

R. Allen Gwinn, Jr.
Associate Director, Computing
Business Information Center
Southern Methodist University
Dallas, TX 75275

Phone: 214/768-3186
EMail: allen@mail.cox.smu.edu or allen@radio.net

Contributing Writer

Stephen S. Hultquist
President
Worldwide Solutions, Inc.
4450 Arapahoe Ave., Suite 100
Boulder, CO 80303

Phone: +1.303.581.0800
EMail: ssh@wwsi.com