Security Audit Checklist

This document discusses methods for performing a thorough and effective security audit on a computer system or network. It will not specifically discuss the technical details of prevention on specific computer systems, but will rather provide a general checklist for examining the security on a computer system.

This document is not an authoritative or comprehensive one; you should check with the information management policy of your particular institution for steps to follow to secure your system. The author of this document shall not be liable for any damage, direct or indirect, incurred in the following of this advice. If you have experienced a security breach, you should contact an experienced security professional to evaluate recovery options.

Prepared by: Assign IT Ltd

Unit 17, Brick Knoll Park

Ashley Road Industrial Estate

St. Albans

Hertfordshire

AL1 5UG

Contents

Physical Security

Physical security is arguably one of the most important part of maintaining the security of a computer system, and is often overlooked by careless system administrators who assume their occasional proximity to a system is enough protection. This may be sufficient for some systems, but in most cases, there are more factors to be considered before a system can be called physically safe and secure.

Is the system located on a sturdy, stable surface as close to the ground as possible?

Is the system safe from excessive sunlight, wind, dust, water, or extreme hot/cold temperatures?

Is this system located in a monitored, isolated area that sees little human traffic?

Is the room/building in which the system is located secured by lock and alarm system to which only a few trusted personnel have access? Are these locks and alarms locked and armed during off-hours?

Is the terminal of the system secured to prevent someone from casually walking up to the system and using it (even if just for a few seconds)? Are all users logged out from the terminal?

Are the power and reset switches protected or disabled?

Are any input devices to the system secured/turned off: are all removable disk drives locked/secured? Are the parallel/serial/infrared/USB/SCSI ports secured or removed? Are any attached hard drives physically locked down to the system?

Network Security

Network security is the next important part of maintaining a system security. While good physical security can go a long way, if you operate your system in a networked/multi-user environment, the system is many times more susceptible to outside attacks than a standalone system. Network security is also harder to evaluate because it requires a thorough understanding of the various components and layers of your system and all the external services that interact with your system.

Physical network: is the network connection a secure "pipe" with no danger of unauthorized rewiring? Do only authorized personnel have physical access to the physical network to which the system is attached? Do you know and trust all of the various points where your physical network connection is managed/administered by another person or entity?

Are the other systems on the same network physically and electronically secure? If your system is reasonably secure but another system on the network is not, your system's vulnerability is increased greatly.

Approved Network Traffic

Do you know the names, functionality, vendor, and nature of the software on your system that participates in any network activity? Have you checked all the vendors for security patches, and do you regularly receive security updates about patches/vulnerabilities to the software you use in a networked environment?

Have you thoroughly tested any and all services that interact with the network to insure that they do not, by default, provide any unauthorized users with useful security information that could be used to attack the system?

Do you effectively limit your users` abilities to make sensitive information about the system available over the network?

Do you only allow trusted users shell/command line access to your system?

Are you aware of any security holes created by certain software packages interacting with each other?

Do you keep sufficient logs of all approved network activity?

Are you aware of all the software that should be interacting with the network, the port numbers they use, the size and location of their binaries, etc.?

Do user accounts that are accessible over the network regularly have their passwords changed?

Do you encrypt sensitive data that is transferred over the network?

Unapproved Network Traffic

Do you regularly check for repeated unauthorized attempts to connect to your system over a network? Do you keep sufficient logs of all network activity related to your system?

Do you regularly check for unauthorized programs running on your system that could potentially allow a user to connect over the network?

Do you monitor for excessive or unusual network activity that comes to your system?

Protocol and Service

The physical and network layers of your system, the next category of evaluation is perhaps one of the largest; computers are made to compute, and depending the purpose of your system, it will be running many different kinds of software and programs at any point in time. It is likely in most cases that, because all of the software was written by different people with different understandings of security (and because there are always people who know more about security), at least one of those programs has some sort of security hole that could be exploited.

While it is generally safe to assume that software that comes pre-installed on a new system is reasonably secure, you should always check with software vendors for security patches, release notes, and other relevant information to your particular configuration.

For any software that you install onto a new system, make sure you are fully aware of the credentials of the vendor, any security patches, existing exploits, and release notes that exist. You should make it a habit to check in with vendors every month or so for new releases that may have security fixes. It's also a good idea to subscribe to mailing lists for your software, or general mailing lists that would announce security holes early.

Misconfiguration is probably the most common cause of someone exploiting a security hole. Most software is written to be reasonably secure, but even the most secure software can be used for

unintended purposes if it is poorly configured. Always follow the vendor's instructions for installing software, and always take notes on any problems you encounter in the configuration process. If a piece of software requires special privileges to be installed or run (e.g. running *setuid* on a UNIX system), make sure you understand the full implications of having it do so, and any side-effects created in the process. Test your configuration of the software thoroughly; try to break it, try to hack into it, and see if others can do the same.

If a program accesses sensitive data, make sure that it can only be executed by authorized users, and make sure that any logs or temporary information is stored in a safe place and promptly disposed of; people can do amazing things with the simple information found in a system log file.

If a piece of software runs as a *daemon* (i.e. it is constantly running and responds to requests from users locally or over the network), make sure it properly handles buffer overflows, denial of service attacks, and general heavy system load. It's generally a good idea to have as few services as possible running as daemons, as they allow continuous and typically unmonitored access to your system.

Be aware of all the services that are supposed to be running on your system, the typical amount of resources (e.g. CPU time, memory, disk space) that they take up. Check for unidentifiable daemons or software, or programs that are unusual in their resource consumption. Remember that most security breaches occur using the existing configuration of a system rather than installing a new one; unless you're careful, an intruder can manipulate the system to their liking and you won't notice anything out of the ordinary.

Run process accounting to keep track of typical software usage patterns of your users.

User Security

The particulars of user security varies widely with the nature of the system you're running. In some cases, a system will be an isolated machine performing mostly server functions with very few users who actually log in to the system and use it directly, most of the users thusly being people interacting with the server functions. In other cases, a system might have hundreds of users directly accessing the system simultaneously. Obviously, the degree to which user security is a concern depends largely on the character of your users, but be aware that one user who attempts to breach security, or who has poor security practices, can affect and possibly endanger an entire system.

Develop a standard method for creating and maintaining user accounts. Develop clear and concise acceptable use policies, and publish them well to your users. Don't create user accounts for people or organizations whom you have not previously interacted with in some form, or who have been known to have security problems on other systems.

You should set limits on the amount of resources a user can consume, from number of logins to amount of disk space; make sure that the user cannot cause a security breach or take down the system out of pure stupidity (e.g. a recursive script that creates a 10 M file each time)

In some cases, you may want to limit the manner in which a user can connect to the system; if you're providing a terminal login, make sure the terminal itself is secure and reasonably maintained. If you provide direct access via protocols such as telnet, consider running services such as tcp_wrappers or identd that verify the user is connecting from the system they claim to be connecting from.

Keep accurate logs of user activity; specifically, connection time, connection duration, and the place where they logged in/connected from. In some cases you may want to log more detail with process accounting, user command history, and activity monitoring.

You should regularly check for irregular user activity; there are many programs available that constantly "patrol" for failed attempts on the part of users to gain administrator privileges, access files that they shouldn't, or perform other unauthorized tasks.

Data Storage Security

Data and file storage, at first, does not seem to present itself as a security risk; either people have access to files or they don't! In reality, it turns out that there are many and complicated ways to access the same data on a given system, and a good system administrator should be aware of these schemes.

Know the file ownership scheme that your system implements; is it group based, user based, role based, or some combination of these? Know the different levels of protection you can apply to files and directories, and be aware of who has access to make changes to these protections.

Know the general structure of your file systems, how much is stored where, and who typically accesses what parts of them. Keep logs of disk activity (e.g. significant changes in disk space used) and of any disk problems.

Make sure that users are only able to access the parts of the system relevant to their use of it; your protection scheme should clearly and easily include a logical and conceptual separation of user and data files from system files.

Make sure that the file ownership schemes are consistent for various directories (i.e. that the owner of a directory owns all the files in that directory, etc.)

Insure that users cannot have access to more disk resources than you intend; often user disk quotes are the best solution to this.

If your file systems are available via any sort of network or sharing protocol, carefully examine the security of these protocols (see the protocols/services section above). Always check your configuration of these services to make sure that only authorized users and hosts are allowed to access shared data; many configurations by default allow for unauthorized access.

Always maintain secure backups of a system; the most standard conventional method is to backup files to a tape disk and then to remove that tape from the site to guard against data loss from fire, flooding, etc. In the case of operating systems, it's a good idea to maintain a known good copy of your operating system's configuration on a read-only media such as a CD-ROM.

If you maintain any databases, make sure that the database is accessible only to authorized users, both on the client side (via a data querying tool such as SQLnet) and on the server side (i.e. the actual database files stored on the disk drive of your system). As with other services, make sure any network and sharing of databases is done securely.

Passwords

Passwords are the central components in most security schemes; user accounts, sensitive websites, system services are all protected by them. If you know the right passwords, you can gain administrative privileges on a system where you may not even be a user or infiltrate an environment you've never even worked with before. They are conventionally accepted as a good way to implement security because they can be incorporated easily into most operating systems and sensitive software, and yet can be made complex enough to be difficult to "crack", while still being remembered by a user. Their downfall as a security scheme are in their power; one password is all you need to have complete access to an entire system, and passwords CAN be cracked. The best you can do is try to make these two events very unlikely.

Require unique, complex passwords for all user accounts on your system; it's not acceptable to have "guest" accounts or other accounts that don't require any sort of authentication. If an account is not ever used for connection (i.e. that account will never be accessed), remove its ability to login altogether.

Passwords should contain at least 6 characters and have a combination of letters and numbers, uppercase and lowercase. Passwords should not resemble any word, name, idea, or concept that might appear in any dictionary anywhere in the world. A good example: jY2EHxqy

Enforce password rotation and expiration; users should never be able to keep a password for more than a few months at a time, as someone could easily (but unnoticeably) brute force hack a password over a long period of time. You should also advise users against using the same password in other places.

The password file or similar mechanism for storing the passwords should be encrypted, and should not be available to the average user if possible (e.g. via shadowing). If a user can obtain the password file, they can use another system to try to crack the passwords without you noticing.

Never write passwords down or store them in anything but human memory.

System passwords should be changed at least once a month, and should not be shared with more people than is necessary.

System Administration

Quality system administration techniques can make all the difference in security prevention. There's not a lot required for most modern systems; many do self-checks and keep the system administrator automatically informed of any suspicious changes. But there are still a few general tips to follow:

Regularly browse through your system, looking at the contents of system directories, logs, and other files. Note file locations, file sizes. Observe the usage patterns of your machine and your users.

Run cracking tools regularly to check for vulnerabilities in your system configuration

Manually try to break into your system through different means.

Be aware of persons or groups who may have intentions of breaking into your system.

Keep your users advised of your techniques and what you expect of them to maintain security.