IT Auditing: Using Controls to Protect Information Assets

Chapter 9. Auditing Unix and Linux Operating Systems

Chris Davis and Mike Schiller
Summary by Martti Vasar
MTAT.03.240 Seminar on Enterprise Software, Fall 2011

Introduction

Unix dates back to 1969, when it was developed by employees at AT&T for the purpose of providing an environment suitable of running programs from multiple users. Security was not one of the goals at the time. There have been several variations of Unix operating systems made from the first system AT&T. One of the Unix operating system variation was BSD (Berkeley Software Distribution), that was and still is popular among the academic circle. In time different variations or distributions have been merged, an despite of the long run, they are still being used and developed.

Linux, a “Unix-like” operating system, came on the scene in 1991 and its author was Linus Torvalds from Finland. Linus programmed a software, that is able to run other programs, this means that Linux is a kernel and not an operating system, it gives the environment to run other applications and system utilities. Most of the programs that allowed to use this system fully came from the GNU project. That is why some people refer to Linux as *GNU/Linux* when speaking of it as an entire operating system.

As the Linux is open-source project, there are many distributions circling around. Each one of them with different tools, applications, system utilities and desktop environment. Today's popular distributions are Red Hat, Ubuntu, Debian, SUSE and Gentoo. Although different distributions have been developed from the same system, there are some differences among the different distributions, such as package management, tools in the system and file system structure.

Auditing Unix and Linux Operating Systems

Auditing these systems, we have to follow some key aspects, in order to get good overview how secure the system is. This chapter from the book is giving brief information about the following: (I) account management and password controls, (ii) file security and controls, (iii) network security and controls, (iv) audit logs and (v) security monitoring and general controls. They also contain information, how to do it and all of these points should consider equally important.

File Security and Controls

*nix operating system has file permissions for every file in the system. There are three sets of rights for every file and folder. They are following: user, group and world. Each of these entities can be granted read, write, and/or execute access. Every file can only have one owner and one group. Folder rights are more restrictive and the rights are following recursively in the file tree. If user is not an owner of the folder nor does he/she belongs to the folder group and folder has rights that world (others) cannot access it, the user is not capable of reading files inside the folder, even if files have all the rights for every set.

File security under *nix can be tricky. If there is a large group containing different users or users can edit shared folder in the file system and the folder does not have sticky bit defined, we might open vulnerability for file spoofing. This means, that we are able to delete one user file in this shared directory and add new file with the same name and with the changed content. We can alter others files

and they might not know about it. It is important to set sticky bit for folder permission (drwxrwxrwt) to avoid these kind of cases.

To check file and folder permissions, there is command *ls -l*, that shows who is the user of file and what group it belongs. Also it shows the current rights set to the file. It is important tool to check super user and restricted area rights with it, so these places should not be world writable (e.g. kernel, logs, user lists). To check the whole file system, it is possible to use recursive command *ls -alR*, that gives all the necessary information about file rights. If user can edit user list */etc/passwd* files, they can change their UID (user identifier) to 0 and therefore become a super user.

User security

Users are one of the weakest points in the system and there are many things to be considered, when managing users and their activities. Most important is to know, who are your user, that there is possibility to track every user to certain people. Otherwise there is no way to punish people, who are compromising the system.

Users are connecting mostly from the Internet, we must be sure that they are using good passwords and secured connections (no plain-text passwords sent over the Internet). Otherwise attacker, who has access to shadowed file */etc/shadow* with encrypted passwords, might use dictionary based brute-force crackers and get access to the system by that user. Default *passwd* tool is not good for changing passwords, as it allows to insert weak passwords. Also, users should change their password as often as they can, this can be forced by setting up some variables in the system. This is not really done in current systems. If the attacker is able to crack some of the passwords, they are no longer valid and it cannot be used to reach the system.

Adding new users and removing users should also audited carefully. There has to be strict policy how new users are added to the system and old ones removed from the system. The system administrator has to move removed user files somewhere else and change the ownership of files or remove them from the system complete and also mark for that user to use invalid shell in the */etc/passwd* file. Even if the removed user is able to login to the old system through trusted systems (does not require password login), he/she cannot do anything because there is no valid shell set. *nix uses UID to mark the file ownership. If new user is added and he/she gets the same UID as the deleted person, he/she gets automatically access to delete user files. Sensitive data can leak and it has to be avoided, so it is important to remove old user files.

User list */etc/passwd* should never contain users with same UID nor have UID as 0. 0 gives super user rights. System administrators have to check that two users does not share the same UID, because otherwise both of the users can kill each other's running processes and change their files.

Conclusion

Auditing is everlasting process and if you want to be good at it, you have to hold eye on the system constantly. It is strongly recommended to go through the logs, look if there has been any suspicious logins or behavior in the system and try to counter act. This means, that logging must be enabled and logs cannot be edited by other users. It is also strongly recommended to ask system administrators, why they have set up the system as it is, why they are running the services and try to document as much as possible. If the system has been compromised, all the users needs to change they passwords, the secret and public keys have to be changed in the system and others should be notified, that there has been breach into the system. This might seem to be dull to go through every detail, but we cannot hold back on the security. If you are interested in the fields of security, you should read this book.

Written by experienced IT audit and security professionals, IT Auditing: Using Controls to Protect Information Assets covers the latest auditing tools alongside real-world examples, ready-to-use checklists, and valuable templates.Â Build and maintain an IT audit function with maximum effectiveness and value * Implement best practice IT audit processes and controls * Analyze UNIX-, Linux-, and Windows-based operating systems * Audit network routers, switches, firewalls, WLANs, and mobile devices * Evaluate entity-level controls, data centers, and disaster recovery plans * Examine Web servers, platforms, and applications for vulnerabilities * Review databases for critical controls * Use the COSO Folks in the information security / IT audit space will enjoy this book. I mostly appreciate the check lists and audit programs at the end of each chapter. Read more.Â It seems auditors are far more likely to be interested in reviewing paperwork than really assessing effectiveness of security controls. Repeatedly I read statements like "evaluate the effectiveness of the security personnel function" by looking at documentation. In a few areas auditors seem to understand the value of real tests, e.g., trying to restore a backup rather than reviewing logs saying backups were completed.