Sunday, April 2, 2017

Ahmet Can Turgut | 40616 | COMP 434 Computer and Network Security – Spring 2017

Providing File System Security for Collaborated Users as a Group

INTRODUCTION

The vast majority record file management systems need techniques should regulate permissions or entry privileges on particular user or bunches of users. These file management systems control the capacity of the clients will view, change, navigate, and execute those substance of the recorded files [1]. Different file systems may allow different file permission techniques to give bunch of users. However, every file system depends on the read, write and execute permissions [2][3]. Let's look, file permissions in Unix based file systems. In Unix based file systems, Unix based file permission notations are used for displaying every individual files permission [4]. Below command line output `ls –l` basically shows which permissions assigned to files.

```
-rwxr-xr-x 1 CanTurgut CanTurgut size date  file_name
```

In Linux based operating systems "`chmod xxx file_name`" gives a file permission to specific file (file_name) with binary xxx number [4]. As in above figure file permission annotations given with three kind of words (r, w, x). These annotations repeated 3 times for, owner of the file, group owning of the file and permissions for the all users of the file system. For the chmod these permissions converted as a binary representation of the 9 digit bits (111 111 111 -> 777) [3]. These file permissions given to users' administrator or root of the operating system. File permissions good way to securing files for the multiple or group user allowed files in operating system. In some cases, users which is not the administrator of the user, may want to change file permissions.

PROBLEM DEFINITION

As I mentioned in the file permission dilemma, some users may want to access to giving file permission without being root or administrator. Let's create a case study example for solving this problem. Assume that we are working in the group project and only our group leader has a valid access rights for the group file. This does not mean that, our admin or root is our group leader.

Operating system or network admin has an only user has a access to change all files permissions. And our group leader gives a full permission to all group member for every files. And we detected some other users not related with our topics. As a helper of our group leader we want give a file permission to specific file or directory for only our group project members for security measurements without any root access.

PROBLEM SOLUTION

1.BASIC SOLUTION

One of the basic solution for our case-study, creating hidden directory whose only we know the name of this file such as “our_project”. If other users can’t find this file, they can’t read, write or execute this file. This solution is not perfect, since as we did not change any permission to any user. This protection method easily lost security with human-factor. Since any other user which not related with our group can see which file is our working file, our file can be detected with basic search.

2.EXTENDED SOLUTION

Again as a group leader helper which we have group leader access rights, we create a file. In that case group leader access rights allows to change permissions for everyone. As a group leader helper, I will create a file which is “our_project” but I will change file permissions for everyone part. Only executable part will be not changed in this part and read and write access permissions will be closed for all users. And with this permission. Only people can access this file where it is. Again in this case human-factor related issues can make our files insecure. But with basic search our files can’t be findable since there is no read access available for other users.

Moreover, grep Linux command may cause a problem. If specific user knows the file content, with recursive search with grep, user can found where our secret file present. Since grep function has a root access for every file in the file system [5].

For the solving above problem, folder name may have hashed or randomized with long character set. In this case file set should be meaningless for any human-being hard to detect. Moreover, content of folders may move to another subdirectory. Our main directory “our_project” filled with wrong content and files. And attacker or not permitted user hard to find file with searching the group file. In this case making sub-directories which include our content makes more secure.

RESULT

In our case study problem, our file is never full secured unless root access rights verified for the group leader. Again there is no full security system available in the world. Always door crack allows to attackers or forbidden users allow to access files. In this solution I tried to make as soon as harder with limited permissions.

REFERENCES

[1] Filesystem/Security - Gentoo Wiki. (n.d.). Retrieved April 2, 2017, from https://wiki.gentoo.org/wiki/Filesystem/Security

[2] File and Folder Permissions. Retrieved April 2, 2017, from https://technet.microsoft.com/en-us/library/bb727008.aspx

[3] Understanding Linux File Permissions | Linux.com | The source for Linux information. (n.d.). Retrieved April 2, 2017, from https://www.linux.com/learn/understanding-linux-file-permissions

[4] Learning the shell - Lesson 7: Permissions Retrieved April 2, 2017, from http://linuxcommand.org/lts0070.php

[5] GNU Grep 3.0. (n.d.). Retrieved April 2, 2017, from https://www.gnu.org/software/grep/manual/grep.html