Week #13 – Access Control

Overview of the week's objectives

This week's material will explore processes, tools, which enable a Linux system administrator to limit access to sensitive data. Given the need to secure a Linux server, you will learn to leverage the following tools; PAM, Access Control Lists, TCP Wrappers, GrSecurity, AppArmor, or SELinux.

TODO List

Please refer to all previous "Week's Overview PDFs" for details / advice relating to, or concerning, each of the tasks detailed in the remainder of this overview. While we focus on instructions specific to this week's material herein, previous instructions still apply.

Learning Activity			**Time in hours**		**Points**
			Expected	**Spent**	
Reading Assignments	O5L1 O5L2	Studying Guides & Videos	2		
Practice Assignments	O5L1-PQ O5L2-PQ	Taking Practice Quizzes	1		
	W13-PA	Working on PAs & Participating to PA forums	5		
Graded Assignments	W13-GQ	Taking Graded Quiz	1		2
	W13-DF	Participating to Discussion forums	3		1
			12		**3**

Task #1 – Study & Practice

Refer to "Week #2's Overview PDF" and/or all previous "Week's Overview PDFs" for detailed instructions on how to use online module guides, practice quizzes *and our* support forum *while working on this task.*

Task #2 – Practice Assignments

Refer to "Week #2's Overview PDF" and/or all previous "Week's Overview PDFs" for detailed instructions applying to all Practice Assignments.

Question #1

Perform the following tasks as root in your virtual machine.

1. Create a group called sales.
2. Create a user named April (and her last name will be YOUR last name). The username will be april.
3. Create a file named budget.
4. Set all permissions for user april to file names budget with read, write and executable rights.
5. If prompted, install setfacl if needed. You should know how to do this by now. Go online and research the following. Explain in your own words: *setfacl -m u:april:rwx budget*
6. Check April's permissions for the budget file.
7. Change April's permissions to read and execute only.
8. Check changed permissions. What changes do you see?
9. Remove all extended ACL entries previously applied in steps 1-8:
10. Check removed permissions again (repeat step 6). What changes do you see?

Question #2

Install Bastille Linux on your virtual machine. Review the available modules. Select two Bastille modules you find useful for security purposes and apply them to your system. Be very careful and read the warning labels carefully!

Question #3

Install SE Linux in Permissive mode on a Fedora virtual machine. Run the command line utility that shows system SELinux status in verbose mode to ensure it is working appropriately

Question #4

Install SELinunx in Enforcing mode on a Ubuntu virtual machine. Run the command line utility that shows system SELinux status in verbose mode to ensure it is working appropriately.

Question #5

On both your Fedora and Ubuntu systems, attempt to alter several system files as a user and then as root and find out what is blocked by SELinux. What does it take to create a SELinux error message?

Task #3 – Discussion Forums

Refer to "Week #2's Overview PDF" and/or all previous "Week's Overview PDFs" for detailed instructions applying to all discussion forums assignments.

Topic #1 – W13DF – SELinux vs. GrSecurity vs. AppArmor

Using the internet, research the differences between SELinux, GrSecurity, and AppArmor in terms of the types of scenarios they would be most appropriate for. Post an example of such scenario for each of the above which illustrates a situation in which it would be definitively selected other the two others. Justify why it is so.

Task #4 – Graded quizzes

Refer to "Week #2's Overview PDF" and/or all previous "Week's Overview PDFs" for detailed instructions applying to all graded quizzes.