Hardening System Configurations Lab Session

Overview

This lab session intends the attendees to get familiarized with the theoretical concepts that are presented in the Hardening System Configurations module with appropriate hands on practices. Briefly, all the exercises that are presented in this piece of work are grouped under seven distinct commonly used workstation and network hardening procedures. All the practical methodologies that can be used to go through the step that are required to complete this lab session can be found on either the lecture notes or the lecture slides for this module. All other missing practical tips will be elaborated within this piece to provide a better understanding of the concepts and tools, by interactively using them in real life situations.

It is required for the participants of this module to follow the stepwise instruction, if they are explicitly presented within a task. These instructions methodologically follow each, therefore to complete a task flawless they all need to be carried out in order. Notably in some of the task, the task is presented as a conceptualized mission. For those tasks it is expected from the participants to revise their knowledge that they gained in the Hardening System Configurations module lectures in systematized way to work out a solution for the given problem.

Outline of the Module

- PART 1: Users, Groups and File Permissions
- PART 2: System Updating, Automatic Notifications and Cron Jobs
- PART 3: Restricting Access
- PART 4: Minimizing and Protecting Privileged Services
- PART 5: Rootkit Hunter Installation and Configurations
- PART 6: uwf Firewall Installation and Configurations

▪ PART 1: Users, Groups and File Permissions

Imagine that you are system administrator in an organization, where the employees and their information is as follows:

Employee 1

Name Surname: John Stew

Position: Manager

Employee 2

Name Surname: Tom Cook

Position: Auditer

Employee 3

Name Surname: Jane Hofman

Position: Manager

Employee 4

Name Surname: Ari Righi

Position: IT Personnel

Employee 5

Name Surname: Tim Allen

Position: IT Personnel

Employee 6

Name Surname: Charlotte Brown

Position: Auditer

By using above presented information, please complete the following steps:

1. Create user accounts for each of these users. For each user generate a password that is secure with numerals included using pwgen (note that you have to install pwgen first).
2. Create groups for managers, it personnel and auditers.
3. Create a file called Report.txt in John's home folder.
4. Change the owner of the file to be John.
5. Change the group of the file to managers.

6. Modify the permissions of Report.txt in a way that owner permissions will be read/write/execute, group permissions will be read/execute and permissions for other users will just be read.
7. Check whether the modification of permissions is applied successfully.
8. You know that Charlotte will quit his job in 3 months. Lock her account in a way that Charlotte's user account will not be accessible after 3 months starting from today.
9. You learnt that Ari quit his job today. Disable his user account without loosing his user data.
10. Modify John's privileges by adding his account in sudoers group.

▪ PART 2: System Updating, Automatic Notifications and Cron Jobs

You started your new job as a system administrator in Middle East Technical University. Regarding the operating system installation on the workstation that you are currently using, as a system administrator you are not sure whether the workstation is up-to-date. Therefore, complete the following steps to be sure about the workstation that you are using have been updated periodically.

1. Check whether your system has the latest operating system updates installed.
2. If they are not installed issue the necessary command on the terminal to complete system updates.
3. You want your system to regularly and automatically complete system updates. What packages you need to install? How can you solve this problem? (hint. Cron-apt?)
4. Install the necessary package that you opt in the previous step by using the aptitude in a terminal shell.
5. Modify the package configurations in way that system will automatically look out for system updates every day.

▪ PART 3: Restricting Access

You are asked to restrict all possible unauthorized access to a workstation. Please complete the following steps to attain necessary workstation hardening measures:

1. You realize that the bootloader is not password protected. What can be the possible risk that freely available grub list can cause?
2. You want to password protect the grub. Choose a strong password, concerning the measures presented in authentication.
3. Calculate a salted hash of the password that you have chosen.
4. Edit /etc/grub.d/40_custom file in way that the password you have chosen will be assigned as the grub password for your user.
5. Update grub configurations.
6. Install both client and server packages for OpenSSH.

7. Modify the port for OpenSSH to 2021 instead of default 22.
8. Modify OpenSSH configurations in a way that only the root user will have the privileges to establish an SSH connection to the workstation in use.

▪ PART 4: Minimizing and Protecting Privileged Services

Assume that you are working on a workstation, which has a fresh operating system installation. You are asked to disable all unnecessary services that are running in the background. Please complete the following steps to accomplish this task:

1. Install sysv-rc-conf package through aptitude.
2. Identify two unneeded daemons that are running on the background.
3. Disable the unneeded deamons by using sysv-rc-conf for all runtimes.
4. Check whether IPv6 is enabled.
5. Edit /etc/sysctl.conf in order to disable IPv6.
6. Restart networking setting to apply changes.

▪ PART 5: Rootkit Hunter Installations and Configurations

Your organizations' network users are having a tough time against the increasing spread of Trojan horses and rootkits. As a system administrator your manager asked you to install and properly configure a rootkit hunter on a virtual test machine. Please follow the following directives to complete this task:

1. Install rkhunter with aptitude through a terminal shell.
2. Use rkhunters command to run a scan.
3. Can you identify any process, which the rkhunter lists that seems to be not normal? If so what might that process be? How can we be sure that it is a rootkit?
4. Edit /etc/rkhunter.conf so that it will watch /dev/.static and /dev/.udev to watch suspicious activities in these locations.

▪ PART 6: ufw Firewall Installation and Configurations

Assume that you are setting up a firewall in correspondence with your organizations network security policy. You are required to complete the following steps to configure Ubuntu's out of the box firewall ufw with the desired rules:

1. Enable uwf.
2. Set ufw's default policy to deny all incoming and outgoing traffic.

3. Assuming that the workstation that you are working on is has an Apache Web server and it needs to be access remotely through ssh. What rules you need to implement on firewall level over the default policies to allow these operations? (Assume that these service are running on their default ports)
4. Modify ufw's configurations to allow access to the services that are mentioned in the previous step.