**Objectives**: In this assignment, you will explore various security measures that can be implemented in Linux system to enhance the security. The assignment will cover security updates, account security, firewall configuration, security log fills, and security audits using Lynis.

**For the tasks below, use the Linux Terminal exclusively. Select only three tasks out of the five options provided.**

1. Security Updates
   1. Find the specific command(s) that can be used to install Ubuntu Security Updates.
   2. Set up an automated process for installing Ubuntu security updates every Wednesday at 11 PM using a CRON job.
   3. Verify the above automated process

|  |  |
| --- | --- |
| 1-sudo apt update & we can use after sudo apt upgrade to installed last packages in kali |  |
| 2-crontab -e after press 1 and go to nano and edit your crontab “0 23 \* \* 3 apt update && apt upgrade -y” save and exit |  |
| 3- crontab -l check your command listed in the output ,  And wait until the schedule time are installed automatically and after you can check manually if the security update it just type this command “ apt list –upgradable “ |  |

1. Secure user account
   1. Password Security: The pam\_cracklib module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more.

Install pam\_cracklib module and document how do you enforce the following password policies:

1. Enforce a minimum password length of 8 characters.
2. Implement requirements for password complexity to include a mix of different character types, such as uppercase letters, lowercase letters, numbers, and special characters.
3. Prevent users from using common dictionary words as passwords.
4. Set a maximum password age, prompting users to change their passwords after a specified period, such as every 90 days.
5. Implement a policy to lock out user accounts after a specified number of failed login attempts (3 attempts)
6. After you applied the above policies, you should verify
   1. Secure Accounts by disabling root login: Secure user accounts by disabling direct root login. Mention the steps on how to disable root login.

|  |  |
| --- | --- |
| A-sudo apt install libpam-pwqaulity |  |
| b- sudo nano /etc/pam.d/common-password after add the new conditions for password password requisite pam\_cracklib.so ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 minlen=8 difok=3 reject\_username enforce\_for\_root retry=3 |  |
| c- cracklib-check to check the condtions for password as we see in picture when your password combine with conditions the system gave you ok |  |
| d- sudo nano /etc/ssh/sshd\_config to make PermitRootLogin no  locate permitrootlogin and delete the hash and insert no then save and exit |  |
| e- check the status  Sudo service ssh status |  |

1. Ubuntu's Uncomplicated Firewall (UFW) is a user-friendly command-line tool for managing firewall rules in Ubuntu-based systems. Document the following:
   1. Installation of UFW
   2. Enable or disable UFW to activate or deactivate the firewall.
   3. List the current firewall rules using UFW.
   4. Adding, modifying, and deleting firewall rules using UFW.

|  |  |
| --- | --- |
| 1- sudo apt install ufw |  |
| 2- sudo ufw enable , sudo ufw disable |  |
| 3- sudo ufw status |  |
| 4- add rule : sudo ufw allow 80  Modifiying rule : sudo ufw delete allow 22  sudo ufw allow 2222  deleting rule :sudo ufw delete 3 |  |

1. Security log files:
   1. Provide where the **security log files** are typically located in Ubuntu. Include specific paths, directories, or file names where the log files are commonly found.
   2. Enable logging of critical events: Configure the system to log critical security events, such as failed login attempts.

Note: the following locations for security log files might help

* /var/log/auth.log: This log file contains authentication-related events, including successful and failed login attempts, password changes, and authentication failures.
* /var/log/syslog: The syslog file captures system-wide log messages, including security-related events. It can include information about unauthorized access attempts, system startup/shutdown, and various other events.
* /var/log/secure: This log file is specific to some distributions, such as CentOS, and contains security-related events like login attempts, authentication failures, and privilege escalations.
* /var/log/messages: Similar to syslog, the messages file captures system messages and events, including security-related logs.

1. Security Audit : Lynis is a security auditing and hardening tool that scans the system for vulnerabilities, misconfigurations, and potential security risks. Document the followings:
   1. Install Lynis on the target system
   2. Launch Lynis and initiate a system security assessment using the appropriate command.
   3. Once the assessment is complete, retrieve the generated Lynis report. Describe the structure and contents of the report, including the severity levels assigned to identified issues

|  |  |
| --- | --- |
| 1- sudo apt install lynis |  |
| 2- sudo lynis audit system “lynis will start scaning the system “ |  |
| 3- sudo nano /var/log/lynis.log  The report provides details on the scan itself, discovered vulnerabilities, warnings, suggestions, and more  Lynis uses the following severity levels:  CRITICAL: Represents critical vulnerabilities or misconfigurations that pose a severe risk to the system's security.  HIGH: Indicates high-risk items that need immediate attention to mitigate potential security risks.  MEDIUM: Signifies medium-risk items that should be addressed to enhance system security.  LOW: Identifies low-risk items that may not have an immediate impact but should still be reviewed and resolved.  INFO: Provides general information and recommendations that can help improve system security. |  |

Students need to submit a detailed report, including screenshots, to describe what has been done and observed. Please provide explanations for any interesting or surprising observations. Late submissions of the assignment will result in a 10% deduction.

**Marking guide:**

|  |  |
| --- | --- |
| **TASKS** | **Mark** |
| Task | 3 |
| Task | 3 |
| Task | 3 |
| **TOTAL SCORE** | **/9** |
|  |

**Links**

Security Audit

<https://www.digitalocean.com/community/tutorials/how-to-perform-security-audits-with-lynis-on-ubuntu-16-04>

Secure user account

<https://deer-run.com/users/hal/sysadmin/pam_cracklib.html>

<https://upcloud.com/resources/tutorials/manage-linux-user-account-security>

<https://www.tenable.com/audits/items/CIS_Debian_Linux_7_v1.0.0_L1.audit:67b87807788470cd6e6df619ecd0c68d>

<https://www.redhat.com/sysadmin/pam-configuration-file>

CRON calculator

<http://www.csgnetwork.com/crongen.html>

Ubuntu's Uncomplicated Firewall (<https://www.youtube.com/watch?v=YV3aDbQTzrs&list=PL6IQ3nFZzWfpoLWZ98Adr5GwBR4vBaPyi&index=23>)