Linux Security Maintenance

Introduction and/or Background

As robust as Linux is it is still vulnerable to attack. Just as a Windows system security management of the OS is required. Two tools amoung many that are available:

- ClamAV
- Lynis

ClamAV

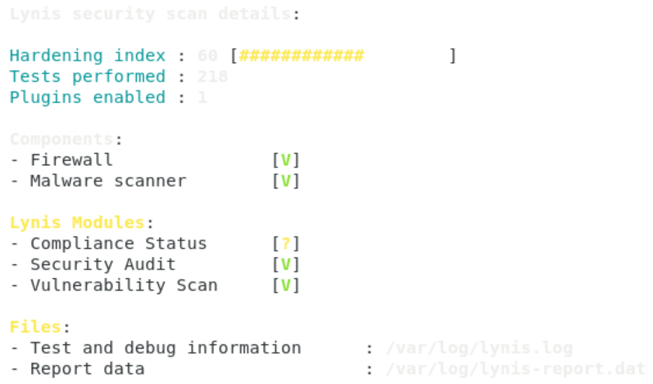
ClamAV is a antivirus system available for Linux, Mac and Windows. In Linux it is a command line tool. ClamAV utilizes a backend to perform auto updates to the malware database. That is ClamAV’s default mode of operation. ClamAV can be operated in a interactive mode as well.

Lynis

Lynis is a host based analytics tool for reporting system status from a security perspective. Lynis itself does not perform any modification or hardening of the OS system. It is left to the administrator to enable the suggested changes to the system. Lynis reports three sections:

- Warnings: a serious corrective is required to harden the system. (one of which is the version in the repositories is old.)
- Suggestions: Those actions that the administrator can take to shrink the attack surface for the OS.
- Summary: Review of the scan, location of the scan log, Lynis version, etc.

Example output:



```
Lynis security scan details:

Hardening index : 60 [############        ]
Tests performed : 218
Plugins enabled : 1

Components:
- Firewall               [V]
- Malware scanner        [V]

Lynis Modules:
- Compliance Status      [?]
- Security Audit         [V]
- Vulnerability Scan     [V]

Files:
- Test and debug information      : /var/log/lynis.log
- Report data                     : /var/log/lynis-report.dat
```

For simplicity sake we will use the Lynis version in the repositories. For those that wish to tap Lynis as a production tool the latest packages are here -- https://packages.cisofy.com/community/#debian-ubuntu -- for Debian and Ubuntu.

Objectives

In this project/lab the student will:

- Gain familiarity Linux security tools

Equipment/Supplies Needed

- As specified in Lab 0.0.1.

Procedure

Perform the steps in this lab in the order they are presented to you. Answer all questions and record the requested information. Use a Linux Virtual Machine to perform lab activities as directed. Unless otherwise stated, all tasks done as a non-root user. If root access is needed use the sudo or su command.

Assignment

Virus Scanning

1. Execute:
2.
   ```
   apt-get install clamav
   ```
3. Next lets check the install:
4.
   ```
   systemctl | grep clam
   ```
5. Take a screen shot of the terminal screen. Add that to your document.
6. Set to an interactive mode:
7.
   ```
   systemctl stop clamav-freshclam.service
   ```
8. First we need to run an update of the database:
9.
   ```
   freshclam
   ```
10. Run a virus scan:
11.
    ```
    clamscan -i --bell -v /home/<your account dir>
    ```
12. How long the scan takes depends on the amount of data in your directory being scanned. At the end you should receive a summary of the results. Take a screen shot of the terminal screen. Add that to your document.
13. Now reset ClamAV back to daemon mode:

14 `systemctl start clamav-freshclam.service`
15 `systemctl status clamav-freshclam.service`

16 Take a screen shot of the terminal screen. Add that to your document.

System Audit

17 Install Lynis

18 `aptitude install lynis`

19 Lynis is a shell script so there is no systemctl review to perform. Promote to root and execute the following:

20 `lynis audit system`

21 Take a screen shot of the summary on the terminal screen. Add that to your document.

22 Execute the following:

23 `lynis audit system --check-all`

24 Take a screen shot of the summary on the terminal screen. Add that to your document.

Reflection Questions

1 What is the function of freshclam?
2 By default Clamav runs in what mode?
3 What is the difference of performing a Lynis audit with and without the –check-all option?

Lab Submissions Proof: Provide screenshots as indicated in the lab; upload your proof to Canvas for grading.

Rubric

Checklist/Single Point Mastery

Concerns *Working Towards Proficiency*	*Criteria* *Standards for This Competency*	*Accomplished* *Evidence of Mastering Competency*
	Criteria #1: Screenshot of ClamAV running *(14 points)*	*ClamAV service running by inspection with systemctl.*
	Criteria #2: Screenshot of clamscan summary. *(14 points)*	*Ability to perform a scan using the utility.*
	Criteria #3: Screenshot of ClamAV returned to daemon mode *(14 points)*	*ClamAV service running in daemon mode and validation of same.*
	Criteria #4: Screenshot of Lynis with audit option *(14 points)*	*Output of the system status using audit option on given OS.*
	Criteria #5: Screenshot of Lynis with –check-all option *(14 points)*	*Output of the system status using audit option on given OS using the –check-all option.*
	Criteria #6: Answer to reflection question 1 *(10 points)*	*Identification of function of the freshclam tool.*
	Criteria #7: Answer to reflection question 2 *(10 points)*	*Identification of the default mode for the ClamAV service.*
	Criteria #8: Answer to reflection question 3 *(10 points)*	*Discern the differences in output of the tool with and without options.*