**Lab Experiment 03**

**B. Tech CSF-CSE Semester III Course: Physical and IT Security**

**By: Dr. Gopal Singh Rawat**

**Lab Objective: Understanding Vulnerabilities in Local Operating Systems**

Use Windows Vulnerability Scanner and 3rd Party Portals for reviewing latest vulnerabilities to understand vulnerabilities on local system, Network and environment for gaining deeper view

**Tools:**

* Windows / Kali Linux OS
* SFC will inspect all of the important Windows files on your computer, including Windows DLL files. If System File Checker finds a problem with any of these protected files, it will replace it.
* Trip Wire (Tripwire is a popular open-source Linux Intrusion Detection System (IDS) that runs on systems to check if any of the files have modified or changed in authentically and alert that to the administrator, if the administrator finds the changes authentic, they can accept the changes by updating Tripwire database)
* CVE Details (<https://www.cvedetails.com/>)
* Lynis OS Audit Scanner (**Lynis** is an open-source security auditing tool for UNIX derivatives like Linux, Mac OS, BSD, other Unix-based operating systems etc. Performing extensive health scan of systems that support**System Hardening** and **Compliance Testing**. An open-source software with GPL License. This tool also scans for general system information, vulnerable software packages, and configuration issues. It is useful for System Administrators, Auditors, Security Professionals)

**Steps to perform:**

1. Run SFC (system file check) on Windows, read the CBS.log file
2. Run Trip Wire on Kali Linux OS
3. Run Lynis on Linux OS as ./lynis audit system --quick --auditor "YOUR\_SAP\_ID"
4. As per the reports generated by the scanners, perform steps to harden the OS and mitigate the vulnerabilities reported.

**Lab #03 File Work:**

1. Perform this Experiment and make a list of 10 reported vulnerabilities in Windows/Kali Linux OS.
2. Review CVE Details to learn about their mitigation steps as per the below table.

|  |  |  |  |
| --- | --- | --- | --- |
| **Type of OS** | **Vulnerability** | **Vulnerability Details** | **Mitigation Steps** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Bonus: Read about crontab, Schedule the tripwire check (daily at 7:30 AM)

Hint: look for “tripwire” directory first

**Windows Log file SFC:**

*%windir%\Logs\CBS*

**Find directory name:**

find / -type d | grep "directory name"

find / -type f -iname file1.txt

find / -type f -name '\*.png'

**To avoid all of the "Permission denied" results, you can use:**

find / -type d -name "directory name" -print 2>/dev/null

**Tripwire commands:**

tripwire -m i // Database initialization

tripwire -m c // Check mode

tripwire -m c -I // Interactive check mode

tripwire -m u //Database update mode

twprint -m d // see database

twadmin -m p // see policy

Look at the tripwire policy “ **/etc/tripwire/twpol.txt”**

tripwire -m t -e $user@$domain //test mode email it

**Tripwire Files:**

ls /etc/tripwire

locate file\_name

tree directory\_name

[How to Search Files on the Linux Terminal | LinuxHostSupport](https://linuxhostsupport.com/blog/how-to-search-files-on-the-linux-terminal/#:~:text=You%20can%20use%20the%20find,that%20you%20want%20to%20search.&text=You%20can%20use%20the%20following,d%20%E2%80%93%20directory)

[command line - How do I save terminal output to a file? - Ask Ubuntu](https://askubuntu.com/questions/420981/how-do-i-save-terminal-output-to-a-file)

[Tripwire intrusion detection tutorial on Linux - Linux Tutorials - Learn Linux Configuration](https://linuxconfig.org/intrusion-detection-systems-using-tripwire-on-linux)

**Install Lynis:**

git clone <https://github.com/CISOfy/lynis.git>

cd lynis/

ls

./lynis -h

**Lynis Commands**:

./lynis show commands

./lynis audit system

ls -l /var/log/lynis.log (logfile)

ls -l /var/log/lynis-report.dat

./lynis show details HRDN-7230

or

apt install lynis

lynis show commands

lynis audit system

lynis show tests

lynis show tests ACCT-9626

[Lynis - Security Tool for Audit and Hardening Linux Systems - GeeksforGeeks](https://www.geeksforgeeks.org/lynis-security-tool-for-audit-and-hardening-linux-systems/)