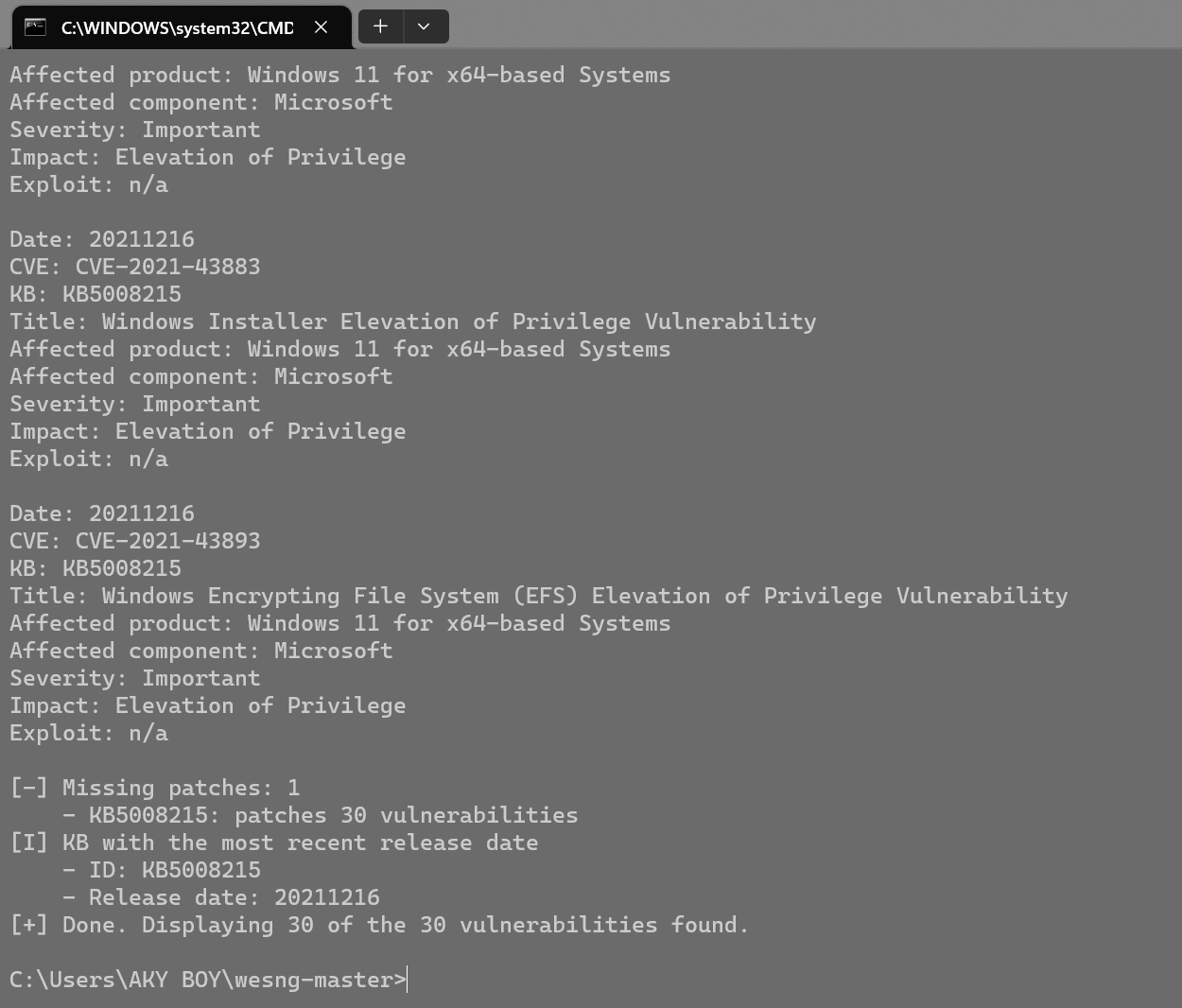
**LAB EXPERIMENT – 3**

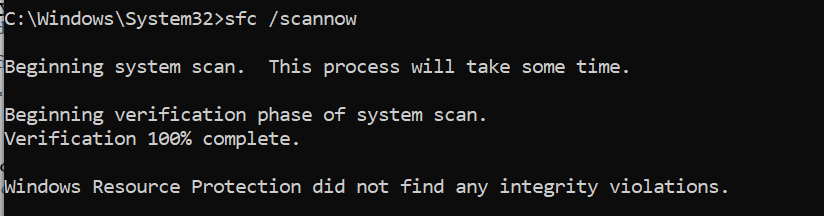
**Understanding Vulnerabilities in Local Operating Systems**

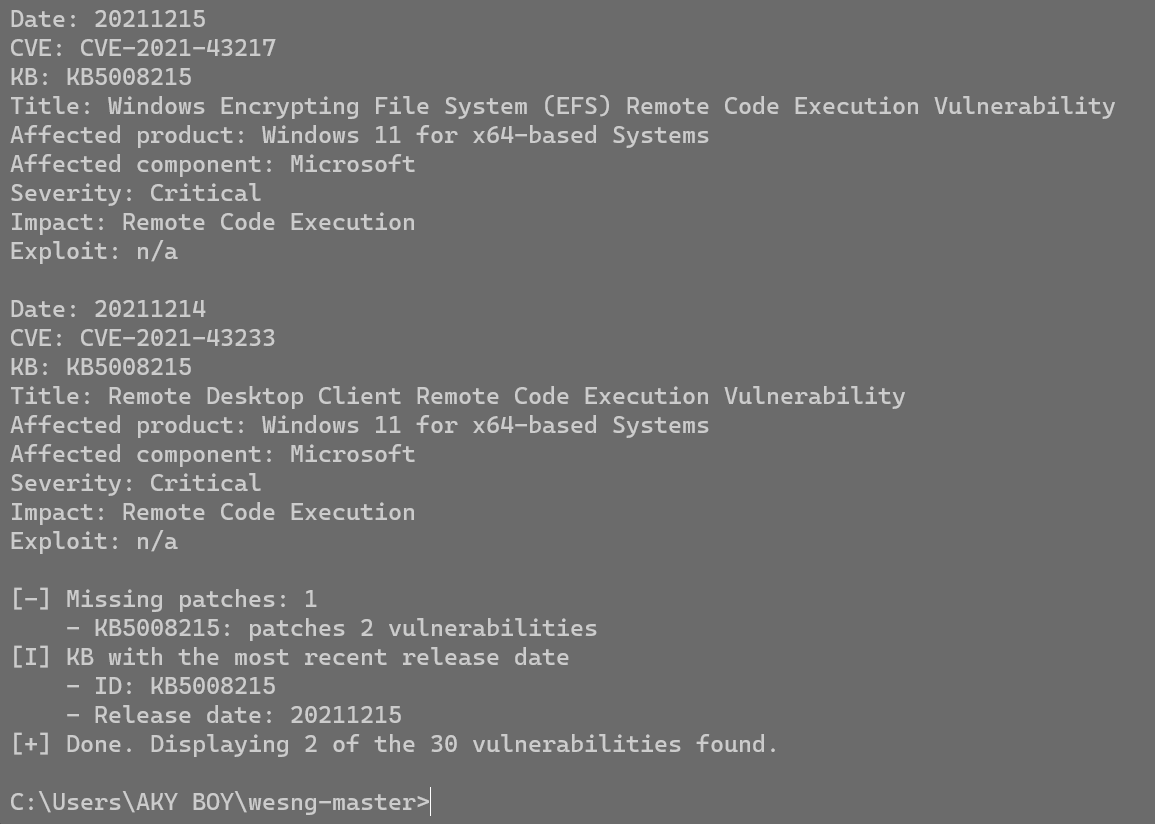
**Windows Vulnerability CHECK**

1. Python --version
2. pip3 install chardet
3. git clone <https://github.com/bitsadmin/wesng.git>
4. systeminfo
5. systeminfo > sysinfo.txt
6. cd wesng-master
7. dir
8. python wes.py ..\sysinfo.txt
9. python wes.py ..\sysinfo.txt -s critical
10. python wes.py ..\sysinfo.txt -s critical > critical.txt

|  |  |  |  |
| --- | --- | --- | --- |
| **Type of OS** | **Vulnerability** | **Vulnerability Details** | **Mitigation Steps** |
| Windows 11 | CVE-2023-24054 | Elevation of privilege vulnerability in Windows Update Assistant | Install the latest security updates from Microsoft. |
| Windows 11 | CVE-2023-21999 | Remote code execution vulnerability in Microsoft Exchange Server | Install the latest security updates from Microsoft. |
| Windows 11 | CVE-2023-21996 | Denial-of-service vulnerability in Microsoft Exchange Server | Install the latest security updates from Microsoft. |
| Windows 11 | CVE-2023-21995 | Remote code execution vulnerability in Microsoft Exchange Server | Install the latest security updates from Microsoft. |
| Windows 11 | CVE-2023-21985 | Remote code execution vulnerability in Windows Print Spooler | Disable the Print Spooler service if not in use. |
| Kali Linux | CVE-2023-24056 | Elevation of privilege vulnerability in OpenSSH | Upgrade to the latest version of OpenSSH. |
| Kali Linux | CVE-2023-24055 | Remote code execution vulnerability in Samba | Upgrade to the latest version of Samba. |
| Kali Linux | CVE-2023-24053 | Denial-of-service vulnerability in Apache HTTP Server | Upgrade to the latest version of Apache HTTP Server. |
| Kali Linux | CVE-2023-24052 | Remote code execution vulnerability in BIND | Upgrade to the latest version of BIND. |
| Kali Linux | CVE-2023-24051 | Remote code execution vulnerability in MySQL | Upgrade to the latest version of MySQL. |







**USING LYNIS**

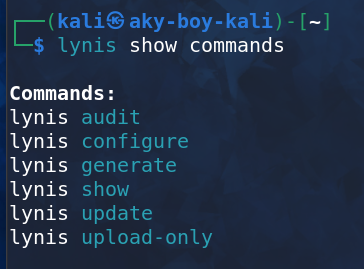
* Install Lynis using command: **sudo apt install lynis**
* Check audit using: **lynis audit system --quick**



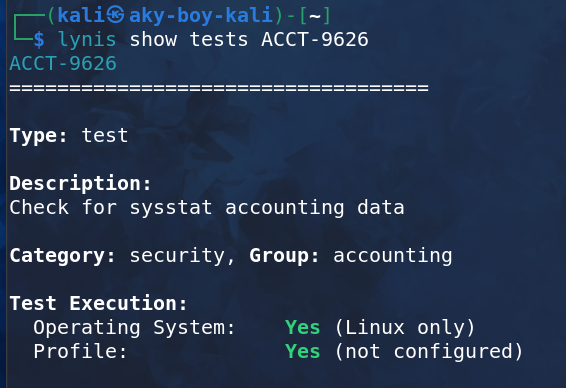
* Warnings and Suggestions by Lynis after detecting OS.



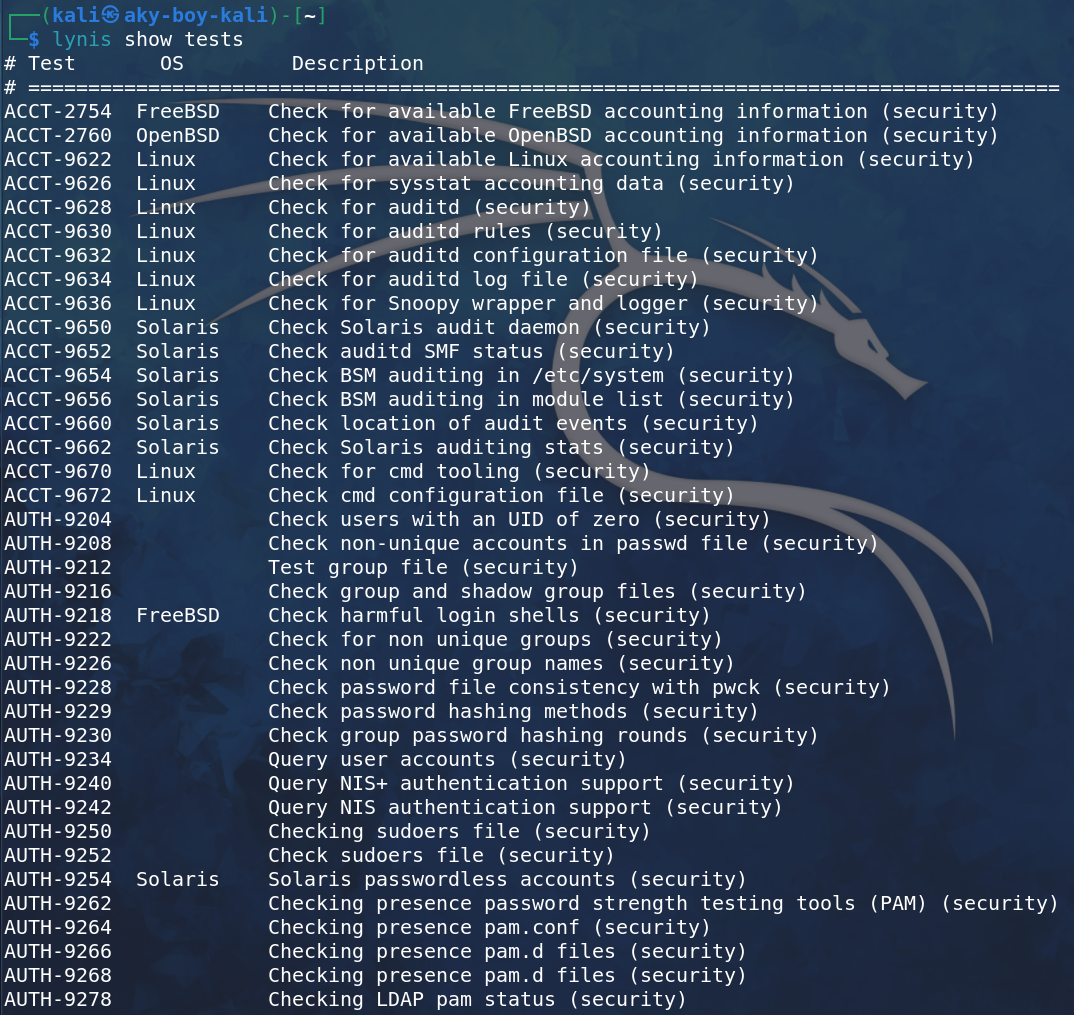
* To view all commands: **lynis show** and to view audit commands: **lynis show commands**



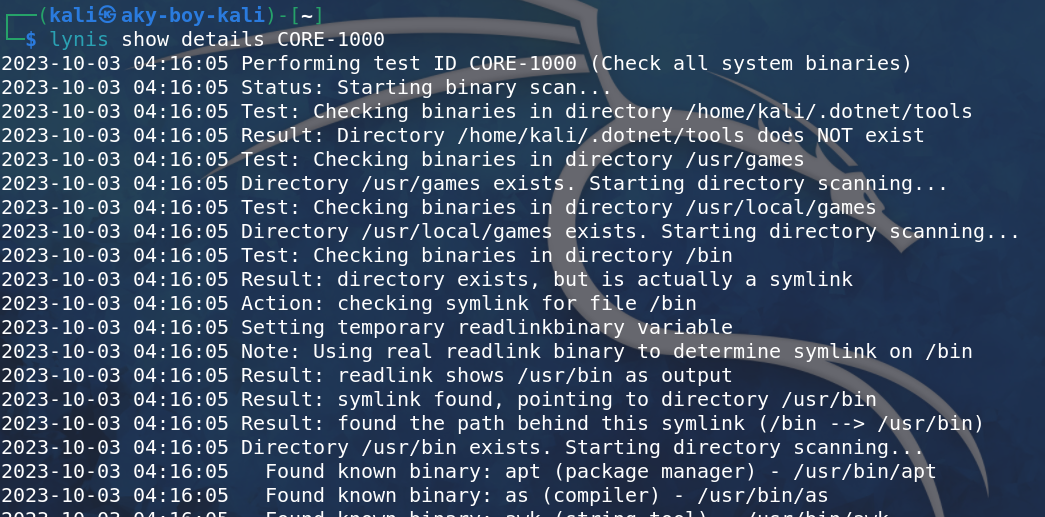
* **Lynis show tests ACCT – 9626** to view particular test.

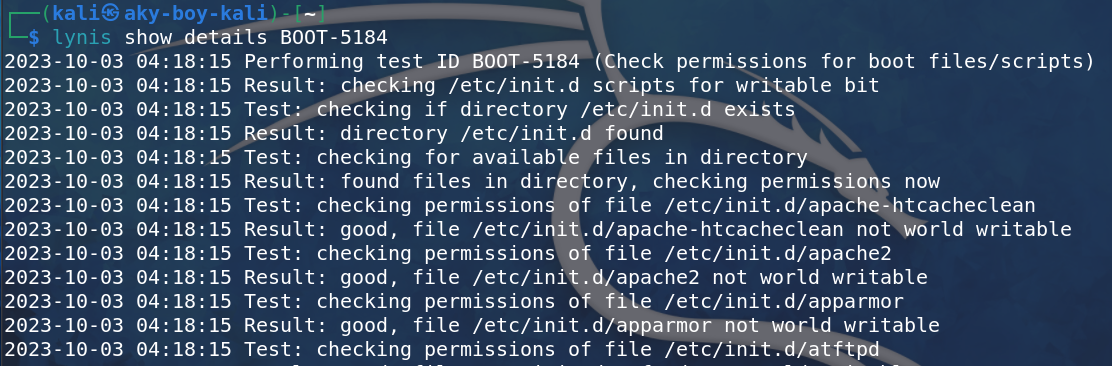


* To view all test together: **Lynis show tests**



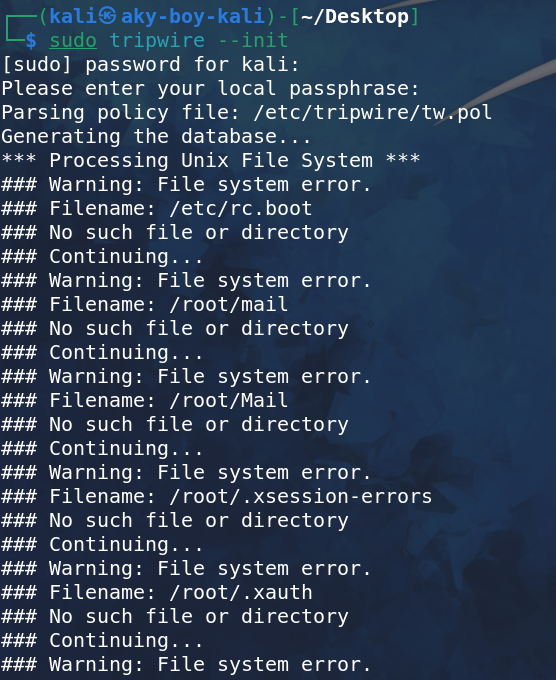
* Some individual details of particular tests.



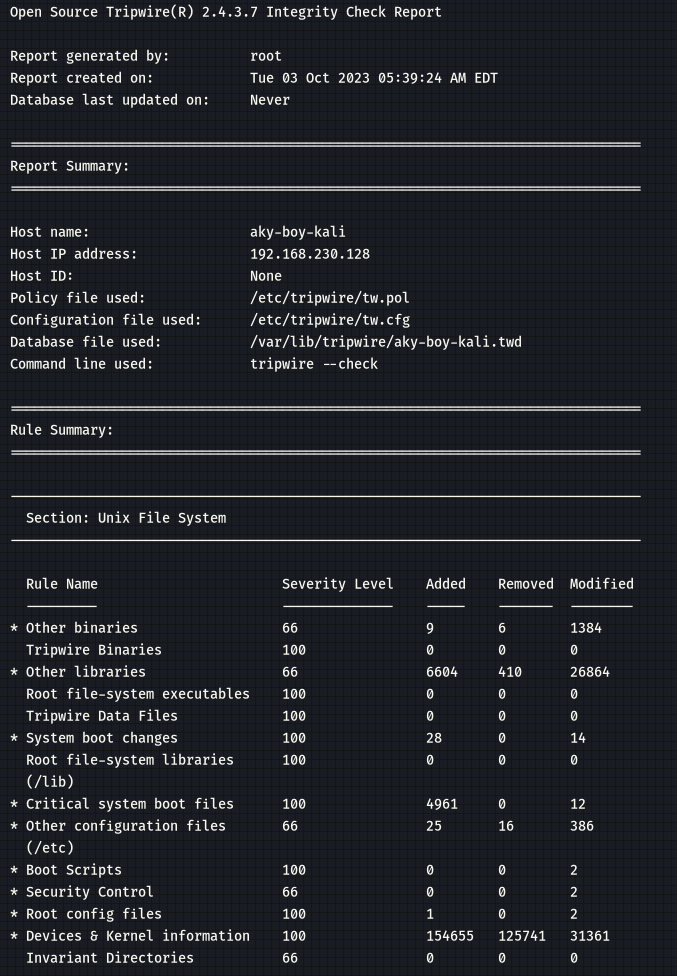


**USING TRIPWIRE**

* Install tripwire using: **sudo apt install tripwire** and do the configuration using same password.
* **Sudo tripwire --init**



* Table below is the Integrity report generated by Tripwire.
* **Sudo apt tripwire –check > tripwire.txt**



**BONUS: Crontab Scheduling**

* To view the number of Crontabs: **crontab -l**



* To install or schedule new crontab using the nano editor: **crontab -e**



* File auto-generated at 7:30 according to 24hr clock with the Integrity Report using Tripwire.

