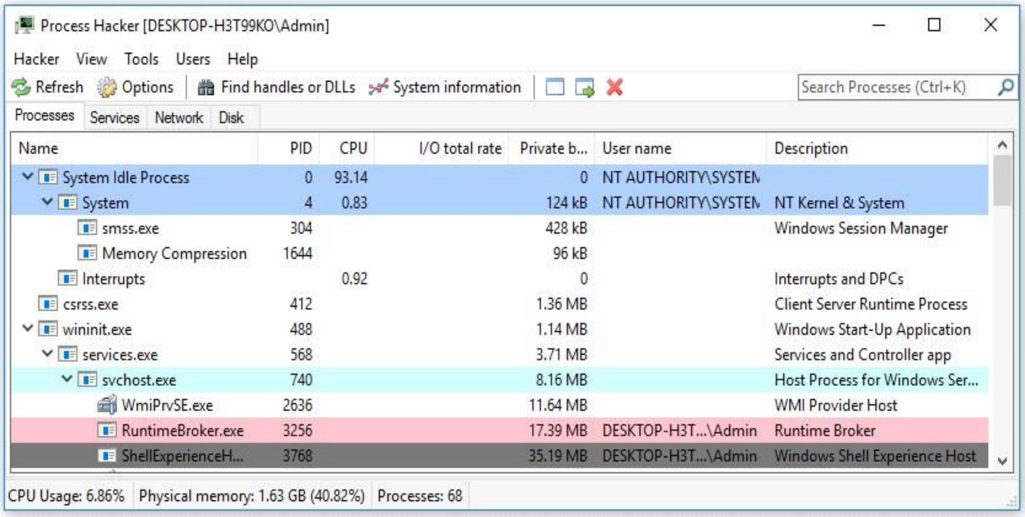
Week 4

1.<u>Process observation and analysis with Process Hacker</u>

Process Hacker is an open-source tool that will allow you to see what processes are running on a device, identify programs that are eating up CPU resources and identify network connections that are associated with a process.

<u>observation and analysis.</u>



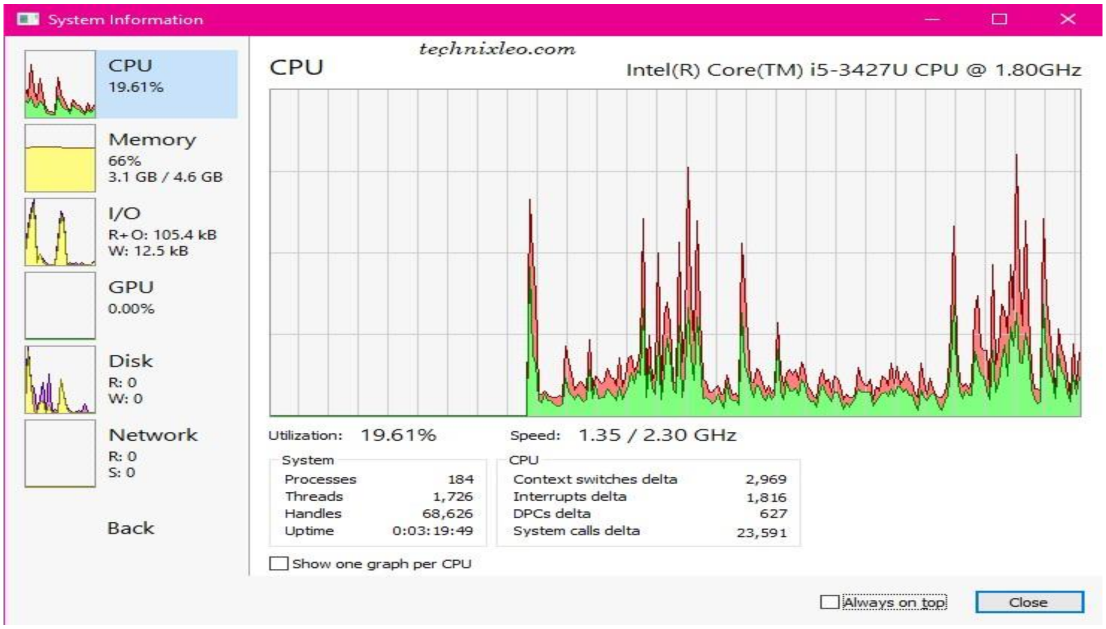
Name	PID	CPU	I/O total rate	Private b...	User name	Description
System Idle Process	0	93.14		0	NT AUTHORITY\SYSTEN	
System	4	0.83		124 kB	NT AUTHORITY\SYSTEN	NT Kernel & System
smss.exe	304			428 kB		Windows Session Manager
Memory Compression	1644			96 kB		
Interrupts		0.92		0		Interrupts and DPCs
csrss.exe	412			1.36 MB		Client Server Runtime Process
wininit.exe	488			1.14 MB		Windows Start-Up Application
services.exe	568			3.71 MB		Services and Controller app
svchost.exe	740			8.16 MB		Host Process for Windows Ser...
WmiPrvSE.exe	2636			11.64 MB		WMI Provider Host
RuntimeBroker.exe	3256			17.39 MB	DESKTOP-H3T...\Admin	Runtime Broker
ShellExperienceH...	3768			35.19 MB	DESKTOP-H3T...\Admin	Windows Shell Experience Host

CPU Usage: 6.86% | Physical memory: 1.63 GB (40.82%) | Processes: 68

- **System** is a **Name** of the running process in your system.
- Here **System** is the *Parent process* and **Smss.exe** is a *Child process*.
- 488 is the **PID** of winning.exe process.**The PID** is the process ID, this is a unique number assigned to the process.
- Double click on particular process to see complete details of a process, including when the process is started.
- 93.14 number is the amount of **CPU** being consumed by the process.
- Also, Notice the **PID** of system process is always 4.
- **Private bytes** indicates the total amount of memory that
- a process has allocated, not including memory shared with other processes.
- **The User name** tab displays which account was used to launch the process

Graphical -view

To see the information in a graphical view, Click on System Information and a new tab opens as folllows.



CPU 19.61%

Memory 66% 3.1 GB / 4.6 GB

I/O R+O: 105.4 kB W: 12.5 kB

GPU 0.00%

Disk R: 0 W: 0

Network R: 0 S: 0

CPU Intel(R) Core(TM) i5-3427U CPU @ 1.80GHz

Utilization: 19.61% Speed: 1.35 / 2.30 GHz

System	
Processes	184
Threads	1,726
Handles	68,626
Uptime	0:03:19:49

CPU	
Context switches delta	2,969
Interrupts delta	1,816
DPCs delta	627
System calls delta	23,591

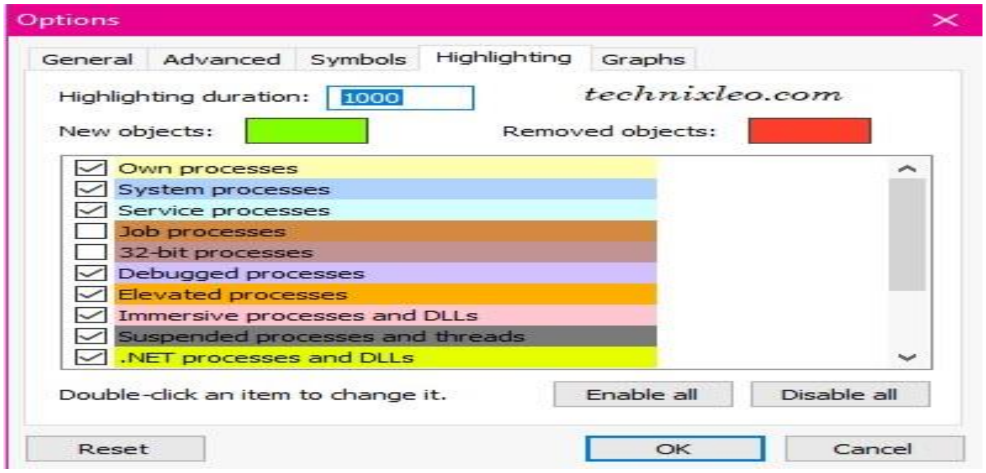
☐ Show one graph per CPU

☐ Always on top

Color-Coding

Process Hacker highlights different processes in different colors.

- The meaning of each color under Option Tab, Then click on Highlighting Tab.
- Same tab you have an option of changing the color and the duration for highlighting.



Highlighting duration: 1000

New objects: 🟩 Removed objects: 🟥

☑ Own processes
☑ System processes
☑ Service processes
☐ Job processes
☐ 32-bit processes
☑ Debugged processes
☑ Elevated processes
☑ Immersive processes and DLLs
☑ Suspended processes and threads
☑ .NET processes and DLLs

Double-click an item to change it.

2.NTFS Permissions

NTFS permissions are used to manage access to the files and folders that are stored in NTFS file systems.

Setting NTFS Permissions:-

1. In Windows Explorer, right-click a file, folder or volume and choose Properties from the context menu. The Properties dialog box appears.
2. Click the Security tab.
3. Under Group or user names, select or add a group or user.
4. At the bottom, allow or deny one of the available permissions.There are both basic and advanced NTFS permissions. You can set each of the permissions to “Allow” or “Deny” to control access to NTFS objects. deny all the available permissions and click on 'apply' and click on 'ok' **Here are the basic types of access permissions:-**

*Full Control — Users can add, modify, move and delete files and directories, as well as their associated properties. In addition, users can change permissions settings for all files and subdirectories

*Modify — Users can view and modify files and file properties, including adding files to or deleting files from a directory, or file properties to or from a file.

*Read & Execute — Users can run executable files, including scripts.

*Read — Users can view files, file properties and directories.

*Write — Users can write to a file and add files to directories.

Share Permissions

Setting Share Permissions:-

*****Right click on the folder

*Go to “Properties”

*Click on the “Sharing” tab

*Click on “Advanced Sharing…”

*Click on “Permissions”

*****deny all the available permissions and click on 'apply' and click on 'ok'

<u>Here are the basic types of access permissions</u>:

Full Control — Users can add, modify, move and delete files and directories, as well as their associated properties. In addition, users can change permissions settings for all files and subdirectories.

Modify — Users can view and modify files and file properties, including adding files to or deleting files from a directory, or file properties to or from a file.

Read & Execute — Users can run executable files, including scripts.

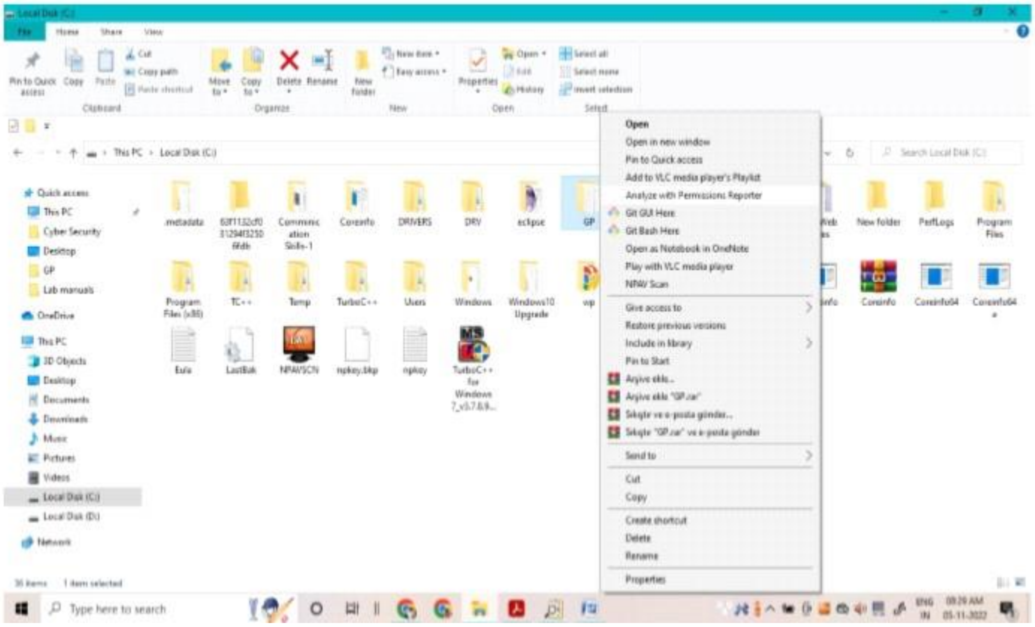
Read — Users can view files, file properties and directories.

Write — Users can write to a file and add files to directories.Share PermissionsWhen you share a folder and want to set the permissions for that folder that's a share. Essentially, share permissions determine the type of access others have to the shared folder across the network.

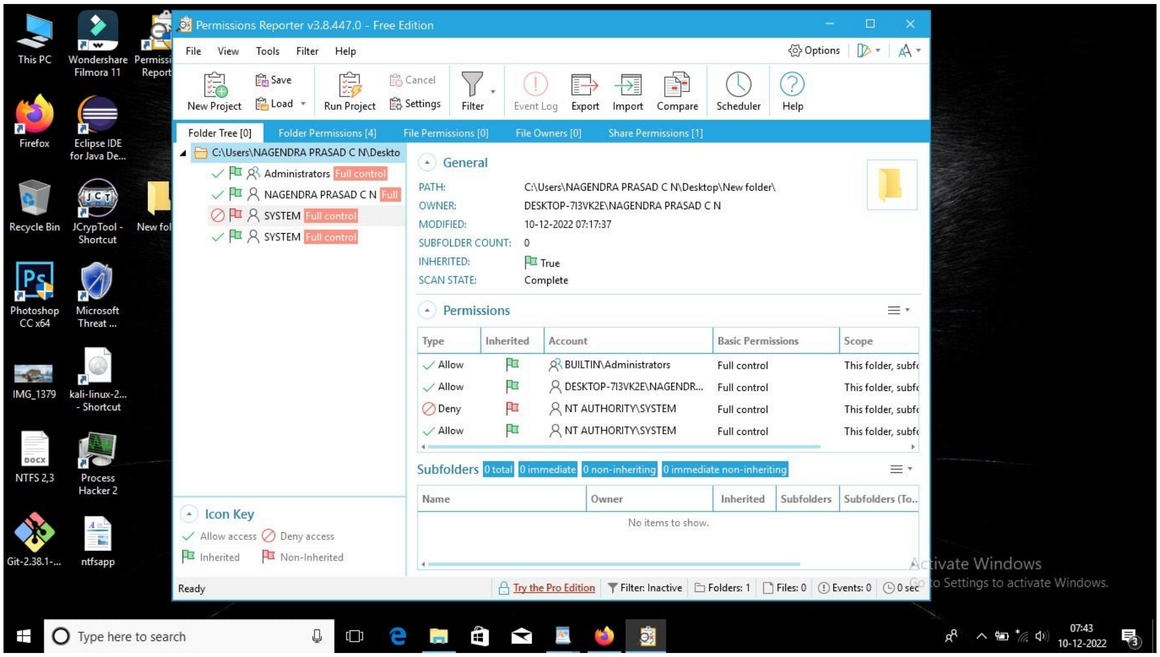
NTFS PERMISSIONS REPORTER

- The NTFS Permissions Reporter by is an excellent tool that allows you to export file and folder permissions for further reviewing.

- Once installed, you can right click on any folder in your Windows Explorer and select the "Analyze with Permissions Reporter" option. Thereafter, you'll be directed to the tool's main page for you to see the various permissions associated with the folder.



*In the bellow picture you see the deny access for the system user folder


Permissions Reporter v3.8.447.0 - Free Edition
File View Tools Filter Help
Options
New Project Save Load Run Project Cancel Settings Filter Event Log Export Import Compare Scheduler Help
Folder Tree [0] Folder Permissions [4] File Permissions [0] File Owners [0] Share Permissions [1]
Icon Key
Allow access Deny access
Inherited Non-Inherited
Ready Try the Pro Edition Filter: Inactive Folders: 1 Files: 0 Events: 0 0 sec
Activate Windows
Go to Settings to activate Windows.
Type here to search
07:43
10-12-2022

C:\Users\NAGENDRA PRASAD C N\Deskto
- Administrators Full control
- NAGENDRA PRASAD C N Full
- SYSTEM Full control
- SYSTEM Full control

General

PATH: C:\Users\NAGENDRA PRASAD C N\Desktop\New folder\
OWNER: DESKTOP-7I3VK2E\NAGENDRA PRASAD C N
MODIFIED: 10-12-2022 07:17:37
SUBFOLDER COUNT: 0
INHERITED: True
SCAN STATE: Complete

Permissions

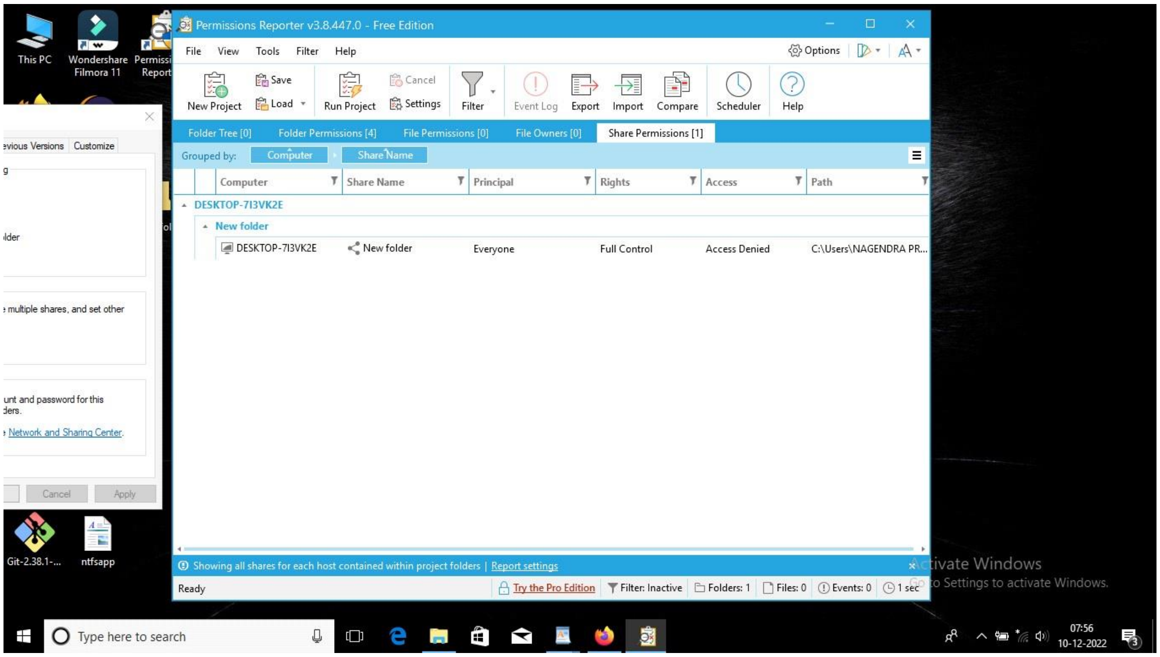
Type	Inherited	Account	Basic Permissions	Scope
✓ Allow		BUILTIN\Administrators	Full control	This folder, subf
✓ Allow		DESKTOP-7I3VK2E\NAGENDR...	Full control	This folder, subf
⊘ Deny		NT AUTHORITY\SYSTEM	Full control	This folder, subf
✓ Allow		NT AUTHORITY\SYSTEM	Full control	This folder, subf

Subfolders 0 total 0 immediate 0 non-inheriting 0 immediate non-inheriting

Name	Owner	Inherited	Subfolders	Subfolders (To...

No items to show.

*click on share permissions


Permissions Reporter v3.8.447.0 - Free Edition
File View Tools Filter Help
Options
New Project Save Load Run Project Cancel Settings Filter Event Log Export Import Compare Scheduler Help
Folder Tree [0] Folder Permissions [4] File Permissions [0] File Owners [0] Share Permissions [1]
Cancel Apply
Ready Try the Pro Edition Filter: Inactive Folders: 1 Files: 0 Events: 0 1 sec
Activate Windows
Go to Settings to activate Windows.
Type here to search
07:56
10-12-2022

Grouped by: Computer ▸ Share Name

Computer	Share Name	Principal	Rights	Access	Path
DESKTOP-7I3VK2E					
New folder					
DESKTOP-7I3VK2E	New folder	Everyone	Full Control	Access Denied	C:\Users\NAGENDRA PR...

Showing all shares for each host contained within project folders | Report settings

*you can see access denied in access coloum

*click on export to export the permission

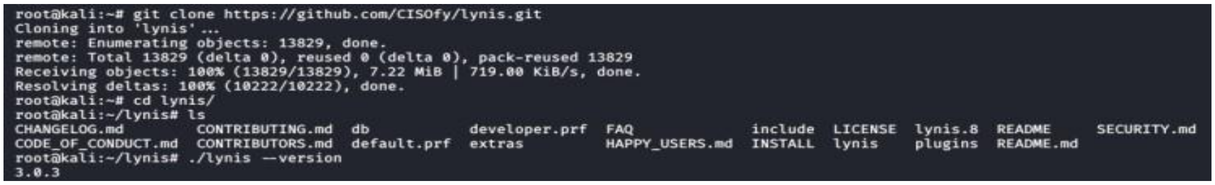
Installation and commands of lynis tool in kali linux.

LYNIS

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.

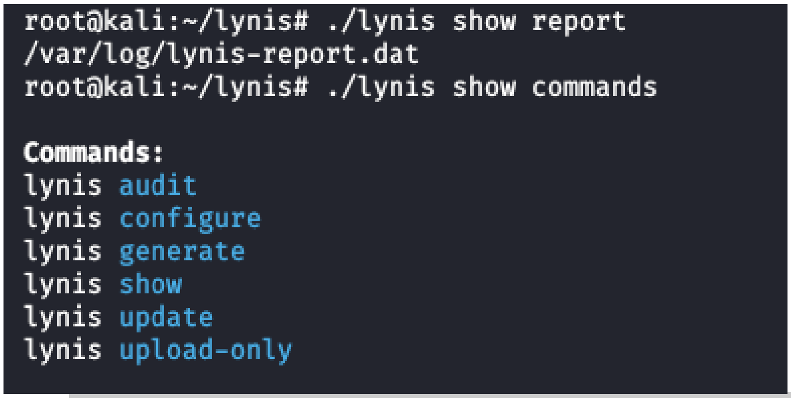
1. Go to root terminal in linux install a lynis if it is not installed using command **apt install lynis**

2. then,type **git clone https://github.com/CISOfy/lynis**



```
root@kali:~# git clone https://github.com/CISOfy/lynis.git
Cloning into 'lynis'...
remote: Enumerating objects: 13829, done.
remote: Total 13829 (delta 0), reused 0 (delta 0), pack-reused 13829
Receiving objects: 100% (13829/13829), 7.22 MiB | 719.00 KiB/s, done.
Resolving deltas: 100% (10222/10222), done.
root@kali:~# cd lynis/
root@kali:~/lynis# ls
CHANGELOG.md         CONTRIBUTING.md  db           developer.prf  FAQ             include  LICENSE  lynis.8  README     SECURITY.md
CODE_OF_CONDUCT.md   CONTRIBUTORS.md  default.prf  extras         HAPPY_USERS.md  INSTALL  lynis    plugins  README.md
root@kali:~/lynis# ./lynis —version
3.0.3
```

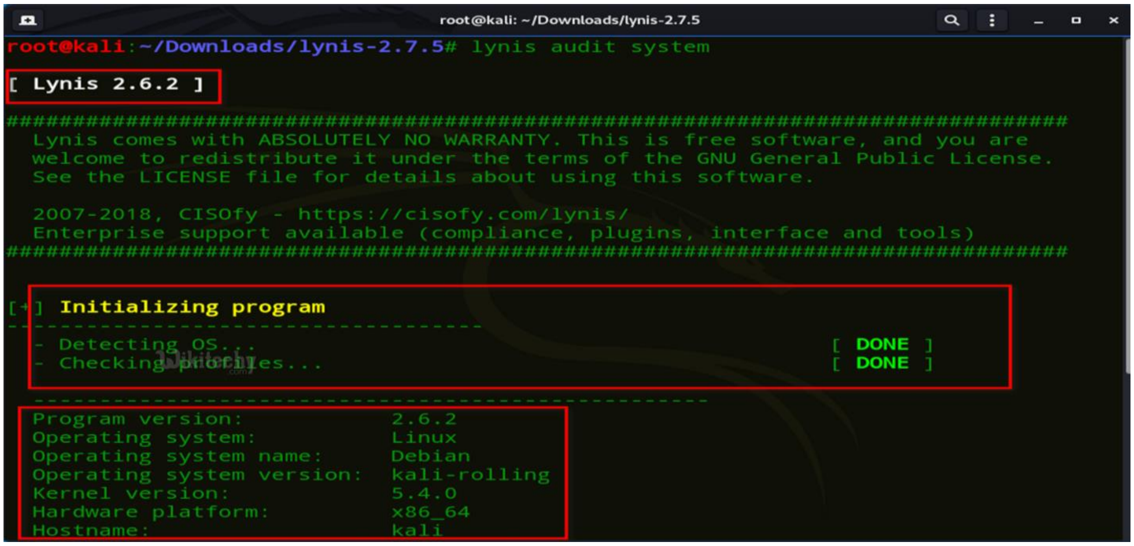
3. **$ cd lynis**   # you are in lynis
4. Type **$ ./lynis show commands**   # main commands of lynis



```
root@kali:~/lynis# ./lynis show report
/var/log/lynis-report.dat
root@kali:~/lynis# ./lynis show commands

Commands:
lynis audit
lynis configure
lynis generate
lynis show
lynis update
lynis upload-only
```

5. **$ ./lynis audit system** (or) **$ ./lynis audit system --quick**   (for faster scanning)

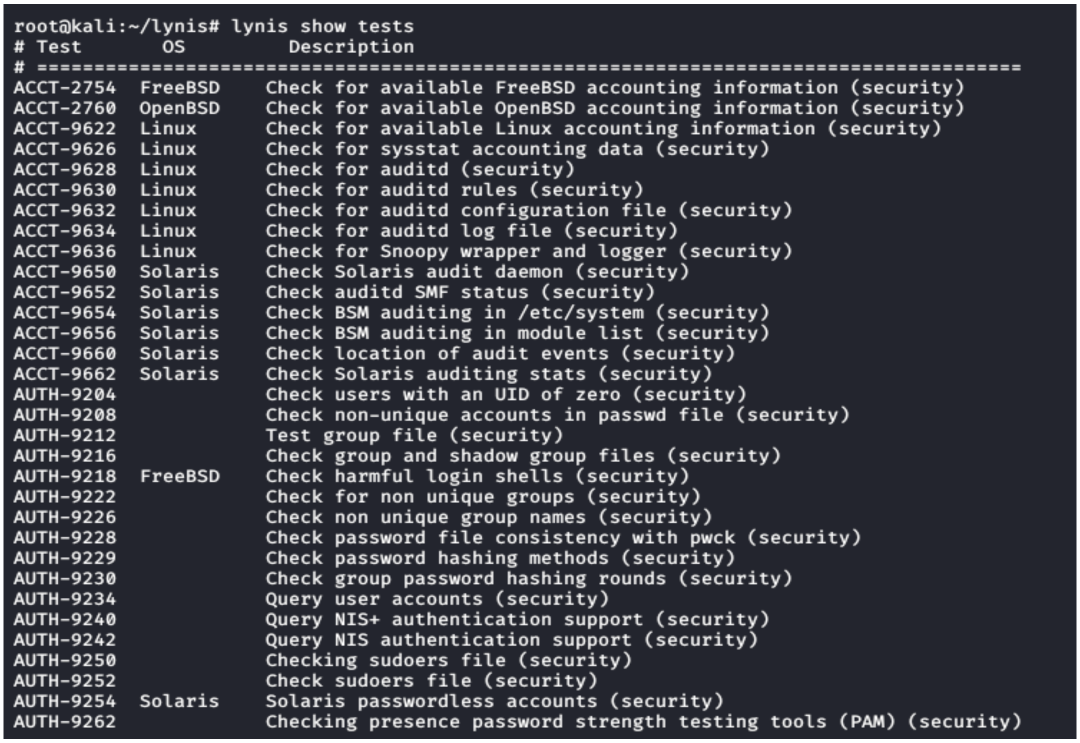
- Type lynis audit system which is used to full scanning mode, means scan your system completely.
- System auditing is started. It will display current system os, os version, hardware, etc.,



```
root@kali:~/Downloads/lynis-2.7.5# lynis audit system

[ Lynis 2.6.2 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2018, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]

  ---------------------------------------------------
  Program version:           2.6.2
  Operating system:          Linux
  Operating system name:     Debian
  Operating system version:  kali-rolling
  Kernel version:            5.4.0
  Hardware platform:         x86_64
  Hostname:                  kali
```

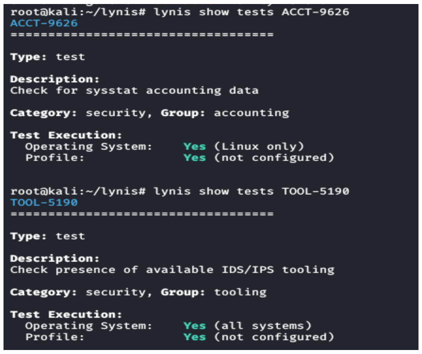
- Finally, the output files stored in **/var/log/lynis.log** which means the output files are stored in .log and .dat formats.

6. $ lynis show tests # To scan a particular test we have to list out the Test IDs



```
root@kali:~/lynis# lynis show tests
# Test         OS          Description
# ==================================================================================
ACCT-2754  FreeBSD    Check for available FreeBSD accounting information (security)
ACCT-2760  OpenBSD    Check for available OpenBSD accounting information (security)
ACCT-9622  Linux      Check for available Linux accounting information (security)
ACCT-9626  Linux      Check for sysstat accounting data (security)
ACCT-9628  Linux      Check for auditd (security)
ACCT-9630  Linux      Check for auditd rules (security)
ACCT-9632  Linux      Check for auditd configuration file (security)
ACCT-9634  Linux      Check for auditd log file (security)
ACCT-9636  Linux      Check for Snoopy wrapper and logger (security)
ACCT-9650  Solaris    Check Solaris audit daemon (security)
ACCT-9652  Solaris    Check auditd SMF status (security)
ACCT-9654  Solaris    Check BSM auditing in /etc/system (security)
ACCT-9656  Solaris    Check BSM auditing in module list (security)
ACCT-9660  Solaris    Check location of audit events (security)
ACCT-9662  Solaris    Check Solaris auditing stats (security)
AUTH-9204             Check users with an UID of zero (security)
AUTH-9208             Check non-unique accounts in passwd file (security)
AUTH-9212             Test group file (security)
AUTH-9216             Check group and shadow group files (security)
AUTH-9218  FreeBSD    Check harmful login shells (security)
AUTH-9222             Check for non unique groups (security)
AUTH-9226             Check non unique group names (security)
AUTH-9228             Check password file consistency with pwck (security)
AUTH-9229             Check password hashing methods (security)
AUTH-9230             Check group password hashing rounds (security)
AUTH-9234             Query user accounts (security)
AUTH-9240             Query NIS+ authentication support (security)
AUTH-9242             Query NIS authentication support (security)
AUTH-9250             Checking sudoers file (security)
AUTH-9252             Check sudoers file (security)
AUTH-9254  Solaris    Solaris passwordless accounts (security)
AUTH-9262             Checking presence password strength testing tools (PAM) (security)
```

7. **$ lynis show tests ACCT-9626** for sysstat accounting data # Check a particular test using the command

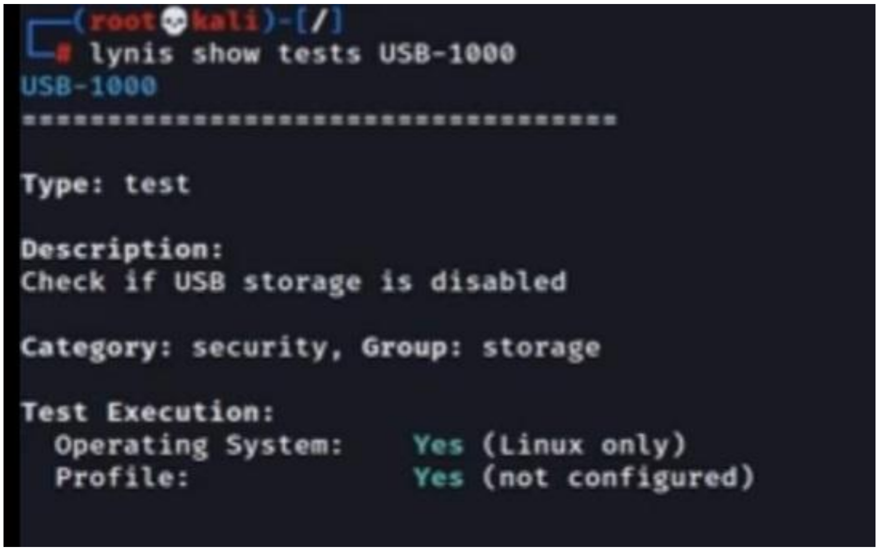


```
root@kali:~/lynis# lynis show tests ACCT-9626
ACCT-9626
===================================

Type: test

Description:
Check for sysstat accounting data

Category: security, Group: accounting

Test Execution:
  Operating System:     Yes (Linux only)
  Profile:              Yes (not configured)


root@kali:~/lynis# lynis show tests TOOL-5190
TOOL-5190
===================================

Type: test

Description:
Check presence of available IDS/IPS tooling

Category: security, Group: tooling

Test Execution:
  Operating System:     Yes (all systems)
  Profile:              Yes (not configured)
```

8. $ **lynis show tests TOOL-5190** It will scan only presence of available ids/ips tooling

9. **$ ./lynis show tests USB -1000**

- **It will check if USB storage is disabled.**



```
┌──(root💀kali)-[/]
└─# lynis show tests USB-1000
USB-1000
===================================

Type: test

Description:
Check if USB storage is disabled

Category: security, Group: storage

Test Execution:
  Operating System:     Yes (Linux only)
  Profile:              Yes (not configured)
```

SElinux

SELinux stands for S ecurity E nhanced Linux, which is an access control system that is built into the Linux kernel. It is used to enforce the resource policies that define what level of access users, programs, and services have on a system.

SELinux Operating Modes

SELinux can operate in two global modes:

- **Permissive mode**, in which permission denials are logged but not enforced.
- **Enforcing mode**, in which permissions denials are both logged and enforced.

Setting SELinux Modes SELinux runs in one of three modes

1) Disabled: The kernel uses only DAC rules for access control. SELinux does not enforce any security policy because no policy is loaded into the kernel.

2) Enforcing: The kernel denies access to users and programs unless permitted by SELinux security policy rules. All denial messages are logged as AVC (Access Vector Cache) denials. This is the default mode that enforces SELinux security policy.

3) Permissive: The kernel does not enforce security policy rules but SELinux sends denial messages to a log file. This allows you to see what actions would have been denied if SELinux were running in enforcing mode. This mode is intended to used for diagnosing the behavior of SELinux.

Commands to Execute SELinux

- To install SELinux package in linux system

```
$ Sudo apt update
```

```
$ Sudo apt install policycoreutils selinux-utils selinux-basics
```

- Next command to enable SELinux on system (execute this command in root terminal)

```
$ Sudo Selinux-activate
```

- Next, reboot system to apply changes

```
$ Reboot
```

- Next, Check the status of selinux

```
$ sestatus
```

- Next set/change SELinux to enforcing mode

```
$ sudo selinux-config-enforcing
```

- Next reboot system to apply changes

```
$ reboot
```

- Next check the status of selinux

```
$ sestatus
```

- To check mode of SELinux

```
$ getenforce
```

- To set the current mode to Enforcing:

```
$ sudo  setenforce   enforcing
```

- To set the current mode to Permissive:

```
$ sudo

$  setenforce   permissive
```

Address Space Layout Randomization

ASLR (Address Space Layout Randomization) is a memory exploitation mitigation technique used on both Linux and Windows systems.

Address space layout randomization (ASLR) is one of the computer security technique involved in preventing exploitation of memory corruption vulnerabilities(memory protection technique). It helps to ensure that the memory addresses associated with running processes on systems are not predictable, thus flaws or vulnerabilities associated with these processes will be more difficult to exploit.

0 = Disabled
1 = Conservative Randomization
2 = Full Randomization

Commands to Execute ASLR

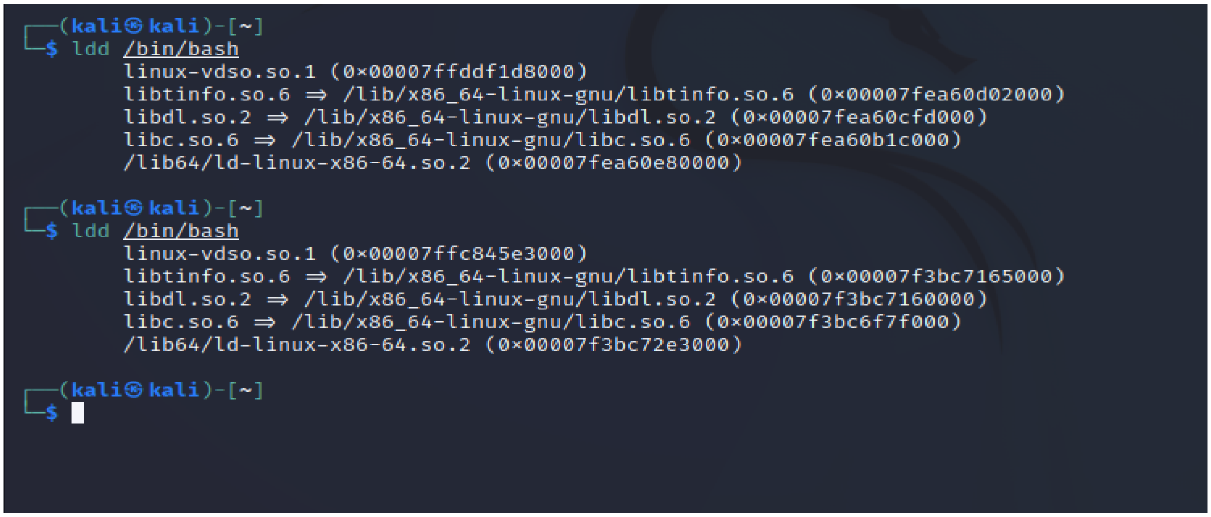
- To view current ASLR settings

  `$ cat /proc/sys/kernel/randomize_va_space`

- To see the effect of randomize

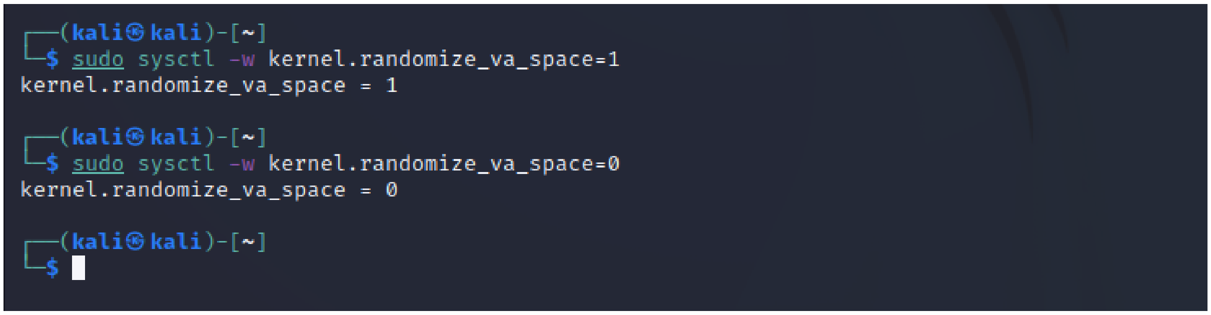
  `$ ldd /bin/bash`

  Output



```
┌──(kali㉿kali)-[~]
└─$ ldd /bin/bash
        linux-vdso.so.1 (0×00007ffddf1d8000)
        libtinfo.so.6 ⇒ /lib/x86_64-linux-gnu/libtinfo.so.6 (0×00007fea60d02000)
        libdl.so.2 ⇒ /lib/x86_64-linux-gnu/libdl.so.2 (0×00007fea60cfd000)
        libc.so.6 ⇒ /lib/x86_64-linux-gnu/libc.so.6 (0×00007fea60b1c000)
        /lib64/ld-linux-x86-64.so.2 (0×00007fea60e80000)

┌──(kali㉿kali)-[~]
└─$ ldd /bin/bash
        linux-vdso.so.1 (0×00007ffc845e3000)
        libtinfo.so.6 ⇒ /lib/x86_64-linux-gnu/libtinfo.so.6 (0×00007f3bc7165000)
        libdl.so.2 ⇒ /lib/x86_64-linux-gnu/libdl.so.2 (0×00007f3bc7160000)
        libc.so.6 ⇒ /lib/x86_64-linux-gnu/libc.so.6 (0×00007f3bc6f7f000)
        /lib64/ld-linux-x86-64.so.2 (0×00007f3bc72e3000)

┌──(kali㉿kali)-[~]
└─$ 
```

- To change the Randomization mode



```
┌──(kali㉿kali)-[~]
└─$ sudo sysctl -w kernel.randomize_va_space=1
kernel.randomize_va_space = 1

┌──(kali㉿kali)-[~]
└─$ sudo sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0

┌──(kali㉿kali)-[~]
└─$ 
```

SSH Hardening

SSH, also known as ***Secure Shell or Secure Socket Shell***, is a network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network.

Step 1: To enable SSh

```
$ systemctl enable ssh
```

Step 2: To Start service of SSh

```
$ service ssh start
```

Step 3: To check the status of SSh

```
$ Systemctl status ssh.service
```

Log Files Commands

The log files generated in a Linux environment can typically be classified into fourdifferent categories:

- Application Logs
- Event Logs
- Service Logs
- System Log

Linux provides a centralized repository of log files that can be located under the **/var/log** directory.

1. In root terminal go to log directory

```
 $ cd  /var/log
```

2. To Show general messages and info regarding the system.

```
$ cat syslog
```

3. To Show system authorization information, including user logins authentication machinsm that were used.

```
$ cat auth.log
```

4. Kern.log stores Kernel logs and warning data.

```
$ cat kern.log        (or)      cat /var/log/kern.log
```

5.maillog stores mail server logs, handy for postfix, smtpd, or email-related services info running on your server.

```
 $ cat maillog        (or)      cat /var/log/mail.log
```

6.to see text files that include information about all the requests processed by the Apache server and error log directory

```
$ cat httpd        (or)      cat /var/log/httpd
```

7.boot.log is a repository of all information related to booting and any messages logged during startup.

```
$ cat boot.log        (or)      cat /var/log/boot.log
```

8.wtmp is a file containing a history of all logins and logouts.

```
$ cat wtmp        (or)      cat /var/log/wtmp
```

9.To show information related to authentication and authorization privileges.

```
$ cat secure        (or)      cat /var/log/secure
```

Logrotation

Log rotate takes care of automatic rotation and compression of growing log files to ensure that saved on the system's available disk space.

1.To see how the logrotate configured, type

```
$ cat /etc/logrotate.conf
```

2.Most of the services (Apache webserver, postgreSQL,

MySql, KDE desktop manager etc.) installed on your system create a configuration file for logrotate in logrotate.d directory.

```
$ ls -l /etc/logrotate.d
```

3.you can also see what is there inside the configuration file

```
$cat /etc/logrotate.d/apt
```