Return Oriented Programming (ROP)

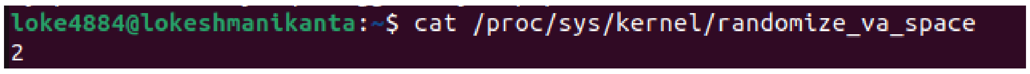
Analyzing Return Oriented Programming (ROP) attacks on Ubuntu or any other Linux-based system involves understanding the system's security mechanisms, identifying vulnerabilities, and implementing mitigations.

Address Space Layout Randomization (ASLR):

ASLR works by randomizing the memory addresses where system executables and shared libraries are loaded, making it more challenging for attackers to predict the location of specific code or gadgets. This randomness adds a layer of defense against exploit techniques like Return Oriented Programming (ROP).

Current ASLR status :

cat /proc/sys/kernel/ randomize_va_space



```
loke4884@lokeshmanikanta:~$ cat /proc/sys/kernel/randomize_va_space
2
```

0: No randomization. Everything is static.

1: Conservative randomization. Shared libraries, stack, mmap(), VDSO, and heap are randomized.

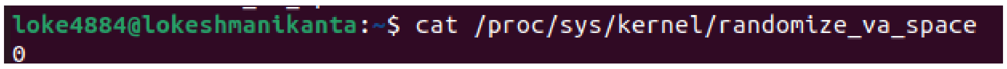
2: Full randomization. In addition to elements randomized in conservative randomization, memory managed through brk() is also randomized.

if you are having randomize_va_space as 0 or 1 you can manually configure to 2 for higher security

to set the system to use conservative randomization

for ex:

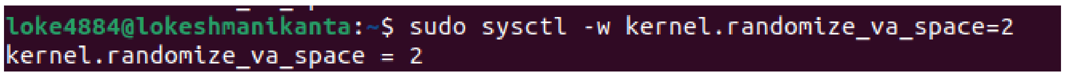
cat /proc/sys/kernel/ randomize_va_space



```
loke4884@lokeshmanikanta:~$ cat /proc/sys/kernel/randomize_va_space
0
```

To temporarily get secured randomization

sudo sysctl -w kernel.randomize_va_space=2



```
loke4884@lokeshmanikanta:~$ sudo sysctl -w kernel.randomize_va_space=2
kernel.randomize_va_space = 2
```

sysctl -w are temporary and will be lost after a system reboot

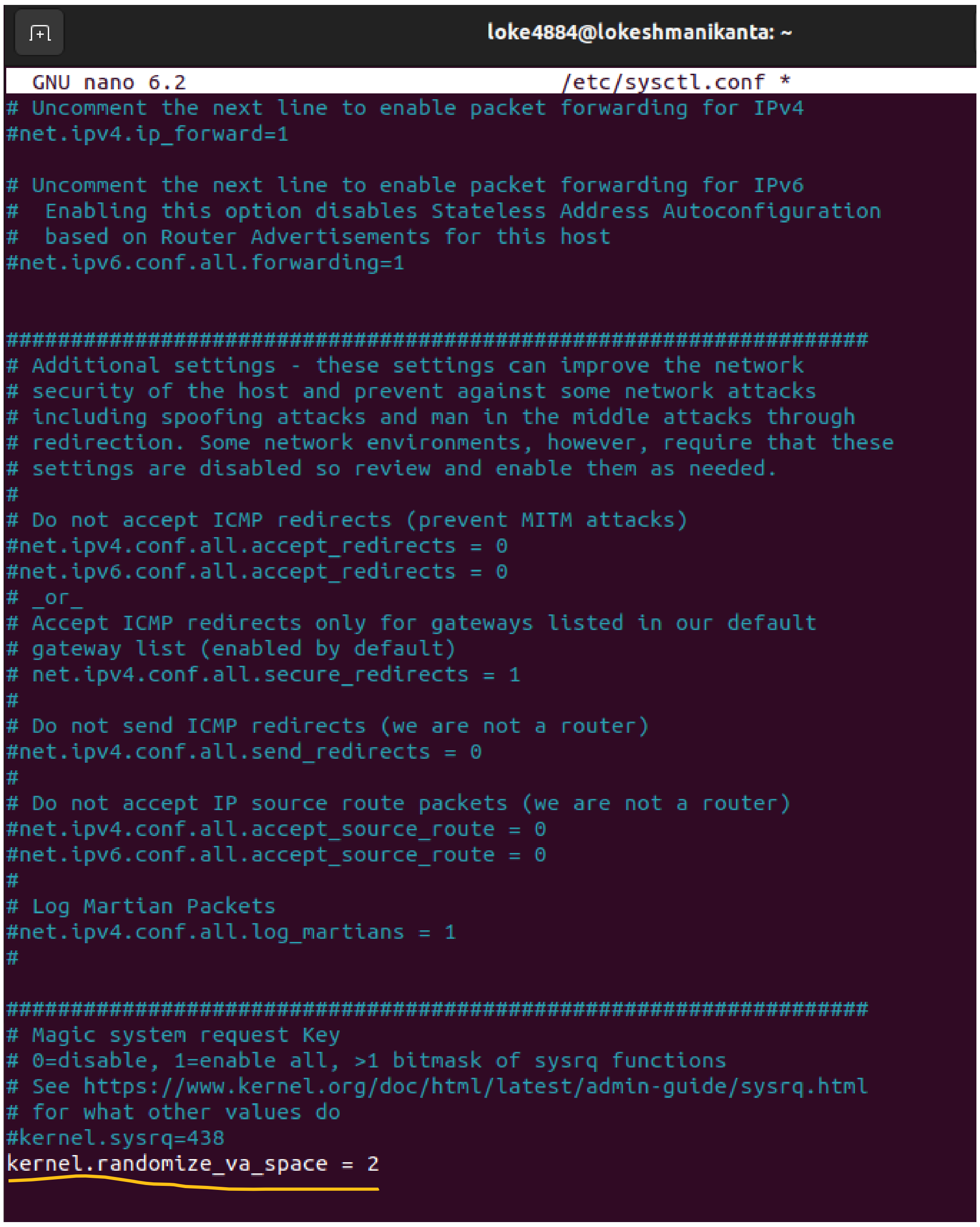
To make the changes persistent across reboots

Then edit the sysctl configuration file.

sudo nano /etc/sysctl.conf

```
loke4884@lokeshmanikanta:~$ sudo nano /etc/sysctl.conf
```

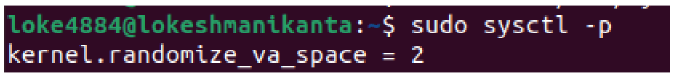
Add kernel.randomize_va_space = 2



```
  GNU nano 6.2                          /etc/sysctl.conf *
# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1


###################################################################
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network environments, however, require that these
# settings are disabled so review and enable them as needed.
#
# Do not accept ICMP redirects (prevent MITM attacks)
#net.ipv4.conf.all.accept_redirects = 0
#net.ipv6.conf.all.accept_redirects = 0
# _or_
# Accept ICMP redirects only for gateways listed in our default
# gateway list (enabled by default)
# net.ipv4.conf.all.secure_redirects = 1
#
# Do not send ICMP redirects (we are not a router)
#net.ipv4.conf.all.send_redirects = 0
#
# Do not accept IP source route packets (we are not a router)
#net.ipv4.conf.all.accept_source_route = 0
#net.ipv6.conf.all.accept_source_route = 0
#
# Log Martian Packets
#net.ipv4.conf.all.log_martians = 1
#

###################################################################
# Magic system request Key
# 0=disable, 1=enable all, >1 bitmask of sysrq functions
# See https://www.kernel.org/doc/html/latest/admin-guide/sysrq.html
# for what other values do
#kernel.sysrq=438
kernel.randomize_va_space = 2
```

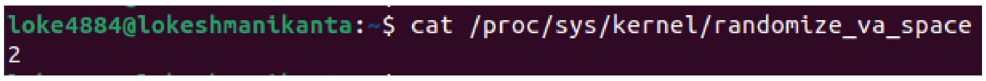
To sysctl configuration file for following changes

sudo sysctl -p



```
loke4884@lokeshmanikanta:~$ sudo sysctl -p
kernel.randomize_va_space = 2
```

cat /proc/sys/kernel/ randomize_va_space



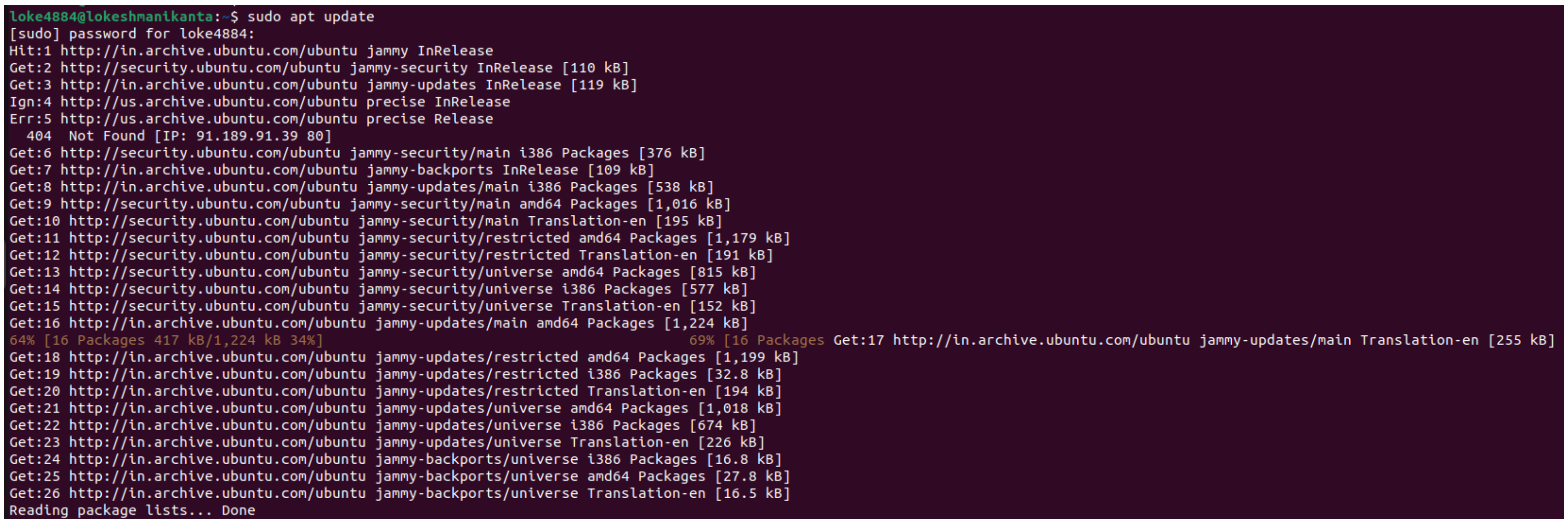
```
loke4884@lokeshmanikanta:~$ cat /proc/sys/kernel/randomize_va_space
2
```

Vulnerability Analysis:

Vulnerability analysis for Return Oriented Programming (ROP) on Ubuntu involves assessing the security posture of the system and identifying potential weaknesses that could be exploited by ROP attacks.

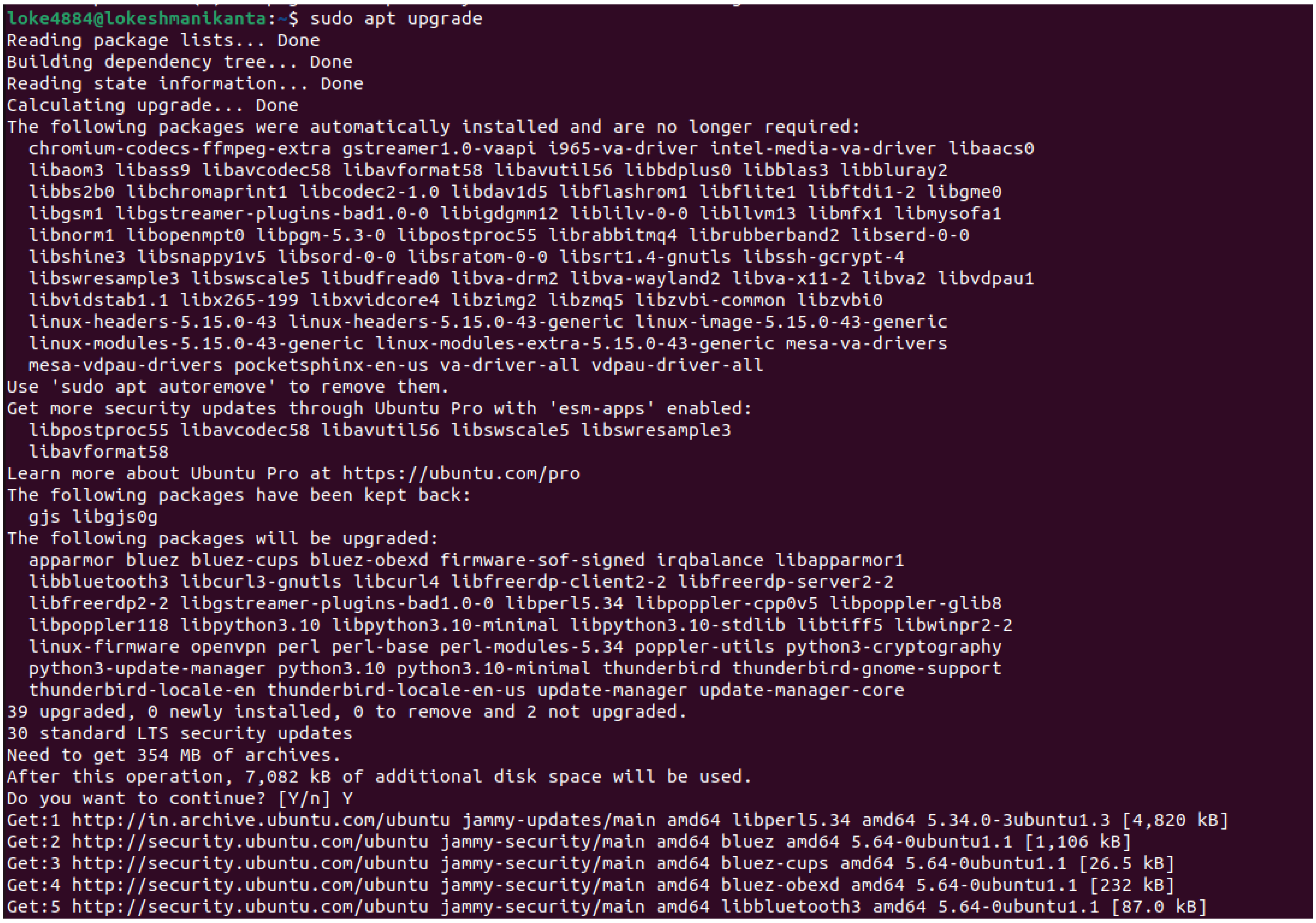
System Patching and Updates: Ensure that the Ubuntu system is regularly updated with the latest security patches. Vulnerabilities in the operating system and installed software are often patched through updates.

sudo apt update



```
loke4884@lokeshmanikanta:~$ sudo apt update
[sudo] password for loke4884:
Hit:1 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Ign:4 http://us.archive.ubuntu.com/ubuntu precise InRelease
Err:5 http://us.archive.ubuntu.com/ubuntu precise Release
  404  Not Found [IP: 91.189.91.39 80]
Get:6 http://security.ubuntu.com/ubuntu jammy-security/main i386 Packages [376 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease [109 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [538 kB]
Get:9 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1,016 kB]
Get:10 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [195 kB]
Get:11 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [1,179 kB]
Get:12 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [191 kB]
Get:13 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [815 kB]
Get:14 http://security.ubuntu.com/ubuntu jammy-security/universe i386 Packages [577 kB]
Get:15 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [152 kB]
Get:16 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1,224 kB]
64% [16 Packages 417 kB/1,224 kB 34%]                                         69% [16 Packages Get:17 http://in.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [255 kB]
Get:18 http://in.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [1,199 kB]
Get:19 http://in.archive.ubuntu.com/ubuntu jammy-updates/restricted i386 Packages [32.8 kB]
Get:20 http://in.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [194 kB]
Get:21 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1,018 kB]
Get:22 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe i386 Packages [674 kB]
Get:23 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [226 kB]
Get:24 http://in.archive.ubuntu.com/ubuntu jammy-backports/universe i386 Packages [16.8 kB]
Get:25 http://in.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [27.8 kB]
Get:26 http://in.archive.ubuntu.com/ubuntu jammy-backports/universe Translation-en [16.5 kB]
Reading package lists... Done
```

sudo apt upgrade

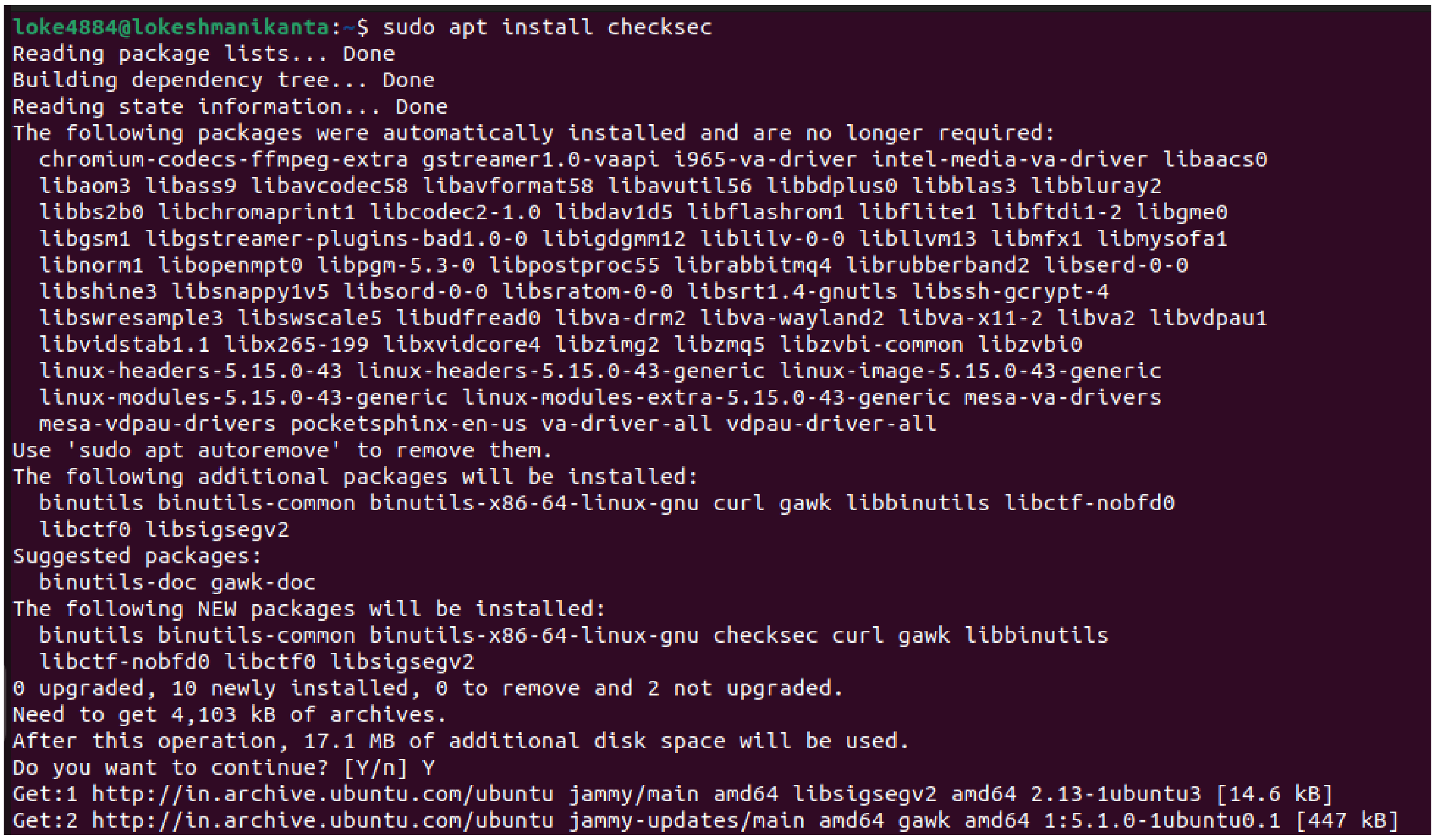


```
loke4884@lokeshmanikanta:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver intel-media-va-driver libaacs0
  libaom3 libass9 libavcodec58 libavformat58 libavutil56 libbdplus0 libblas3 libbluray2
  libbs2b0 libchromaprint1 libcodec2-1.0 libdav1d5 libflashrom1 libflite1 libftdi1-2 libgme0
  libgsm1 libgstreamer-plugins-bad1.0-0 libigdgmm12 liblilv-0-0 libllvm13 libmfx1 libmysofa1
  libnorm1 libopenmpt0 libpgm-5.3-0 libpostproc55 librabbitmq4 librubberband2 libserd-0-0
  libshine3 libsnappy1v5 libsord-0-0 libsratom-0-0 libsrt1.4-gnutls libssh-gcrypt-4
  libswresample3 libswscale5 libudfread0 libva-drm2 libva-wayland2 libva-x11-2 libva2 libvdpau1
  libvidstab1.1 libx265-199 libxvidcore4 libzimg2 libzmq5 libzvbi-common libzvbi0
  linux-headers-5.15.0-43 linux-headers-5.15.0-43-generic linux-image-5.15.0-43-generic
  linux-modules-5.15.0-43-generic linux-modules-extra-5.15.0-43-generic mesa-va-drivers
  mesa-vdpau-drivers pocketsphinx-en-us va-driver-all vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
Get more security updates through Ubuntu Pro with 'esm-apps' enabled:
  libpostproc55 libavcodec58 libavutil56 libswscale5 libswresample3
  libavformat58
Learn more about Ubuntu Pro at https://ubuntu.com/pro
The following packages have been kept back:
  gjs libgjs0g
The following packages will be upgraded:
  apparmor bluez bluez-cups bluez-obexd firmware-sof-signed irqbalance libapparmor1
  libbluetooth3 libcurl3-gnutls libcurl4 libfreerdp-client2-2 libfreerdp-server2-2
  libfreerdp2-2 libgstreamer-plugins-bad1.0-0 libperl5.34 libpoppler-cpp0v5 libpoppler-glib8
  libpoppler118 libpython3.10 libpython3.10-minimal libpython3.10-stdlib libtiff5 libwinpr2-2
  linux-firmware openvpn perl perl-base perl-modules-5.34 poppler-utils python3-cryptography
  python3-update-manager python3.10 python3.10-minimal thunderbird thunderbird-gnome-support
  thunderbird-locale-en thunderbird-locale-en-us update-manager update-manager-core
39 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
30 standard LTS security updates
Need to get 354 MB of archives.
After this operation, 7,082 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libperl5.34 amd64 5.34.0-3ubuntu1.3 [4,820 kB]
Get:2 http://security.ubuntu.com/ubuntu jammy-security/main amd64 bluez amd64 5.64-0ubuntu1.1 [1,106 kB]
Get:3 http://security.ubuntu.com/ubuntu jammy-security/main amd64 bluez-cups amd64 5.64-0ubuntu1.1 [26.5 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security/main amd64 bluez-obexd amd64 5.64-0ubuntu1.1 [232 kB]
Get:5 http://security.ubuntu.com/ubuntu jammy-security/main amd64 libbluetooth3 amd64 5.64-0ubuntu1.1 [87.0 kB]
```

Binary Protections: Check if binaries are compiled with security features like Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP/NX bit).

If checksec is not installed

sudo apt install checksec

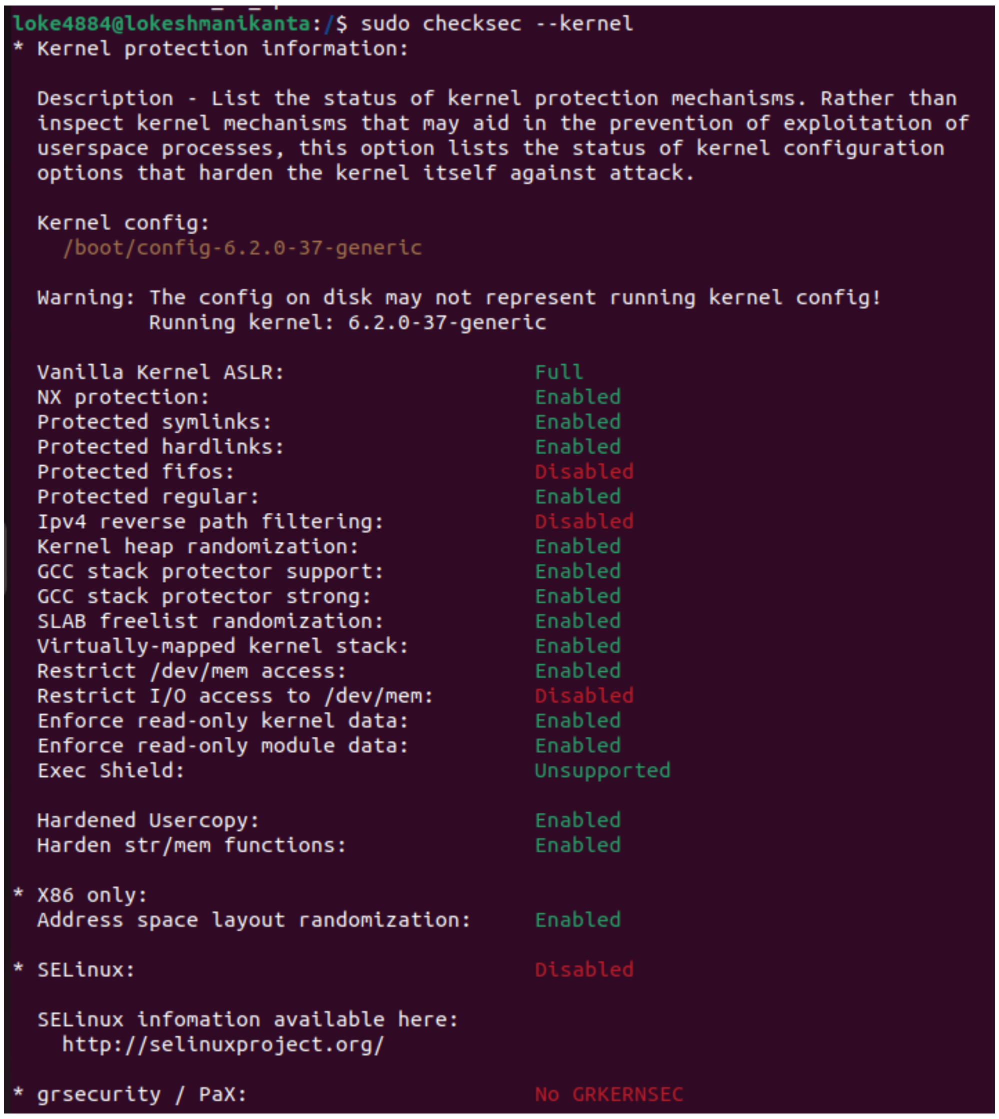


```
loke4884@lokeshmanikanta:~$ sudo apt install checksec
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver intel-media-va-driver libaacs0
  libaom3 libass9 libavcodec58 libavformat58 libavutil56 libbdplus0 libblas3 libbluray2
  libbs2b0 libchromaprint1 libcodec2-1.0 libdav1d5 libflashrom1 libflite1 libftdi1-2 libgme0
  libgsm1 libgstreamer-plugins-bad1.0-0 libigdgmm12 liblilv-0-0 libllvm13 libmfx1 libmysofa1
  libnorm1 libopenmpt0 libpgm-5.3-0 libpostproc55 librabbitmq4 librubberband2 libserd-0-0
  libshine3 libsnappy1v5 libsord-0-0 libsratom-0-0 libsrt1.4-gnutls libssh-gcrypt-4
  libswresample3 libswscale5 libudfread0 libva-drm2 libva-wayland2 libva-x11-2 libva2 libvdpau1
  libvidstab1.1 libx265-199 libxvidcore4 libzimg2 libzmq5 libzvbi-common libzvbi0
  linux-headers-5.15.0-43 linux-headers-5.15.0-43-generic linux-image-5.15.0-43-generic
  linux-modules-5.15.0-43-generic linux-modules-extra-5.15.0-43-generic mesa-va-drivers
  mesa-vdpau-drivers pocketsphinx-en-us va-driver-all vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu curl gawk libbinutils libctf-nobfd0
  libctf0 libsigsegv2
Suggested packages:
  binutils-doc gawk-doc
The following NEW packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu checksec curl gawk libbinutils
  libctf-nobfd0 libctf0 libsigsegv2
0 upgraded, 10 newly installed, 0 to remove and 2 not upgraded.
Need to get 4,103 kB of archives.
After this operation, 17.1 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 libsigsegv2 amd64 2.13-1ubuntu3 [14.6 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 gawk amd64 1:5.1.0-1ubuntu0.1 [447 kB]
```

To check centain security features enabled or not

The checksec --kernel command checks various security features and configurations related to the Linux kernel. This includes settings such as ASLR (Address Space Layout Randomization), NX (No-Execute) bit, and other kernel-level security parameters.

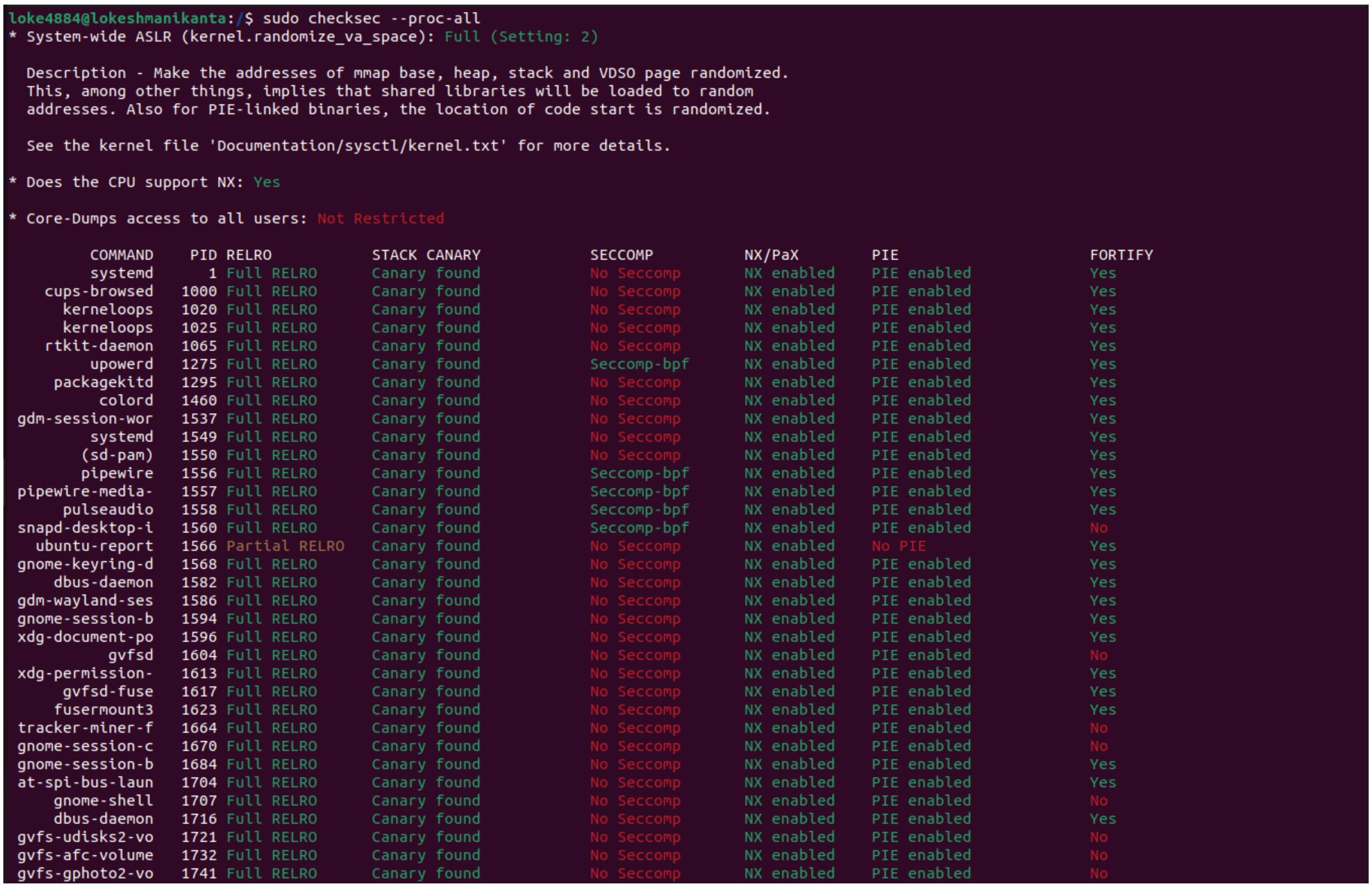
sudo checksec –kernel



```
loke4884@lokeshmanikanta:/$ sudo checksec --kernel
* Kernel protection information:

  Description - List the status of kernel protection mechanisms. Rather than
  inspect kernel mechanisms that may aid in the prevention of exploitation of
  userspace processes, this option lists the status of kernel configuration
  options that harden the kernel itself against attack.

  Kernel config:
    /boot/config-6.2.0-37-generic

  Warning: The config on disk may not represent running kernel config!
           Running kernel: 6.2.0-37-generic

  Vanilla Kernel ASLR:                    Full
  NX protection:                          Enabled
  Protected symlinks:                     Enabled
  Protected hardlinks:                    Enabled
  Protected fifos:                        Disabled
  Protected regular:                      Enabled
  Ipv4 reverse path filtering:            Disabled
  Kernel heap randomization:              Enabled
  GCC stack protector support:            Enabled
  GCC stack protector strong:             Enabled
  SLAB freelist randomization:            Enabled
  Virtually-mapped kernel stack:          Enabled
  Restrict /dev/mem access:               Enabled
  Restrict I/O access to /dev/mem:        Disabled
  Enforce read-only kernel data:          Enabled
  Enforce read-only module data:          Enabled
  Exec Shield:                            Unsupported

  Hardened Usercopy:                      Enabled
  Harden str/mem functions:               Enabled

* X86 only:
  Address space layout randomization:     Enabled

* SELinux:                                Disabled

  SELinux infomation available here:
    http://selinuxproject.org/

* grsecurity / PaX:                       No GRKERNSEC
```

The command checks the security features and settings for all active processes on the system.

checksec --proc-all



```
loke4884@lokeshmanikanta:/$ sudo checksec --proc-all
* System-wide ASLR (kernel.randomize_va_space): Full (Setting: 2)

  Description - Make the addresses of mmap base, heap, stack and VDSO page randomized.
  This, among other things, implies that shared libraries will be loaded to random
  addresses. Also for PIE-linked binaries, the location of code start is randomized.

  See the kernel file 'Documentation/sysctl/kernel.txt' for more details.

* Does the CPU support NX: Yes

* Core-Dumps access to all users: Not Restricted

        COMMAND   PID RELRO           STACK CANARY             SECCOMP          NX/PaX        PIE                      FORTIFY
        systemd     1 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              Yes
   cups-browsed  1000 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              Yes
     kerneloops  1020 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              Yes
     kerneloops  1025 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              Yes
   rtkit-daemon  1065 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              Yes
        upowerd  1275 Full RELRO      Canary found             Seccomp-bpf      NX enabled    PIE enabled              Yes
    packagekitd  1295 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              Yes
         colord  1460 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              Yes
gdm-session-wor  1537 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              Yes
        systemd  1549 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              Yes
       (sd-pam)  1550 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              Yes
       pipewire  1556 Full RELRO      Canary found             Seccomp-bpf      NX enabled    PIE enabled              Yes
pipewire-media-  1557 Full RELRO      Canary found             Seccomp-bpf      NX enabled    PIE enabled              Yes
     pulseaudio  1558 Full RELRO      Canary found             Seccomp-bpf      NX enabled    PIE enabled              Yes
snapd-desktop-i  1560 Full RELRO      Canary found             Seccomp-bpf      NX enabled    PIE enabled              No
  ubuntu-report  1566 Partial RELRO   Canary found             No Seccomp       NX enabled    No PIE                   Yes
gnome-keyring-d  1568 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              Yes
    dbus-daemon  1582 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              Yes
gdm-wayland-ses  1586 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              Yes
gnome-session-b  1594 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              Yes
xdg-document-po  1596 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              Yes
          gvfsd  1604 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              No
xdg-permission-  1613 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              Yes
     gvfsd-fuse  1617 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              Yes
    fusermount3  1623 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              Yes
tracker-miner-f  1664 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              No
gnome-session-c  1670 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              No
gnome-session-b  1684 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              Yes
at-spi-bus-laun  1704 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              Yes
    gnome-shell  1707 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              No
    dbus-daemon  1716 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              Yes
gvfs-udisks2-vo  1721 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              No
gvfs-afc-volume  1732 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              No
gvfs-gphoto2-vo  1741 Full RELRO      Canary found             No Seccomp       NX enabled    PIE enabled              No
```

Interpreting the Output:

Canary found: Indicates whether a stack canary is present in the process.

NX disabled: Indicates whether the No-Execute (NX) bit is disabled. This is related to Data Execution Prevention (DEP).

No PIE: Indicates whether the process is a Position Independent Executable (PIE).

No RPATH, No RUNPATH: Indicates the absence of specific dynamic linker search paths.

FORTIFY: Indicates whether FORTIFY_SOURCE protections are present.

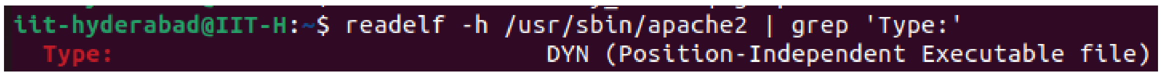
Fortified, Fortifiable: Relates to compile-time and runtime buffer overflow protections.

Position Independent Executables (PIE):

Check if a Binary is Position Independent:

Look for "DYN (Shared object file)" in the output. If it's present, the binary is position independent.

readelf -h <binary_name> | grep 'Type:'

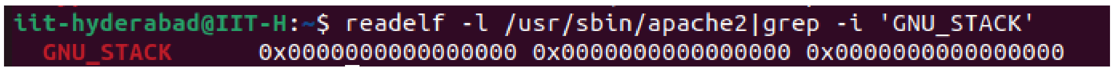


```
iit-hyderabad@IIT-H:~$ readelf -h /usr/sbin/apache2 | grep 'Type:'
  Type:                              DYN (Position-Independent Executable file)
```

Check if PIE is Enabled in a Binary:

Look for "GNU_STACK" and check if the "RWE" flags are present, indicating that the binary supports execution from a writable and executable stack.

readelf -l <binary_name> | grep -i 'GNU_STACK'



```
iit-hyderabad@IIT-H:~$ readelf -l /usr/sbin/apache2|grep -i 'GNU_STACK'
  GNU_STACK      0x0000000000000000 0x0000000000000000 0x0000000000000000
```