```
Audit Report - Tue Nov 19 04:55:27 PM IST 2024
-------------------------------------------------------------------------------
System Hostname: abhi-IdeaPad-Gaming-3-15IHU6
------------------------------------------------------------------------------
Current User: root
------------------------------------------------------------------------------
Current Directory: /home/abhi/Downloads/OS/backend
------------------------------------------------------------------------------
System Uptime: up 1 hour, 20 minutes
------------------------------------------------------------------------------
System Load Average: 0.65, 0.69, 0.72
-------------------------------------------------------------------------------
Currently logged in users:
abhi     tty2         2024-11-19 15:36 (tty2)
abhi     pts/3        2024-11-19 16:55
-----------------------------------------------------------------------------
Last logged in users (last 10):
abhi     tty2         tty2             Tue Nov 19 15:36   still logged in
reboot   system boot  6.8.0-48-generic Tue Nov 19 21:05   still running
abhi     tty2         tty2             Tue Nov 19 13:46 - down   (01:04)
reboot   system boot  6.8.0-48-generic Tue Nov 19 19:15 - 14:51  (-4:24)
abhi     tty2         tty2             Sun Nov 17 00:45 - down   (00:00)
abhi     tty2         tty2             Sat Nov 16 22:51 - 00:45  (01:53)
reboot   system boot  6.8.0-48-generic Sat Nov 16 22:50 - 00:46  (01:55)
abhi     tty2         tty2             Sat Nov 16 22:45 - down   (00:00)
reboot   system boot  6.8.0-48-generic Sat Nov 16 22:43 - 22:45  (00:02)
abhi     tty2         tty2             Sat Nov 16 21:52 - down   (00:50)

wtmp begins Tue Aug 20 17:22:01 2024
-----------------------------------------------------------------------------
Last commands executed (last 15):
-----------------------------------------------------------------------------
Recent Activity (top 10 users by activity):
abhi     tty2     tty2             15:36     ?     0.00s  0.00s /usr/libexec/gno
me-session-binary --session=ubuntu
abhi     pts/3    -                16:55    0.00s  0.00s  0.00s sudo -S /home/ab
hi/Downloads/OS/backend/scripts/LinuxAudit.sh
-------------------------------------------------------------------------------
Disk Space Usage:
Filesystem     1K-blocks     Used Available Use% Mounted on
tmpfs            1615568     2472   1613096   1% /run
/dev/sda3       47745772 13663524  31624444  31% /
tmpfs            8077840    26388   8051452   1% /dev/shm
tmpfs               5120        4      5116   1% /run/lock
efivarfs             184      113        67  64% /sys/firmware/efi/efivars
/dev/nvme0n1p1     98304    47620     50684  49% /boot/efi
/dev/sda4      102540216  2124516  95160740   3% /home
tmpfs            1615568      124   1615444   1% /run/user/1000
-------------------------------------------------------------------------------
Memory Usage:
               total        used        free      shared  buff/cache   available
Mem:            15Gi       3.6Gi       8.1Gi       1.0Gi       3.6Gi        10Gi
Swap:             0B          0B          0B
-------------------------------------------------------------------------------
Top 10 Processes by CPU usage:
    PID COMMAND         %CPU
   2999 code             9.8
   4137 firefox          6.3
   1712 gnome-shell      5.4
  13302 Isolated Web Co  4.3
   3186 code             3.2
   2732 code             2.5
```

```
  13208 Isolated Web Co  1.3
   2438 code             1.2
   3677 node             1.0
   2530 Xwayland         0.7
-------------------------------------------------------------------------------
Top 10 Processes by Memory usage:
    PID COMMAND         %MEM
   4137 firefox          3.2
   2999 code             2.8
  13208 Isolated Web Co  2.5
   3677 node             2.5
   1712 gnome-shell      2.0
  15711 file:// Content  1.5
  13302 Isolated Web Co  1.5
   3186 code             1.3
   4380 Isolated Web Co  1.2
   2438 code             1.2
-------------------------------------------------------------------------------
Network Interfaces and Addresses:
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp3s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOW
N group default qlen 1000
    link/ether e4:a8:df:d2:4f:79 brd ff:ff:ff:ff:ff:ff
3: wlp0s20f3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
group default qlen 1000
    link/ether f8:9e:94:f2:72:6d brd ff:ff:ff:ff:ff:ff
    inet 172.31.110.90/18 brd 172.31.127.255 scope global dynamic noprefixroute
wlp0s20f3
       valid_lft 81930sec preferred_lft 81930sec
    inet6 fe80::17b8:1412:5142:f1d1/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
-------------------------------------------------------------------------------
MAC Addresses:
e4:a8:df:d2:4f:79
f8:9e:94:f2:72:6d
-------------------------------------------------------------------------------
IP Address and loopback address:
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
    inet 172.31.110.90/18 brd 172.31.127.255 scope global dynamic noprefixroute
wlp0s20f3
    inet6 fe80::17b8:1412:5142:f1d1/64 scope link noprefixroute
-------------------------------------------------------------------------------
Operating System Information:
PRETTY_NAME="Ubuntu 22.04.5 LTS"
NAME="Ubuntu"
VERSION_ID="22.04"
VERSION="22.04.5 LTS (Jammy Jellyfish)"
VERSION_CODENAME=jammy
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-poli
cy"
```

```
UBUNTU_CODENAME=jammy
--------------------------------------------------------------------------------
Network Traffic Report
--------------------------------------------------------------------------------
Active Connections (netstat):
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3000            0.0.0.0:*               LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 :::3001                 :::*                    LISTEN
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp        0      0 0.0.0.0:35427           0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp6       0      0 :::42085                :::*
udp6       0      0 :::5353                 :::*
--------------------------------------------------------------------------------
Socket Statistics (ss):
Netid State  Recv-Q Send-Q Local Address:Port  Peer Address:PortProcess
udp   UNCONN 0      0      127.0.0.53%lo:53         0.0.0.0:*
udp   UNCONN 0      0            0.0.0.0:35427      0.0.0.0:*
udp   UNCONN 0      0            0.0.0.0:5353       0.0.0.0:*
udp   UNCONN 0      0               [::]:42085         [::]:*
udp   UNCONN 0      0               [::]:5353          [::]:*
tcp   LISTEN 0      4096   127.0.0.53%lo:53         0.0.0.0:*
tcp   LISTEN 0      128        127.0.0.1:631        0.0.0.0:*
tcp   LISTEN 0      511          0.0.0.0:3000       0.0.0.0:*
tcp   LISTEN 0      128            [::1]:631           [::]:*
tcp   LISTEN 0      511                *:3001             *:*
--------------------------------------------------------------------------------
Active and Failed Services (systemd):
  UNIT LOAD ACTIVE SUB DESCRIPTION
0 loaded units listed.
--------------------------------------------------------------------------------
Sudoers File (Users with Sudo Access):
abhi
--------------------------------------------------------------------------------
System Uptime (from uptime command):
 16:55:27 up  1:20,  2 users,  load average: 0.65, 0.69, 0.72
--------------------------------------------------------------------------------
Status of All Services (service --status-all):
 [ + ]  acpid
 [ + ]  apparmor
 [ + ]  apport
 [ + ]  avahi-daemon
 [ + ]  bluetooth
 [ + ]  cron
 [ + ]  cups
 [ + ]  cups-browsed
 [ + ]  dbus
 [ + ]  gdm3
 [ + ]  irqbalance
 [ + ]  kerneloops
 [ + ]  kmod
 [ + ]  openvpn
 [ + ]  plymouth-log
 [ + ]  procps
 [ + ]  udev
 [ + ]  ufw
 [ + ]  unattended-upgrades
--------------------------------------------------------------------------------
```

```
Netstat (Active Network Connections):
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
822/systemd-resolve
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
1023/cupsd
tcp        0      0 0.0.0.0:3000            0.0.0.0:*               LISTEN
3677/node
tcp        0      0 172.31.110.90:42128     172.64.155.209:443      TIME_WAIT
-
tcp        0      0 127.0.0.1:3000          127.0.0.1:45738         ESTABLISHED
3677/node
tcp        0      0 127.0.0.1:45738         127.0.0.1:3000          ESTABLISHED
4137/firefox
tcp        0      0 172.31.110.90:46906     163.70.145.60:443       ESTABLISHED
4137/firefox
tcp        0      0 172.31.110.90:59462     34.107.243.93:443       ESTABLISHED
4137/firefox
tcp        0      0 172.31.110.90:57218     157.240.198.60:443      ESTABLISHED
4137/firefox
tcp        0      0 172.31.110.90:39652     172.64.155.209:443      TIME_WAIT
-
tcp        0      0 172.31.110.90:51674     157.240.198.60:443      ESTABLISHED
4137/firefox
tcp        0      0 127.0.0.1:33140         127.0.0.1:3001          ESTABLISHED
4137/firefox
tcp        0      0 172.31.110.90:34706     163.70.145.60:443       ESTABLISHED
4137/firefox
tcp        0      0 172.31.110.90:60282     216.58.200.174:443      ESTABLISHED
4137/firefox
tcp        0      0 172.31.110.90:57720     20.42.73.31:443         ESTABLISHED
2782/Code --standar
tcp        0      0 172.31.110.90:46430     163.70.145.60:443       ESTABLISHED
4137/firefox
tcp6       0      0 ::1:631                 :::*                    LISTEN
1023/cupsd
tcp6       0      0 :::3001                 :::*                    LISTEN
18532/node
tcp6       0      0 127.0.0.1:3001          127.0.0.1:33140         ESTABLISHED
18532/node
--------------------------------------------------------------------------------
Network Interfaces (ifconfig -a):
enp3s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether e4:a8:df:d2:4f:79  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 27761  bytes 6377458 (6.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27761  bytes 6377458 (6.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.31.110.90  netmask 255.255.192.0  broadcast 172.31.127.255
        inet6 fe80::17b8:1412:5142:f1d1  prefixlen 64  scopeid 0x20<link>
        ether f8:9e:94:f2:72:6d  txqueuelen 1000  (Ethernet)
        RX packets 73314  bytes 25802660 (25.8 MB)
        RX errors 0  dropped 23  overruns 0  frame 0
        TX packets 15416  bytes 9298208 (9.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

-------------------------------------------------------------------------------
Iptables (Firewall Rules):
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

-------------------------------------------------------------------------------
Routing Table (route command):
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    600    0        0 wlp0s20f
3
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 wlp0s20f
3
172.31.64.0     0.0.0.0         255.255.192.0   U     600    0        0 wlp0s20f
3
-------------------------------------------------------------------------------
```