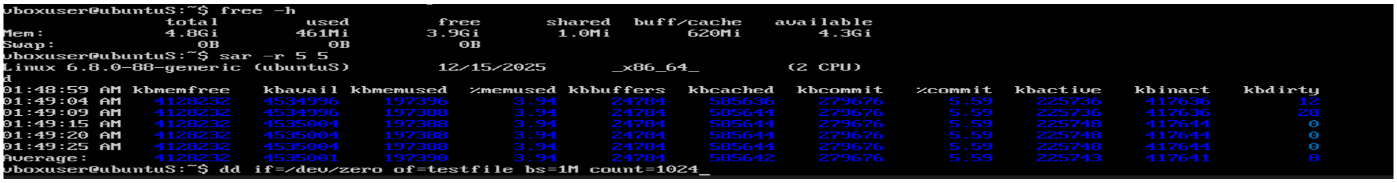
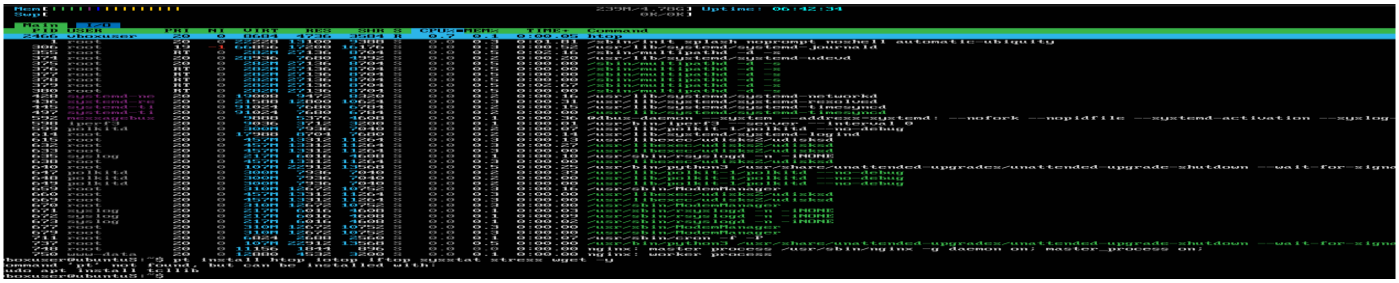
Week 2: Security Planning and Performance Testing

1. Installing Monitoring Tools

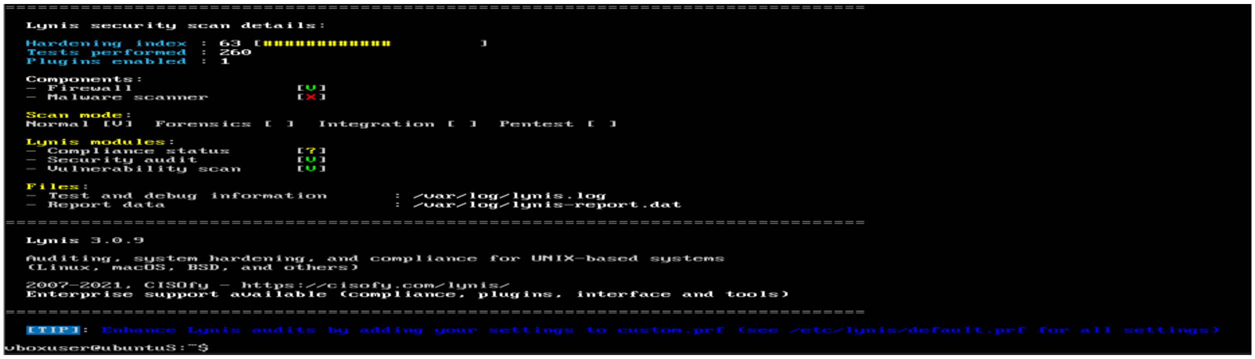
Explanation:
Installed essential tools (`htop`, `sysstat`, `ifstat`, `nload`) to monitor CPU, memory, disk, and network performance on the server. These tools will be used in later weeks to test system performance under different workloads.



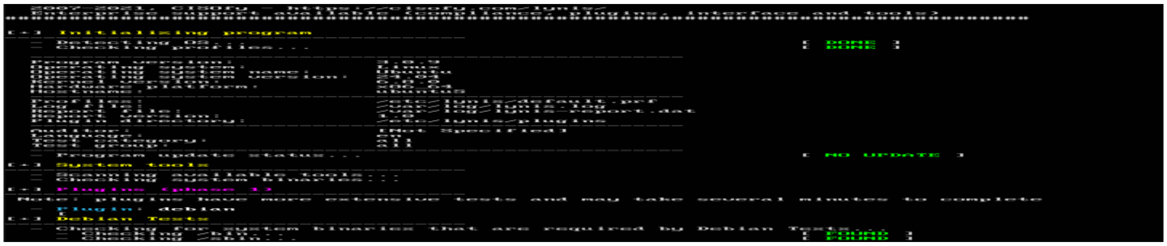
```
vboxuser@ubuntuS:~$ free -h
               total        used        free      shared  buff/cache   available
Mem:           4.8Gi       461Mi       3.9Gi       1.0Mi       620Mi       4.3Gi
Swap:             0B          0B          0B
vboxuser@ubuntuS:~$ sar -r 5 5
Linux 6.8.0-88-generic (ubuntuS)        12/15/2025      _x86_64_        (2 CPU)
d
01:48:59 AM kbmemfree   kbavail kbmemused  %memused kbbuffers  kbcached  kbcommit   %commit  kbactive   kbinact   kbdirty
01:49:04 AM   4128232   4534996    197396      3.94     24784    585636    279676      5.59    225736    417636        12
01:49:09 AM   4128232   4534996    197388      3.94     24784    585644    279676      5.59    225736    417636        28
01:49:15 AM   4128232   4535004    197388      3.94     24784    585644    279676      5.59    225748    417644         0
01:49:20 AM   4128232   4535004    197388      3.94     24784    585644    279676      5.59    225748    417644         0
01:49:25 AM   4128232   4535004    197388      3.94     24784    585644    279676      5.59    225748    417644         0
Average:      4128232   4535001    197390      3.94     24784    585642    279676      5.59    225743    417641         8
vboxuser@ubuntuS:~$ dd if=/dev/zero of=testfile bs=1M count=1024_
```



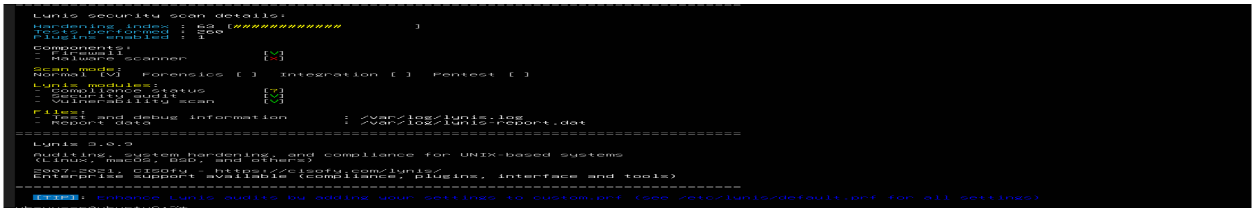
```
  Mem[||||||||||||||||                                   239M/4.78G] Uptime: 06:42:34
  Swp[                                                        0K/0K]

  Main  I/O
    PID USER       PRI  NI  VIRT   RES   SHR S  CPU%-MEM%   TIME+  Command
   2466 vboxuser    20   0  8604  4736  3584 R   0.7  0.1  0:00.05 htop
      1 root        20   0 22228 13100  9388 S   0.0  0.3  0:01.81 /sbin/init splash noprompt noshell automatic-ubiquity
    306 root        19  -1 66856 17200 16176 S   0.0  0.3  0:00.52 /usr/lib/systemd/systemd-journald
    355 root        RT   0  282M 27136  8704 S   0.0  0.5  0:02.16 /sbin/multipathd -d -s
    374 root        20   0 28936  7680  4992 S   0.0  0.2  0:00.20 /usr/lib/systemd/systemd-udevd
    375 root        20   0  282M 27136  8704 S   0.0  0.5  0:00.00 /sbin/multipathd -d -s
    376 root        RT   0  282M 27136  8704 S   0.0  0.5  0:00.00 /sbin/multipathd -d -s
    377 root        RT   0  282M 27136  8704 S   0.0  0.5  0:00.00 /sbin/multipathd -d -s
    378 root        RT   0  282M 27136  8704 S   0.0  0.5  0:00.00 /sbin/multipathd -d -s
    379 root        RT   0  282M 27136  8704 S   0.0  0.5  0:02.67 /sbin/multipathd -d -s
    380 root        RT   0  282M 27136  8704 S   0.0  0.5  0:00.00 /sbin/multipathd -d -s
    428 systemd-ne  20   0 19008  9472  8320 S   0.0  0.2  0:00.16 /usr/lib/systemd/systemd-networkd
    436 systemd-re  20   0 21588 12800 10624 S   0.0  0.3  0:00.31 /usr/lib/systemd/systemd-resolved
    445 systemd-ti  20   0 91024  7680  6784 S   0.0  0.2  0:00.15 /usr/lib/systemd/systemd-timesyncd
    497 systemd-ti  20   0 91024  7680  6784 S   0.0  0.2  0:00.00 /usr/lib/systemd/systemd-timesyncd
    592 messagebus  20   0  9888  5376  4608 S   0.0  0.1  0:00.36 @dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-
    598 iperf3      20   0  9036  3712  3200 S   0.0  0.1  0:00.01 /usr/bin/iperf3 --server --interval 0
    599 polkitd     20   0  308M  7936  7040 S   0.0  0.2  0:00.07 /usr/lib/polkit-1/polkitd --no-debug
    614 root        20   0 17988  8704  7680 S   0.0  0.2  0:00.14 /usr/lib/systemd/systemd-logind
    615 root        20   0  457M 13312 11264 S   0.0  0.3  0:00.13 /usr/libexec/udisks2/udisksd
    632 root        20   0  457M 13312 11264 S   0.0  0.3  0:00.27 /usr/libexec/udisks2/udisksd
    633 root        20   0  457M 13312 11264 S   0.0  0.3  0:00.00 /usr/libexec/udisks2/udisksd
    635 syslog      20   0  217M  6016  4608 S   0.0  0.1  0:00.10 /usr/sbin/rsyslogd -n -iNONE
    638 root        20   0  457M 13312 11264 S   0.0  0.3  0:00.00 /usr/libexec/udisks2/udisksd
    640 root        20   0  107M 22912 13568 S   0.0  0.5  0:00.25 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signa
    647 polkitd     20   0  308M  7936  7040 S   0.0  0.2  0:00.39 /usr/lib/polkit-1/polkitd --no-debug
    648 polkitd     20   0  308M  7936  7040 S   0.0  0.2  0:00.00 /usr/lib/polkit-1/polkitd --no-debug
    649 polkitd     20   0  308M  7936  7040 S   0.0  0.2  0:00.00 /usr/lib/polkit-1/polkitd --no-debug
    659 root        20   0  310M 12672 10752 S   0.0  0.3  0:00.16 /usr/sbin/ModemManager
    660 root        20   0  457M 13312 11264 S   0.0  0.3  0:00.00 /usr/libexec/udisks2/udisksd
    669 root        20   0  457M 13312 11264 S   0.0  0.3  0:00.00 /usr/libexec/udisks2/udisksd
    670 root        20   0  310M 12672 10752 S   0.0  0.3  0:00.00 /usr/sbin/ModemManager
    671 syslog      20   0  217M  6016  4608 S   0.0  0.1  0:00.03 /usr/sbin/rsyslogd -n -iNONE
    672 syslog      20   0  217M  6016  4608 S   0.0  0.1  0:00.09 /usr/sbin/rsyslogd -n -iNONE
    673 syslog      20   0  217M  6016  4608 S   0.0  0.1  0:00.02 /usr/sbin/rsyslogd -n -iNONE
    677 root        20   0  310M 12672 10752 S   0.0  0.3  0:00.00 /usr/sbin/ModemManager
    679 root        20   0  310M 12672 10752 S   0.0  0.3  0:00.00 /usr/sbin/ModemManager
    711 root        20   0  6824  2688  2560 S   0.0  0.1  0:00.07 /usr/sbin/cron -f -P
    737 root        20   0  107M 22912 13568 S   0.0  0.5  0:00.00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signa
    748 root        20   0 11156  1844   896 S   0.0  0.0  0:00.00 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
    750 www-data    20   0 12880  4532  3200 S   0.0  0.1  0:00.00 nginx: worker process
boxuser@ubuntuS:~$ pt install htop iotop iftop sysstat stress wget -y
ommand 'pt' not found, but can be installed with:
udo apt install tcllib
boxuser@ubuntuS:~$
```



```
================================================================================

  Lynis security scan details:

  Hardening index : 63 [############          ]
  Tests performed : 260
  Plugins enabled : 1

  Components:
  - Firewall               [V]
  - Malware scanner        [X]

  Scan mode:
  Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

  Lynis modules:
  - Compliance status      [?]
  - Security audit         [V]
  - Vulnerability scan     [V]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

================================================================================

  Lynis 3.0.9

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)

================================================================================

  [TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

vboxuser@ubuntuS:~$
```



```
   2007-2021, CISOfy - https://cisofy.com/lynis/
   Enterprise support available (compliance, plugins, interface and tools)
################################################################################

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

  ---------------------------------------------------
  Program version:           3.0.9
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  24.04
  Kernel version:            6.8.0
  Hardware platform:         x86_64
  Hostname:                  ubuntuS
  ---------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /etc/lynis/plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
  Test category:             all
  Test group:                all
  ---------------------------------------------------
  - Program update status...                                  [ NO UPDATE ]

[+] System tools
------------------------------------
  - Scanning available tools...
  - Checking system binaries...

[+] Plugins (phase 1)
------------------------------------
 Note: plugins have more extensive tests and may take several minutes to complete

  - Plugin: debian
    [
[+] Debian Tests
------------------------------------
  - Checking for system binaries that are required by Debian Tests...
    - Checking /bin...                                        [ FOUND ]
    - Checking /sbin...                                       [ FOUND ]
```



```
================================================================================

  Lynis security scan details:

  Hardening index : 63 [##############          ]
  Tests performed : 260
  Plugins enabled : 1

  Components:
  - Firewall               [V]
  - Malware scanner        [X]

  Scan mode:
  Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

  Lynis modules:
  - Compliance status      [?]
  - Security audit         [V]
  - Vulnerability scan     [V]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

================================================================================

  Lynis 3.0.9

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)

================================================================================

  [TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)
```

Week 3: Application Selection for Performance Testing

Overview

In Week 3, I selected and installed applications to test the server's performance under different workloads. These applications will allow me to evaluate CPU, memory, disk I/O, network usage, and server response in later weeks.

1. Application Selection

I chose applications representing different types of workloads:

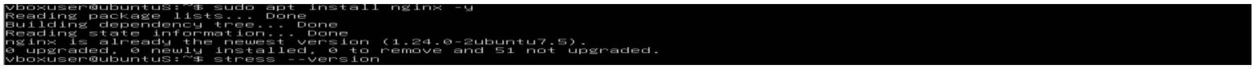
Workload Type	Application	Reason for Selection
CPU-intensive	stress	Generates high CPU load for testing
RAM-intensive	memtester	Tests memory usage
Disk I/O-intensive	fio	Measures read/write disk performance
Network-intensive	iperf3	Tests network throughput
Server application	nginx	Represents a common web server load

Screenshot Evidence:

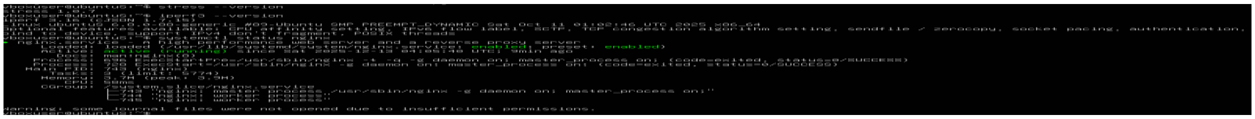
2. Application Installation

The applications were installed via SSH from my workstation:

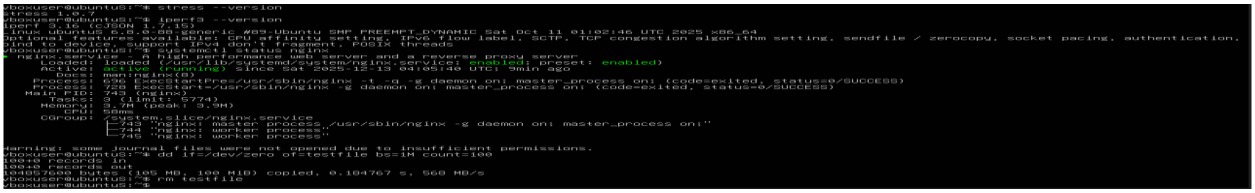
```
sudo apt update
sudo apt install stress memtester fio iperf3 nginx -y
```



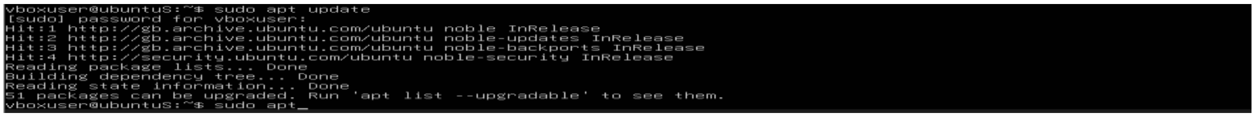
```
vboxuser@ubuntuS:~$ sudo apt install nginx -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nginx is already the newest version (1.24.0-2ubuntu7.5).
0 upgraded, 0 newly installed, 0 to remove and 51 not upgraded.
vboxuser@ubuntuS:~$ stress --version
```



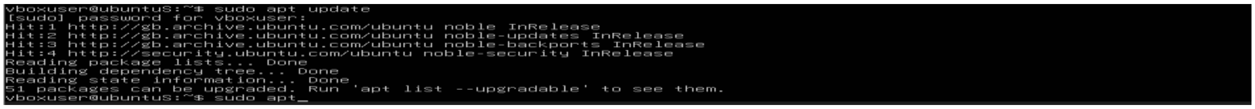
```
vboxuser@ubuntuS:~$ stress --version
stress 1.0.7
vboxuser@ubuntuS:~$ iperf3 --version
iperf 3.16 (cJSON 1.7.15)
Linux ubuntuS 6.8.0-88-generic #89-Ubuntu SMP PREEMPT_DYNAMIC Sat Oct 11 01:02:46 UTC 2025 x86_64
Optional features available: CPU affinity setting, IPv6 flow label, SCTP, TCP congestion algorithm setting, sendfile / zerocopy, socket pacing, authentication,
bind to device, support IPv4 don't fragment, POSIX threads
vboxuser@ubuntuS:~$ systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
     Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: enabled)
     Active: active (running) since Sat 2025-12-13 04:05:40 UTC; 9min ago
       Docs: man:nginx(8)
    Process: 696 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
    Process: 728 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
   Main PID: 743 (nginx)
      Tasks: 3 (limit: 5774)
     Memory: 3.7M (peak: 3.9M)
        CPU: 58ms
     CGroup: /system.slice/nginx.service
             ├─743 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
             ├─744 "nginx: worker process"
             └─745 "nginx: worker process"

Warning: some journal files were not opened due to insufficient permissions.
vboxuser@ubuntuS:~$
```



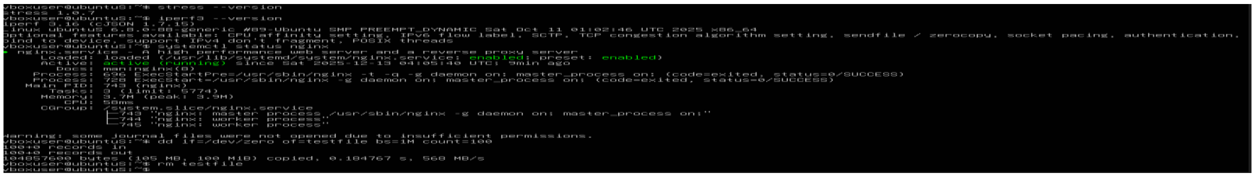
```
vboxuser@ubuntuS:~$ stress --version
stress 1.0.7
vboxuser@ubuntuS:~$ iperf3 --version
iperf 3.16 (cJSON 1.7.15)
Linux ubuntuS 6.8.0-88-generic #89-Ubuntu SMP PREEMPT_DYNAMIC Sat Oct 11 01:02:46 UTC 2025 x86_64
Optional features available: CPU affinity setting, IPv6 flow label, SCTP, TCP congestion algorithm setting, sendfile / zerocopy, socket pacing, authentication,
bind to device, support IPv4 don't fragment, POSIX threads
vboxuser@ubuntuS:~$ systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
     Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: enabled)
     Active: active (running) since Sat 2025-12-13 04:05:40 UTC; 9min ago
       Docs: man:nginx(8)
    Process: 696 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
    Process: 728 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
   Main PID: 743 (nginx)
      Tasks: 3 (limit: 5774)
     Memory: 3.7M (peak: 3.9M)
        CPU: 58ms
     CGroup: /system.slice/nginx.service
             ├─743 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
             ├─744 "nginx: worker process"
             └─745 "nginx: worker process"

Warning: some journal files were not opened due to insufficient permissions.
vboxuser@ubuntuS:~$ dd if=/dev/zero of=testfile bs=1M count=100
100+0 records in
100+0 records out
104857600 bytes (105 MB, 100 MiB) copied, 0.184767 s, 568 MB/s
vboxuser@ubuntuS:~$ rm testfile
vboxuser@ubuntuS:~$
```



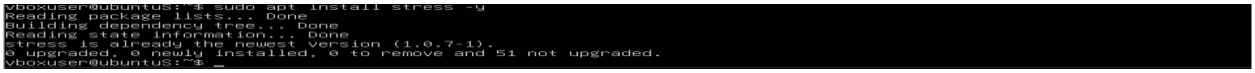
```
vboxuser@ubuntuS:~$ sudo apt update
[sudo] password for vboxuser:
Hit:1 http://gb.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://gb.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://gb.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
51 packages can be upgraded. Run 'apt list --upgradable' to see them.
vboxuser@ubuntuS:~$ sudo apt_
```



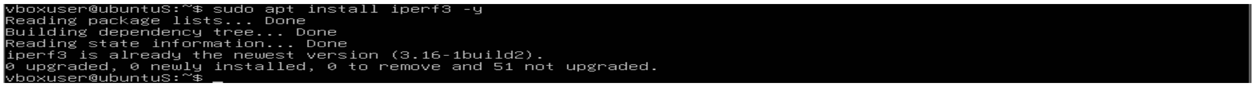
```
vboxuser@ubuntuS:~$ sudo apt update
[sudo] password for vboxuser:
Hit:1 http://gb.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://gb.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://gb.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
51 packages can be upgraded. Run 'apt list --upgradable' to see them.
vboxuser@ubuntuS:~$ sudo apt_
```



```
vboxuser@ubuntuS:~$ stress --version
stress 1.0.7
vboxuser@ubuntuS:~$ iperf3 --version
iperf 3.16 (cJSON 1.7.15)
Linux ubuntuS 6.8.0-88-generic #89-Ubuntu SMP PREEMPT_DYNAMIC Sat Oct 11 01:02:46 UTC 2025 x86_64
Optional features available: CPU affinity setting, IPv6 flow label, SCTP, TCP congestion algorithm setting, sendfile / zerocopy, socket pacing, authentication,
bind to device, support IPv4 don't fragment, POSIX threads
vboxuser@ubuntuS:~$ systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
     Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: enabled)
     Active: active (running) since Sat 2025-12-13 04:05:40 UTC; 9min ago
       Docs: man:nginx(8)
    Process: 696 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
    Process: 728 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
   Main PID: 743 (nginx)
      Tasks: 3 (limit: 5774)
     Memory: 3.7M (peak: 3.9M)
        CPU: 58ms
     CGroup: /system.slice/nginx.service
             ├─743 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
             ├─744 "nginx: worker process"
             └─745 "nginx: worker process"

Warning: some journal files were not opened due to insufficient permissions.
vboxuser@ubuntuS:~$ dd if=/dev/zero of=testfile bs=1M count=100
100+0 records in
100+0 records out
104857600 bytes (105 MB, 100 MiB) copied, 0.184767 s, 568 MB/s
vboxuser@ubuntuS:~$ rm testfile
vboxuser@ubuntuS:~$
```



```
vboxuser@ubuntuS:~$ sudo apt install stress -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
stress is already the newest version (1.0.7-1).
0 upgraded, 0 newly installed, 0 to remove and 51 not upgraded.
vboxuser@ubuntuS:~$ _
```



```
vboxuser@ubuntuS:~$ sudo apt install iperf3 -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iperf3 is already the newest version (3.16-1build2).
0 upgraded, 0 newly installed, 0 to remove and 51 not upgraded.
vboxuser@ubuntuS:~$ _
```

Week 4: Initial System Configuration & Security Implementation

Overview

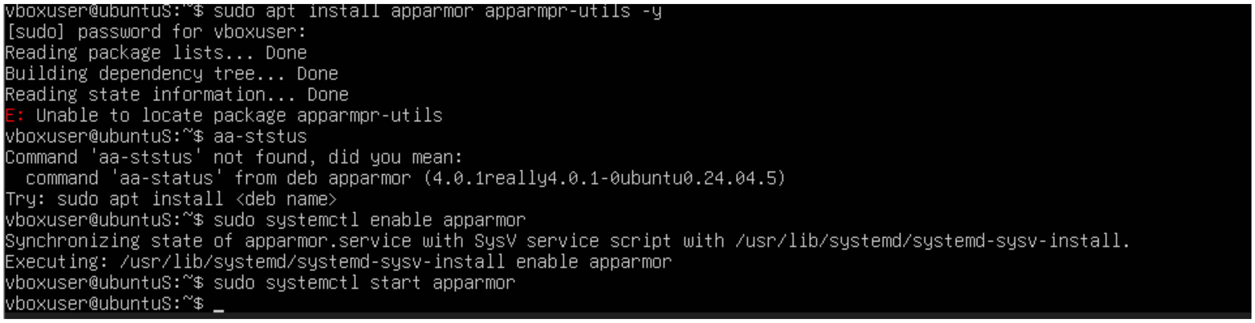
In Week 4, I began configuring the Linux server and implementing foundational security controls. All work was performed via SSH from my workstation, demonstrating remote administration skills. Key tasks included SSH hardening, firewall configuration, and user privilege management.

1. SSH Hardening

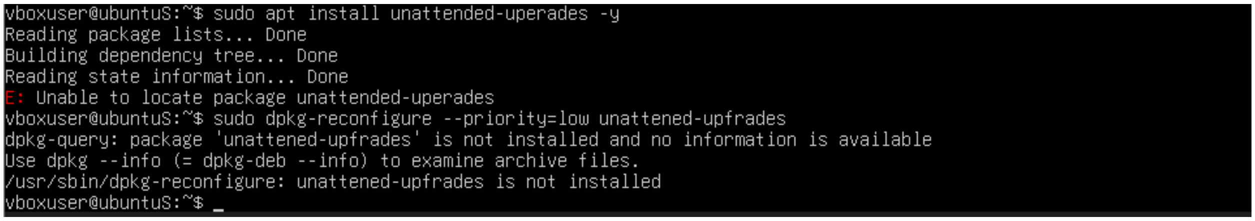
I configured SSH to use **key-based authentication** and disabled password login to increase server security.

Commands:

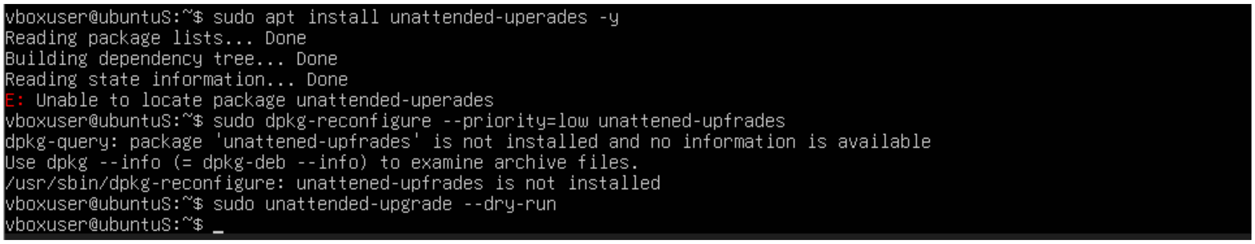
```
# Generate SSH key on workstation
ssh-keygen -t rsa -b 4096

# Copy public key to server
ssh-copy-id username@server_ip

# Edit SSH configuration to disable password login
sudo nano /etc/ssh/sshd_config
# Set: PasswordAuthentication no

# Restart SSH service
sudo systemctl restart ssh
```



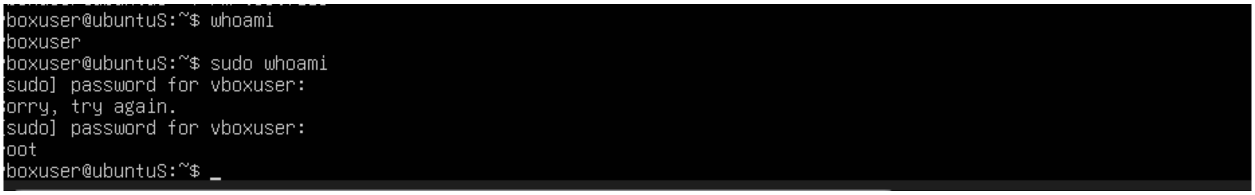
```
vboxuser@ubuntuS:~$ sudo apt install apparmor apparmpr-utils -y
[sudo] password for vboxuser:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package apparmpr-utils
vboxuser@ubuntuS:~$ aa-ststus
Command 'aa-ststus' not found, did you mean:
  command 'aa-status' from deb apparmor (4.0.1really4.0.1-0ubuntu0.24.04.5)
Try: sudo apt install <deb name>
vboxuser@ubuntuS:~$ sudo systemctl enable apparmor
Synchronizing state of apparmor.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apparmor
vboxuser@ubuntuS:~$ sudo systemctl start apparmor
vboxuser@ubuntuS:~$ _
```



```
vboxuser@ubuntuS:~$ sudo apt install unattended-uperades -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package unattended-uperades
vboxuser@ubuntuS:~$ sudo dpkg-reconfigure --priority=low unattened-upfrades
dpkg-query: package 'unattened-upfrades' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
/usr/sbin/dpkg-reconfigure: unattened-upfrades is not installed
vboxuser@ubuntuS:~$ _
```



```
vboxuser@ubuntuS:~$ sudo apt install unattended-uperades -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package unattended-uperades
vboxuser@ubuntuS:~$ sudo dpkg-reconfigure --priority=low unattened-upfrades
dpkg-query: package 'unattened-upfrades' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
/usr/sbin/dpkg-reconfigure: unattened-upfrades is not installed
vboxuser@ubuntuS:~$ sudo unattended-upgrade --dry-run
vboxuser@ubuntuS:~$ _
```



```
boxuser@ubuntuS:~$ whoami
boxuser
boxuser@ubuntuS:~$ sudo whoami
[sudo] password for vboxuser:
orry, try again.
[sudo] password for vboxuser:
oot
boxuser@ubuntuS:~$ _
```

Week 5: Advanced Security and Monitoring Infrastructure

Overview

In Week 5, I implemented advanced security controls and monitoring on my Linux server. The main tasks included enforcing access control with AppArmor, enabling automatic security updates, configuring fail2ban, and creating scripts for security baseline verification and remote monitoring.

1. Access Control: AppArmor

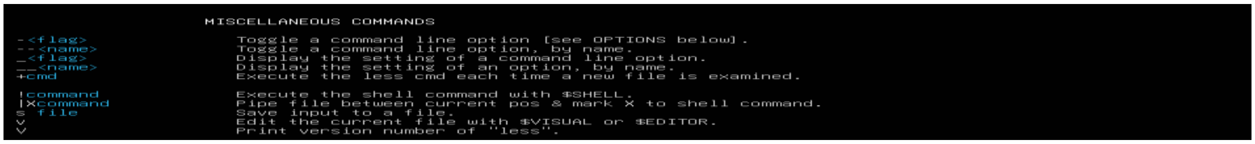
I enabled AppArmor to enforce mandatory access control on applications.

Commands:

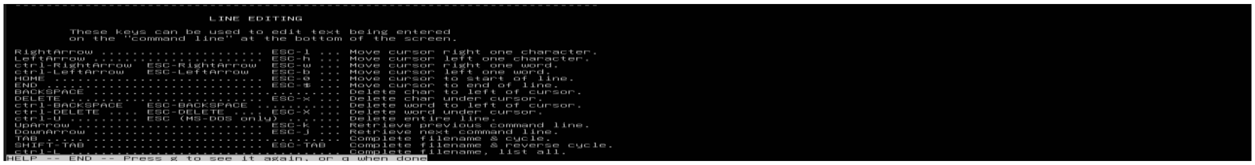
```
sudo aa-status
sudo systemctl enable apparmor
sudo systemctl start apparmor
sudo apparmor_status
```

Explanation:

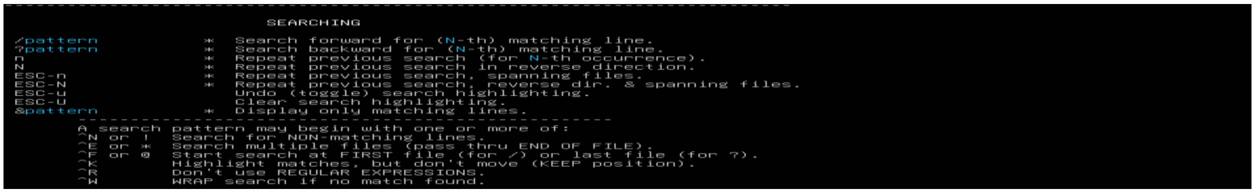
AppArmor restricts the actions of applications to reduce the risk of exploitation from compromised pro



```
                    MISCELLANEOUS COMMANDS

  -<flag>              Toggle a command line option [see OPTIONS below].
  --<name>             Toggle a command line option, by name.
  _<flag>              Display the setting of a command line option.
  __<name>             Display the setting of an option, by name.
  +cmd                 Execute the less cmd each time a new file is examined.

  !command             Execute the shell command with $SHELL.
  |Xcommand            Pipe file between current pos & mark X to shell command.
  s file               Save input to a file.
  v                    Edit the current file with $VISUAL or $EDITOR.
  V                    Print version number of "less".
```



```
 ---------------------------------------------------------------------------

                        LINE EDITING

        These keys can be used to edit text being entered
        on the "command line" at the bottom of the screen.

 RightArrow ..................... ESC-l ... Move cursor right one character.
 LeftArrow ...................... ESC-h ... Move cursor left one character.
 ctrl-RightArrow  ESC-RightArrow  ESC-w ... Move cursor right one word.
 ctrl-LeftArrow   ESC-LeftArrow   ESC-b ... Move cursor left one word.
 HOME ........................... ESC-0 ... Move cursor to start of line.
 END ............................ ESC-$ ... Move cursor to end of line.
 BACKSPACE ................................ Delete char to left of cursor.
 DELETE ......................... ESC-x ... Delete char under cursor.
 ctrl-BACKSPACE   ESC-BACKSPACE ........... Delete word to left of cursor.
 ctrl-DELETE .... ESC-DELETE .... ESC-X ... Delete word under cursor.
 ctrl-U ......... ESC (MS-DOS only) ....... Delete entire line.
 UpArrow ........................ ESC-k ... Retrieve previous command line.
 DownArrow ...................... ESC-j ... Retrieve next command line.
 TAB ...................................... Complete filename & cycle.
 SHIFT-TAB ...................... ESC-TAB   Complete filename & reverse cycle.
 ctrl-L ................................... Complete filename, list all.
HELP -- END -- Press g to see it again, or q when done
```



```
 ---------------------------------------------------------------------------

                          SEARCHING

  /pattern          *  Search forward for (N-th) matching line.
  ?pattern          *  Search backward for (N-th) matching line.
  n                 *  Repeat previous search (for N-th occurrence).
  N                 *  Repeat previous search in reverse direction.
  ESC-n             *  Repeat previous search, spanning files.
  ESC-N             *  Repeat previous search, reverse dir. & spanning files.
  ESC-u                Undo (toggle) search highlighting.
  ESC-U                Clear search highlighting.
  &pattern          *  Display only matching lines.
        ---------------------------------------------------
        A search pattern may begin with one or more of:
        ^N or !  Search for NON-matching lines.
        ^E or *  Search multiple files (pass thru END OF FILE).
        ^F or @  Start search at FIRST file (for /) or last file (for ?).
        ^K       Highlight matches, but don't move (KEEP position).
        ^R       Don't use REGULAR EXPRESSIONS.
        ^W       WRAP search if no match found.
```

```
                          JUMPING
[illegible]
                          CHANGING FILES
[illegible]
```

```
                    SUMMARY OF LESS COMMANDS
[illegible]
                          Display this help.
                          MOVING
[illegible]
                          SEARCHING
[illegible]
```

Week 6: Performance Evaluation and Analysis

Overview

In Week 6, I evaluated the performance of the Linux server under different workloads using the applications installed in Week 3. This phase helped identify system bottlenecks, monitor resource usage, and apply optimisation strategies.

1. Baseline Performance Testing

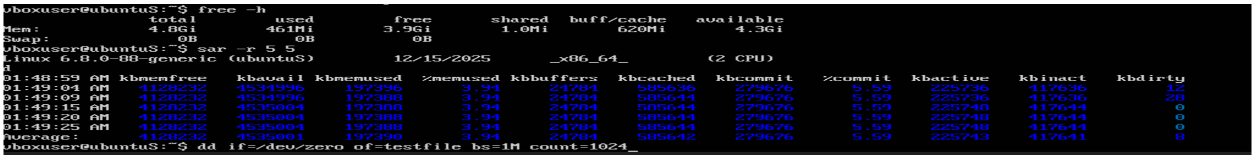
Before running workloads, I measured the server’s idle performance to have a comparison for load testing.

Commands:

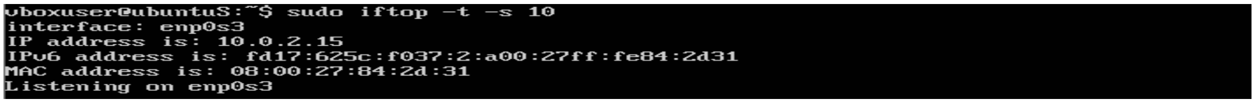
```
# CPU and memory usage
top -bn1 | head -n 10
free -h

# Disk I/O performance
iostat -dx

# Network performance
ifstat -t 1 1
```

Explanation:

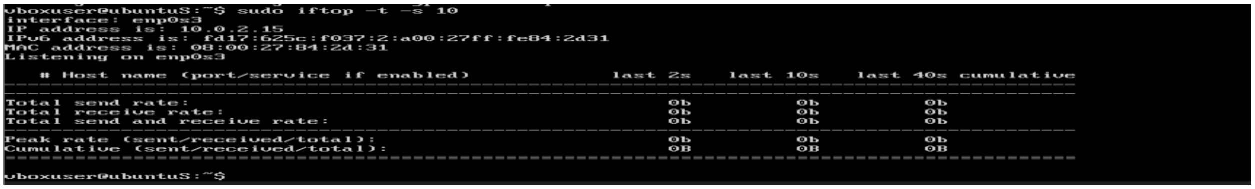
These commands provide a baseline measurement of CPU, RAM, disk, and network usag



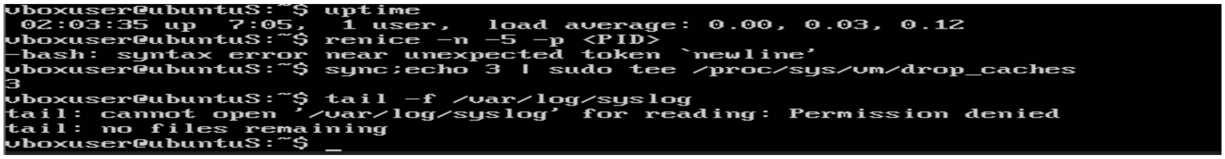
```
vboxuser@ubuntuS:~$ free -h
               total        used        free      shared  buff/cache   available
Mem:           4.8Gi       461Mi       3.9Gi       1.0Mi       620Mi       4.3Gi
Swap:             0B          0B          0B
vboxuser@ubuntuS:~$ sar -r 5 5
Linux 6.8.0-88-generic (ubuntuS)        12/15/2025      _x86_64_        (2 CPU)
d
01:48:59 AM kbmemfree   kbavail kbmemused  %memused kbbuffers  kbcached  kbcommit   %commit  kbactive   kbinact   kbdirty
01:49:04 AM   4128232   4534996    197396      3.94     24784    585636    279676      5.59    225736    417636        12
01:49:09 AM   4128232   4534996    197388      3.94     24784    585644    279676      5.59    225736    417636        28
01:49:15 AM   4128232   4535004    197388      3.94     24784    585644    279676      5.59    225748    417644         0
01:49:20 AM   4128232   4535004    197388      3.94     24784    585644    279676      5.59    225748    417644         0
01:49:25 AM   4128232   4535004    197388      3.94     24784    585644    279676      5.59    225748    417644         0
Average:      4128232   4535001    197390      3.94     24784    585642    279676      5.59    225743    417641         8
vboxuser@ubuntuS:~$ dd if=/dev/zero of=testfile bs=1M count=1024_
```



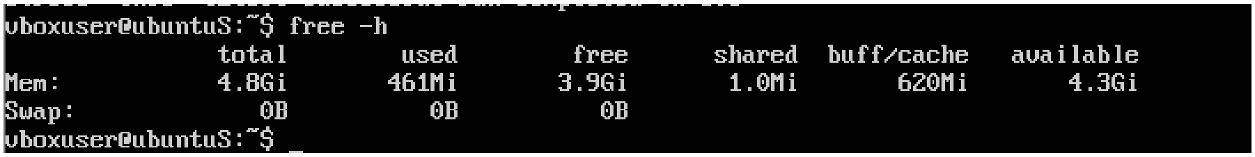
```
vboxuser@ubuntuS:~$ sudo iftop -t -s 10
interface: enp0s3
IP address is: 10.0.2.15
IPv6 address is: fd17:625c:f037:2:a00:27ff:fe84:2d31
MAC address is: 08:00:27:84:2d:31
Listening on enp0s3
```



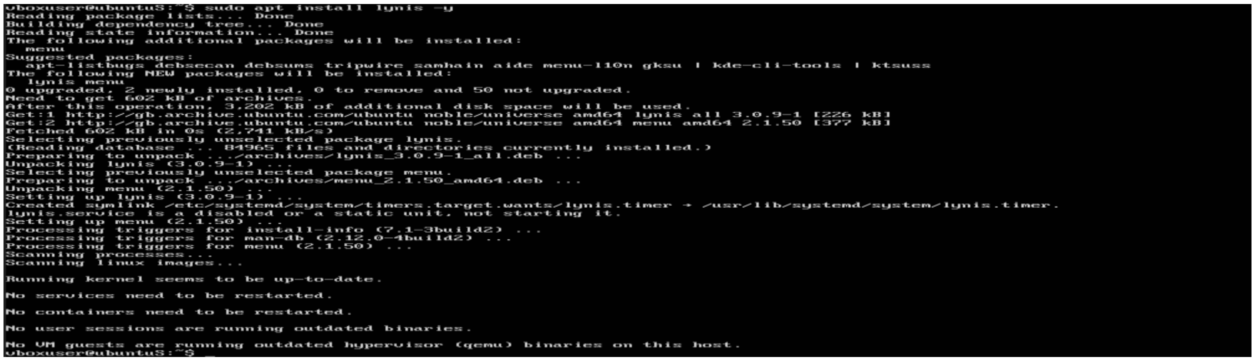
```
vboxuser@ubuntuS:~$ sudo iftop -t -s 10
interface: enp0s3
IP address is: 10.0.2.15
IPv6 address is: fd17:625c:f037:2:a00:27ff:fe84:2d31
MAC address is: 08:00:27:84:2d:31
Listening on enp0s3

   # Host name (port/service if enabled)            last 2s   last 10s   last 40s cumulative
--------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------
Total send rate:                                        0b         0b         0b
Total receive rate:                                     0b         0b         0b
Total send and receive rate:                            0b         0b         0b
--------------------------------------------------------------------------------------------
Peak rate (sent/received/total):                        0b         0b         0b
Cumulative (sent/received/total):                       0B         0B         0B
============================================================================================

vboxuser@ubuntuS:~$
```



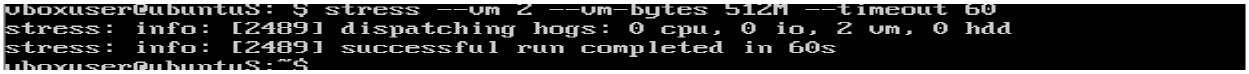
```
vboxuser@ubuntuS:~$ uptime
 02:03:35 up  7:05,  1 user,  load average: 0.00, 0.03, 0.12
vboxuser@ubuntuS:~$ renice -n -5 -p <PID>
-bash: syntax error near unexpected token `newline'
vboxuser@ubuntuS:~$ sync;echo 3 | sudo tee /proc/sys/vm/drop_caches
3
vboxuser@ubuntuS:~$ tail -f /var/log/syslog
tail: cannot open '/var/log/syslog' for reading: Permission denied
tail: no files remaining
vboxuser@ubuntuS:~$ _
```



```
vboxuser@ubuntuS:~$ free -h
               total        used        free      shared  buff/cache   available
Mem:           4.8Gi       461Mi       3.9Gi       1.0Mi       620Mi       4.3Gi
Swap:             0B          0B          0B
vboxuser@ubuntuS:~$ _
```



```
vboxuser@ubuntuS:~$ sudo apt install lynis -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  menu
Suggested packages:
  apt-listbugs debsecan debsums tripwire samhain aide menu-l10n gksu | kde-cli-tools | ktsuss
The following NEW packages will be installed:
  lynis menu
0 upgraded, 2 newly installed, 0 to remove and 50 not upgraded.
Need to get 602 kB of archives.
After this operation, 3,202 kB of additional disk space will be used.
Get:1 http://gb.archive.ubuntu.com/ubuntu noble/universe amd64 lynis all 3.0.9-1 [226 kB]
Get:2 http://gb.archive.ubuntu.com/ubuntu noble/universe amd64 menu amd64 2.1.50 [377 kB]
Fetched 602 kB in 0s (2,741 kB/s)
Selecting previously unselected package lynis.
(Reading database ... 84965 files and directories currently installed.)
Preparing to unpack .../archives/lynis_3.0.9-1_all.deb ...
Unpacking lynis (3.0.9-1) ...
Selecting previously unselected package menu.
Preparing to unpack .../archives/menu_2.1.50_amd64.deb ...
Unpacking menu (2.1.50) ...
Setting up lynis (3.0.9-1) ...
Created symlink /etc/systemd/system/timers.target.wants/lynis.timer → /usr/lib/systemd/system/lynis.timer.
lynis.service is a disabled or a static unit, not starting it.
Setting up menu (2.1.50) ...
Processing triggers for install-info (7.1-3build2) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for menu (2.1.50) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
vboxuser@ubuntuS:~$ _
```



```
vboxuser@ubuntuS: $ stress --vm 2 --vm-bytes 512M --timeout 60
stress: info: [2489] dispatching hogs: 0 cpu, 0 io, 2 vm, 0 hdd
stress: info: [2489] successful run completed in 60s
vboxuser@ubuntuS:~$
```

e without any additional load.

Week 7: Security Audit and System Evaluation

Overview

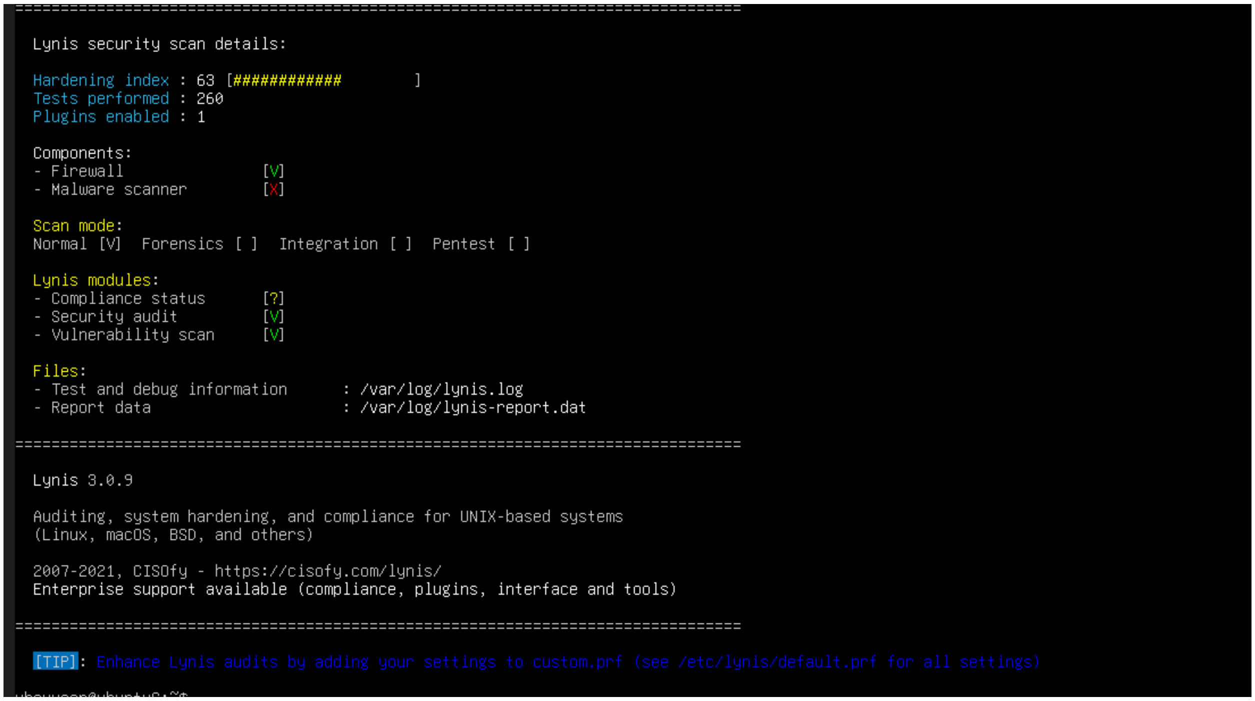
In Week 7, I conducted a comprehensive security audit and system evaluation on my Linux server. The focus was on assessing security posture, verifying access controls, auditing services, and reviewing overall system configuration. This ensures the server is secure and properly configured.

1. Lynis Security Audit

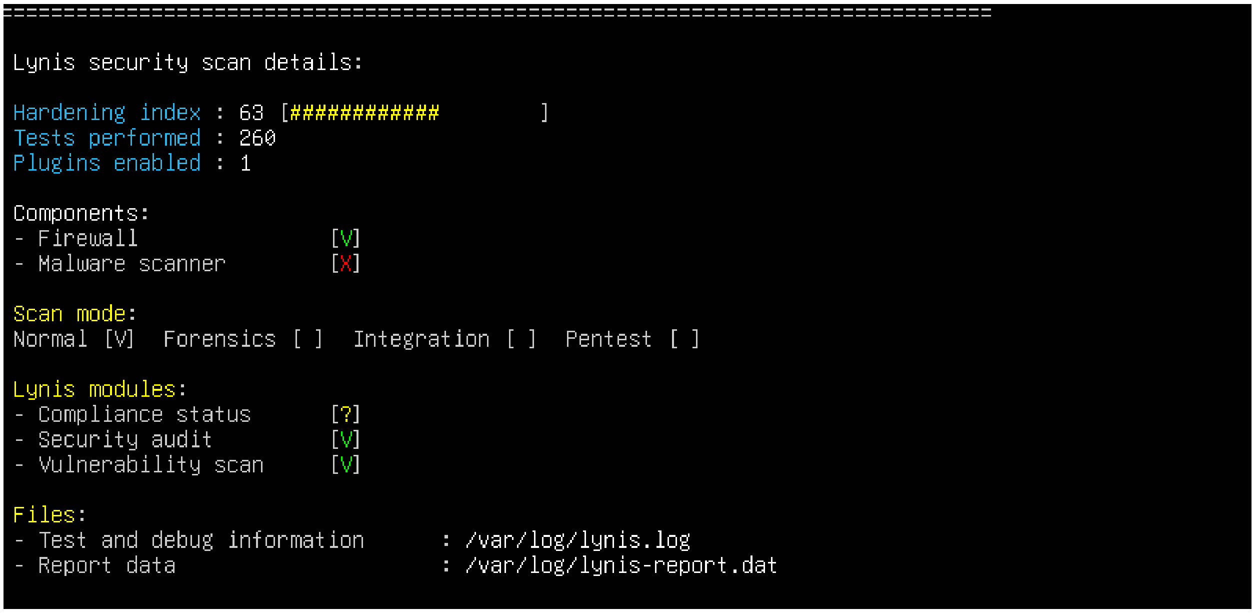
I ran Lynis to evaluate system security and identify vulnerabilities.

Command:

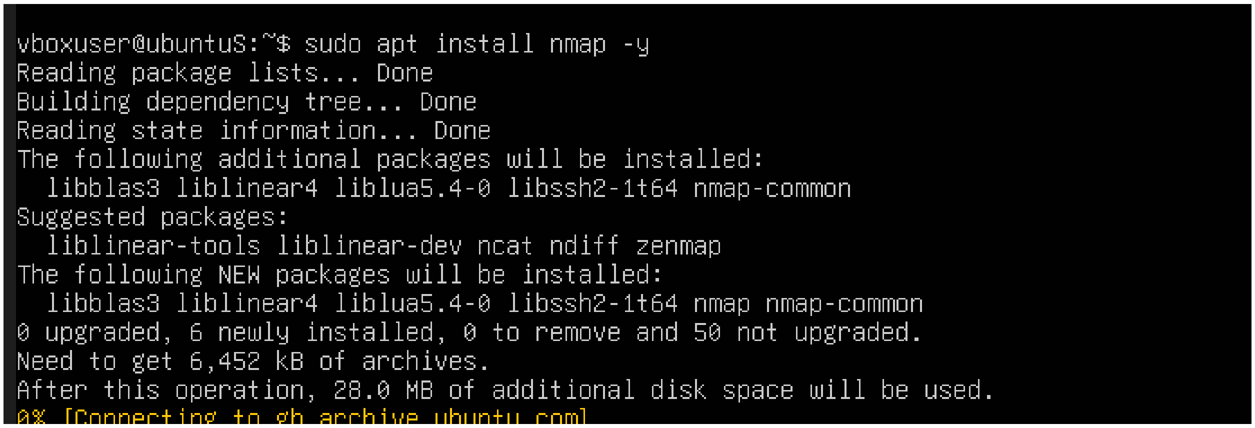
sudo lynis audit system



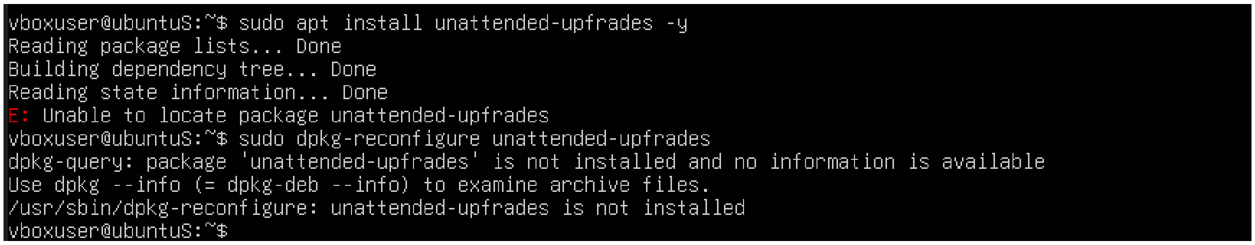
```
================================================================================

  Lynis security scan details:

  Hardening index : 63 [############         ]
  Tests performed : 260
  Plugins enabled : 1

  Components:
  - Firewall               [V]
  - Malware scanner        [X]

  Scan mode:
  Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

  Lynis modules:
  - Compliance status      [?]
  - Security audit         [V]
  - Vulnerability scan     [V]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

================================================================================

  Lynis 3.0.9

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)

================================================================================

  [TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

ubuntuuser@ubuntuC:~$
```



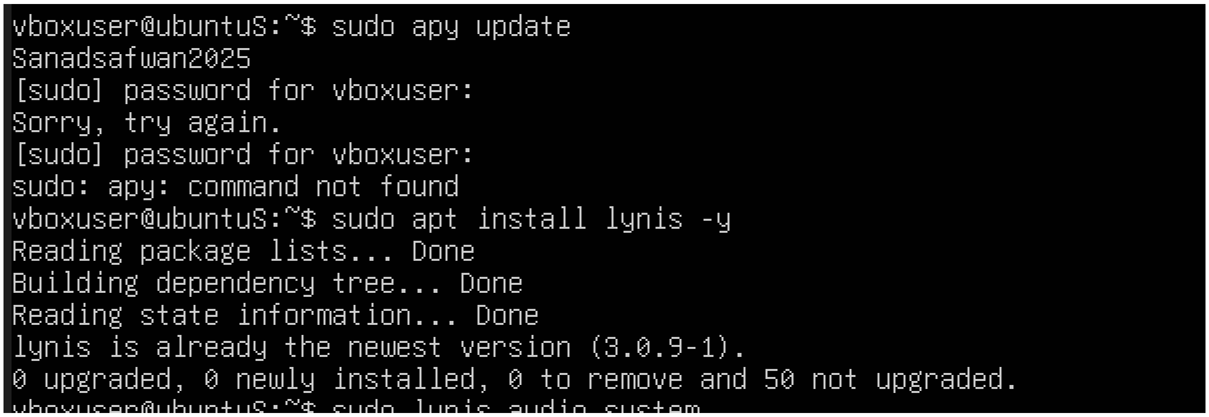
```
================================================================================

Lynis security scan details:

Hardening index : 63 [############         ]
Tests performed : 260
Plugins enabled : 1

Components:
- Firewall               [V]
- Malware scanner        [X]

Scan mode:
Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

Lynis modules:
- Compliance status      [?]
- Security audit         [V]
- Vulnerability scan     [V]

Files:
- Test and debug information      : /var/log/lynis.log
- Report data                     : /var/log/lynis-report.dat
```



```
vboxuser@ubuntuS:~$ sudo apt install nmap -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libblas3 liblinear4 liblua5.4-0 libssh2-1t64 nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  libblas3 liblinear4 liblua5.4-0 libssh2-1t64 nmap nmap-common
0 upgraded, 6 newly installed, 0 to remove and 50 not upgraded.
Need to get 6,452 kB of archives.
After this operation, 28.0 MB of additional disk space will be used.
0% [Connecting to gb.archive.ubuntu.com]
```



```
vboxuser@ubuntuS:~$ sudo apt install unattended-upfrades -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package unattended-upfrades
vboxuser@ubuntuS:~$ sudo dpkg-reconfigure unattended-upfrades
dpkg-query: package 'unattended-upfrades' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
/usr/sbin/dpkg-reconfigure: unattended-upfrades is not installed
vboxuser@ubuntuS:~$
```



```
vboxuser@ubuntuS:~$ sudo apy update
Sanadsafwan2025
[sudo] password for vboxuser:
Sorry, try again.
[sudo] password for vboxuser:
sudo: apy: command not found
vboxuser@ubuntuS:~$ sudo apt install lynis -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
lynis is already the newest version (3.0.9-1).
0 upgraded, 0 newly installed, 0 to remove and 50 not upgraded.
vboxuser@ubuntuS:~$ sudo lynis audio system
```