WEB HOSTING ON LINUX OS ON A VM

TASK 1: Installing and Configuring Apache

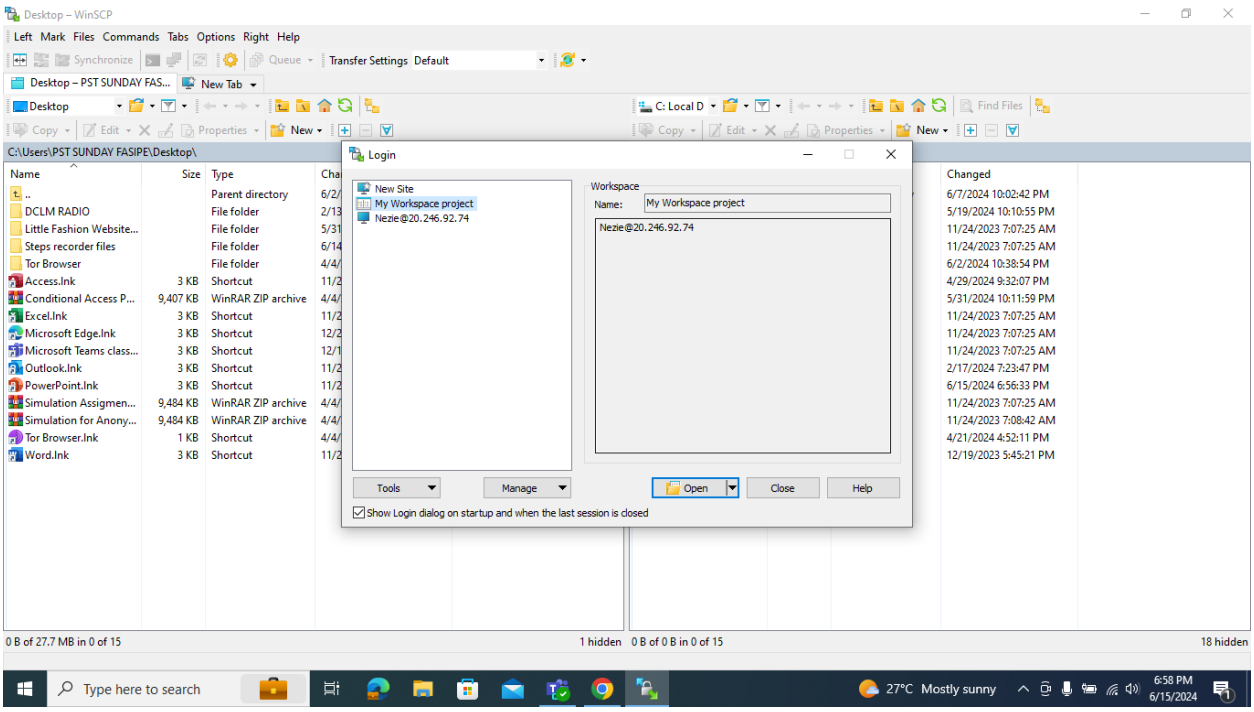
1. Update the VM
   sudo apt update
   sudo apt install apache2
2. A Directory was created named webfolder (mkdir webfolder)
3. The web template files were downloaded
4. After downloading the template, the files were saved on the desktop.
5. 'winscp' was downloaded from the browser and installed

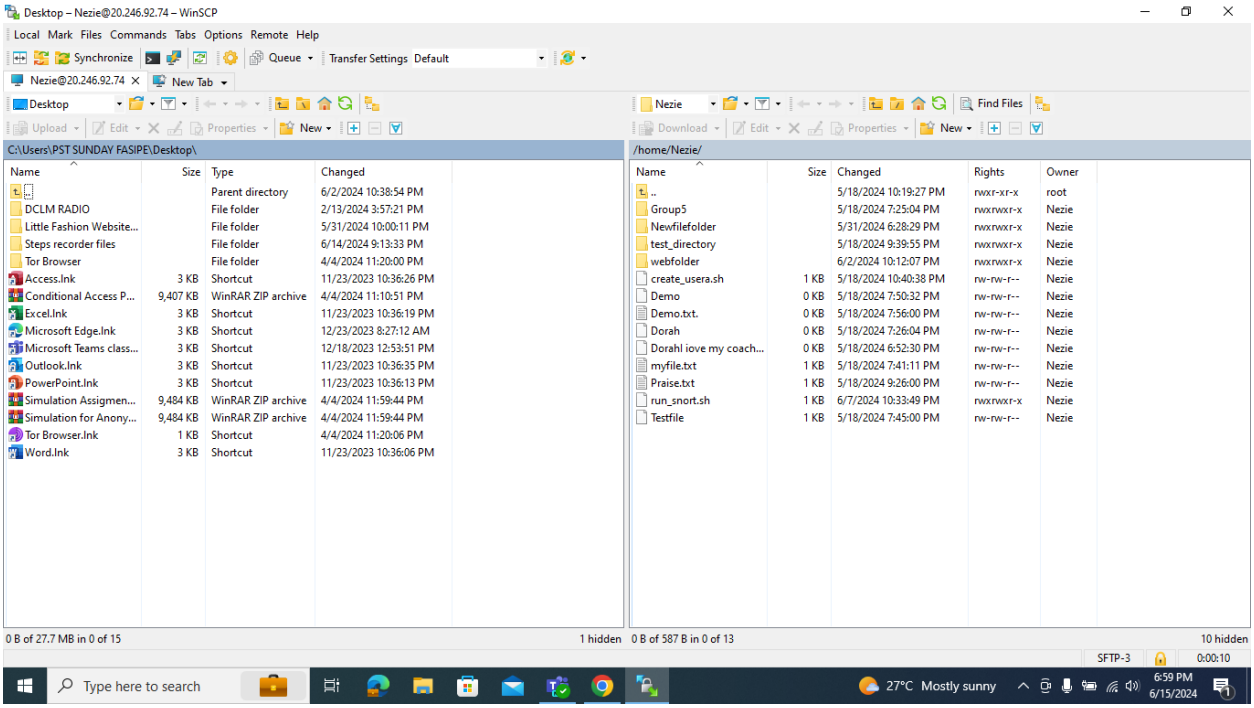
6. The installed winscp was opened and the IP address was entered as the host name, then the username accordingly.

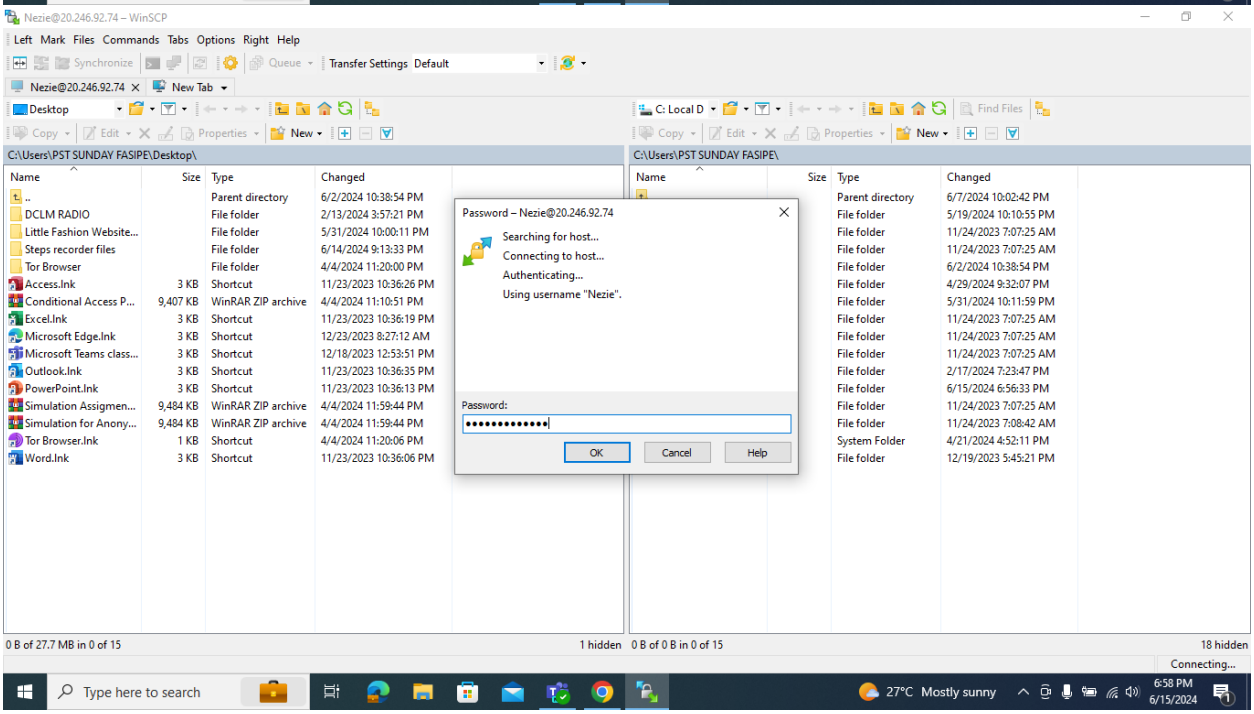
7. From the winscp, the downloaded web template files were moved to the webfolder created on the VM.

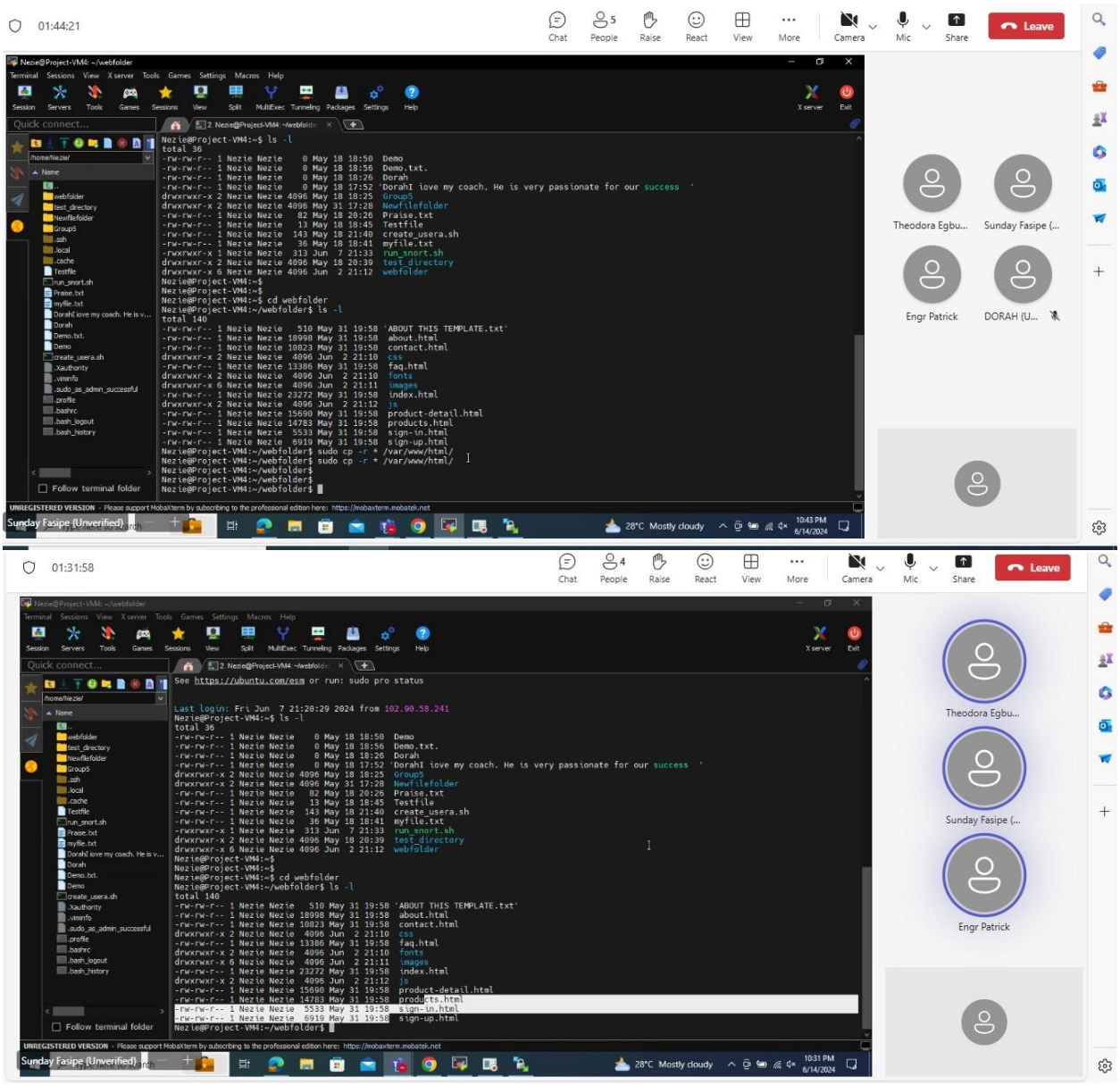
8. Then, we went back to the command line on VM to confirm the template files are already in the webfolder directory created with the command (ls -l).

9. We changed to the directory (cd webfolder) and run the command (sudo cp -r * /var/www/html/).



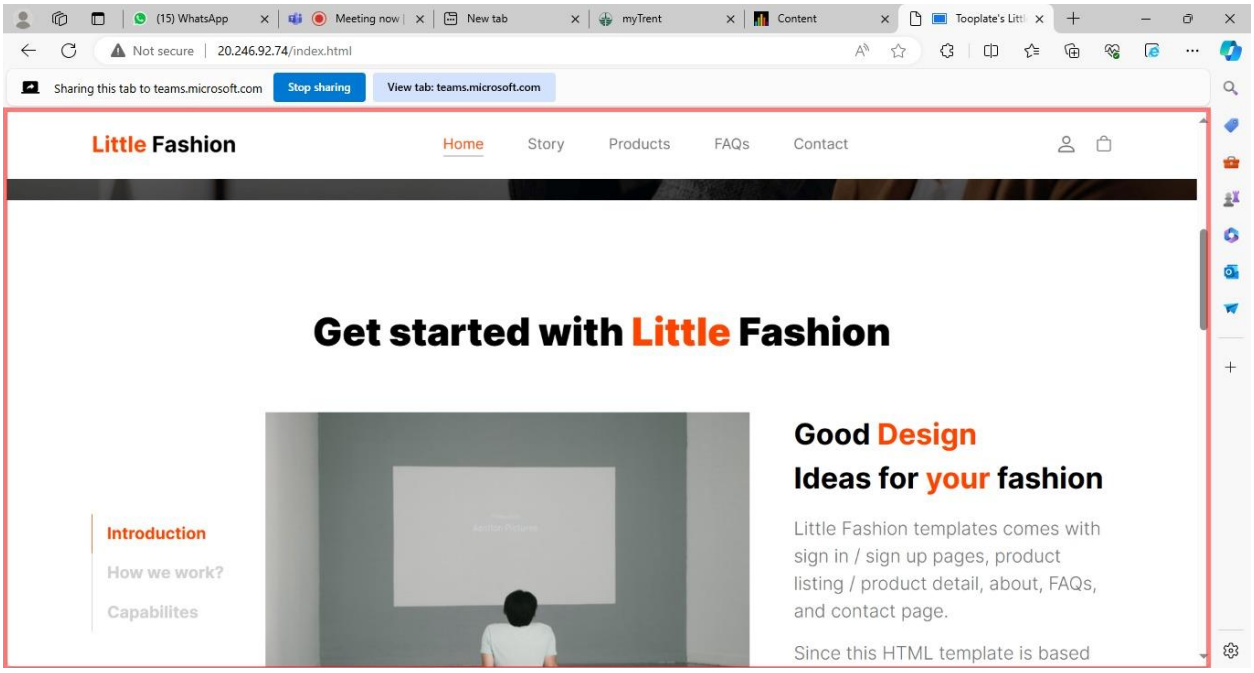

Desktop – Nezie@20.246.92.74 – WinSCP
Local Mark Files Commands Tabs Options Remote Help
Synchronize
Queue
Transfer Settings Default
Nezie@20.246.92.74
New Tab
Desktop
Upload
Edit
Properties
New
C:\Users\PST SUNDAY FASIPE\Desktop\
Name Size Type Changed
Parent directory 6/2/2024 10:38:54 PM
DCLM RADIO File folder 2/13/2024 3:57:21 PM
Little Fashion Website... File folder 5/31/2024 10:00:11 PM
Steps recorder files File folder 6/14/2024 9:13:33 PM
Tor Browser File folder 4/4/2024 11:20:00 PM
Access.lnk 3 KB Shortcut 11/23/2023 10:36:26 PM
Conditional Access P... 9,407 KB WinRAR ZIP archive 4/4/2024 11:10:51 PM
Excel.lnk 3 KB Shortcut 11/23/2023 10:36:19 PM
Microsoft Edge.lnk 3 KB Shortcut 12/23/2023 8:27:12 AM
Microsoft Teams class... 3 KB Shortcut 12/18/2023 12:53:51 PM
Outlook.lnk 3 KB Shortcut 11/23/2023 10:36:35 PM
PowerPoint.lnk 3 KB Shortcut 11/23/2023 10:36:13 PM
Simulation Assigmen... 9,484 KB WinRAR ZIP archive 4/4/2024 11:59:44 PM
Simulation for Anony... 9,484 KB WinRAR ZIP archive 4/4/2024 11:59:44 PM
Tor Browser.lnk 1 KB Shortcut 4/4/2024 11:20:06 PM
Word.lnk 3 KB Shortcut 11/23/2023 10:36:06 PM
0 B of 27.7 MB in 0 of 15
1 hidden
Nezie
Download
Edit
Properties
New
Find Files
/home/Nezie/
Name Size Changed Rights Owner
.. 5/18/2024 10:19:27 PM rwxr-xr-x root
Group5 5/18/2024 7:25:04 PM rwxrwxr-x Nezie
Newfilefolder 5/31/2024 6:28:29 PM rwxrwxr-x Nezie
test_directory 5/18/2024 9:39:55 PM rwxrwxr-x Nezie
webfolder 6/2/2024 10:12:07 PM rwxrwxr-x Nezie
create_usera.sh 1 KB 5/18/2024 10:40:38 PM rw-rw-r-- Nezie
Demo 0 KB 5/18/2024 7:50:32 PM rw-rw-r-- Nezie
Demo.txt. 0 KB 5/18/2024 7:56:00 PM rw-rw-r-- Nezie
Dorah 0 KB 5/18/2024 7:26:04 PM rw-rw-r-- Nezie
Dorahl iove my coach... 0 KB 5/18/2024 6:52:30 PM rw-rw-r-- Nezie
myfile.txt 1 KB 5/18/2024 7:41:11 PM rw-rw-r-- Nezie
Praise.txt 1 KB 5/18/2024 9:26:00 PM rw-rw-r-- Nezie
run_snort.sh 1 KB 6/7/2024 10:33:49 PM rwxrwxr-x Nezie
Testfile 1 KB 5/18/2024 7:45:00 PM rw-rw-r-- Nezie
0 B of 587 B in 0 of 13
10 hidden
SFTP-3
0:00:10
Type here to search
27°C Mostly sunny
6:59 PM
6/15/2024


Nezie@20.246.92.74 – WinSCP
Left Mark Files Commands Tabs Options Right Help
Synchronize
Queue
Transfer Settings Default
Nezie@20.246.92.74
New Tab
Desktop
Copy
Edit
Properties
New
C:\Users\PST SUNDAY FASIPE\Desktop\
Name Size Type Changed
Parent directory 6/2/2024 10:38:54 PM
DCLM RADIO File folder 2/13/2024 3:57:21 PM
Little Fashion Website... File folder 5/31/2024 10:00:11 PM
Steps recorder files File folder 6/14/2024 9:13:33 PM
Tor Browser File folder 4/4/2024 11:20:00 PM
Access.lnk 3 KB Shortcut 11/23/2023 10:36:26 PM
Conditional Access P... 9,407 KB WinRAR ZIP archive 4/4/2024 11:10:51 PM
Excel.lnk 3 KB Shortcut 11/23/2023 10:36:19 PM
Microsoft Edge.lnk 3 KB Shortcut 12/23/2023 8:27:12 AM
Microsoft Teams class... 3 KB Shortcut 12/18/2023 12:53:51 PM
Outlook.lnk 3 KB Shortcut 11/23/2023 10:36:35 PM
PowerPoint.lnk 3 KB Shortcut 11/23/2023 10:36:13 PM
Simulation Assigmen... 9,484 KB WinRAR ZIP archive 4/4/2024 11:59:44 PM
Simulation for Anony... 9,484 KB WinRAR ZIP archive 4/4/2024 11:59:44 PM
Tor Browser.lnk 1 KB Shortcut 4/4/2024 11:20:06 PM
Word.lnk 3 KB Shortcut 11/23/2023 10:36:06 PM
0 B of 27.7 MB in 0 of 15
1 hidden
Password – Nezie@20.246.92.74
Searching for host...
Connecting to host...
Authenticating...
Using username "Nezie".
Password:
OK
Cancel
Help
C: Local D
Find Files
C:\Users\PST SUNDAY FASIPE\
Name Size Type Changed
Parent directory 6/7/2024 10:02:42 PM
File folder 5/19/2024 10:10:55 PM
File folder 11/24/2023 7:07:25 AM
File folder 11/24/2023 7:07:25 AM
File folder 6/2/2024 10:38:54 PM
File folder 4/29/2024 9:32:07 PM
File folder 5/31/2024 10:11:59 PM
File folder 11/24/2023 7:07:25 AM
File folder 11/24/2023 7:07:25 AM
File folder 11/24/2023 7:07:25 AM
File folder 2/17/2024 7:23:47 PM
File folder 6/15/2024 6:56:33 PM
File folder 11/24/2023 7:07:25 AM
File folder 11/24/2023 7:08:42 AM
System Folder 4/21/2024 4:52:11 PM
File folder 12/19/2023 5:45:21 PM
0 B of 0 B in 0 of 15
18 hidden
Connecting...
Type here to search
27°C Mostly sunny
6:58 PM
6/15/2024



10. We then typed the IP address on the window browser to reload the webserver to confirm that the website is setup on the VM.


10:57
20.246.92.74
Little Fashion
Retail sh
owners
TE
EXPLORE PRODUCTS
Clear all
3.99 GB AVAILABLE /8.00 GB

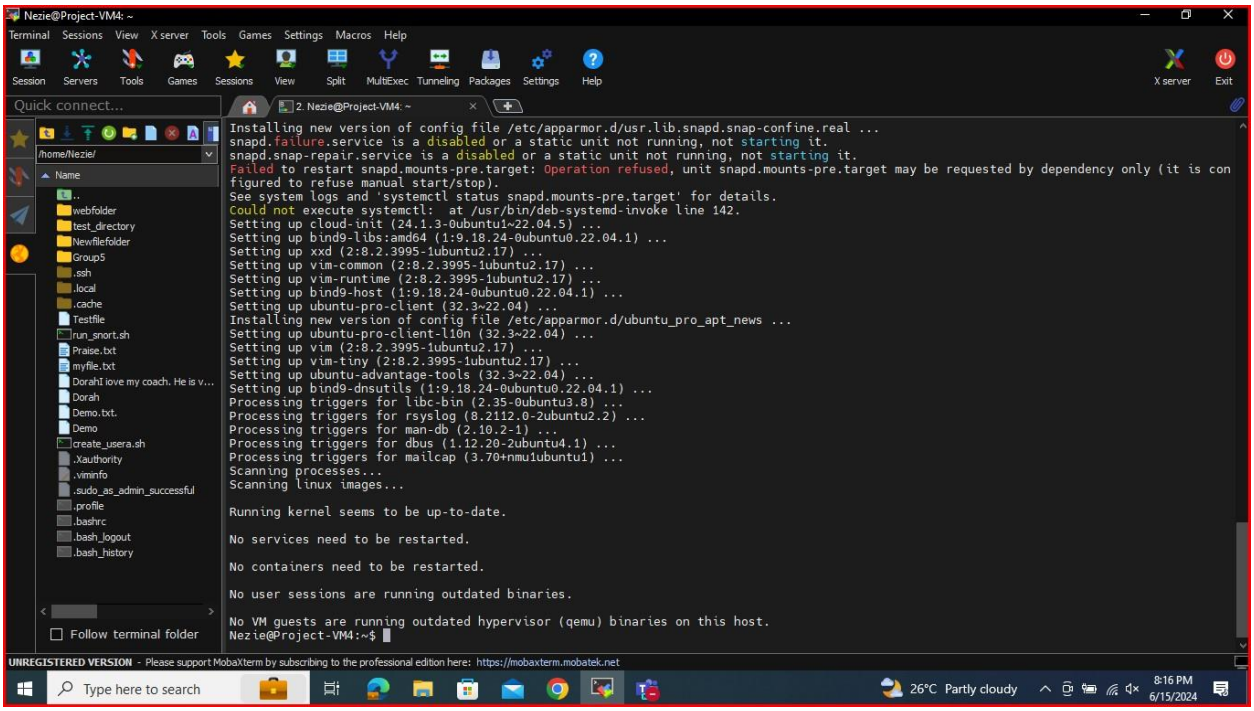


TASK 2: SECURITY AUDIT AND FILE INTEGRITY CHECK

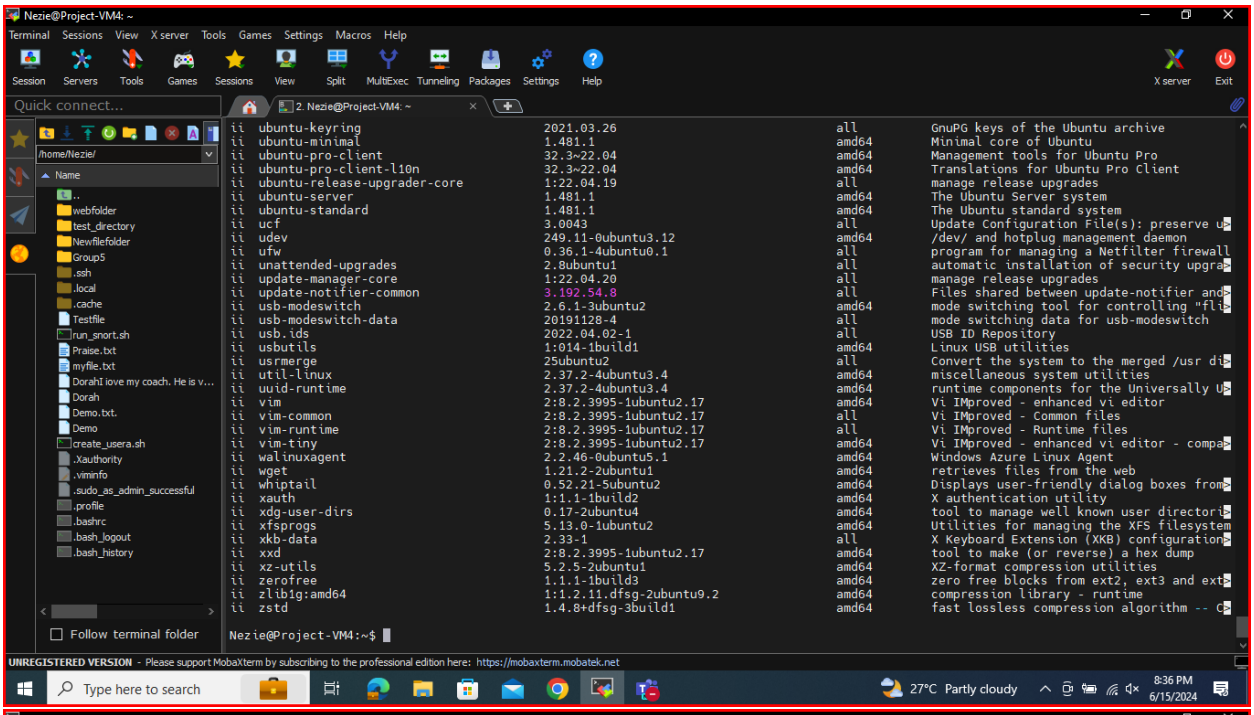
In order to perform security audit, the following steps were followed.

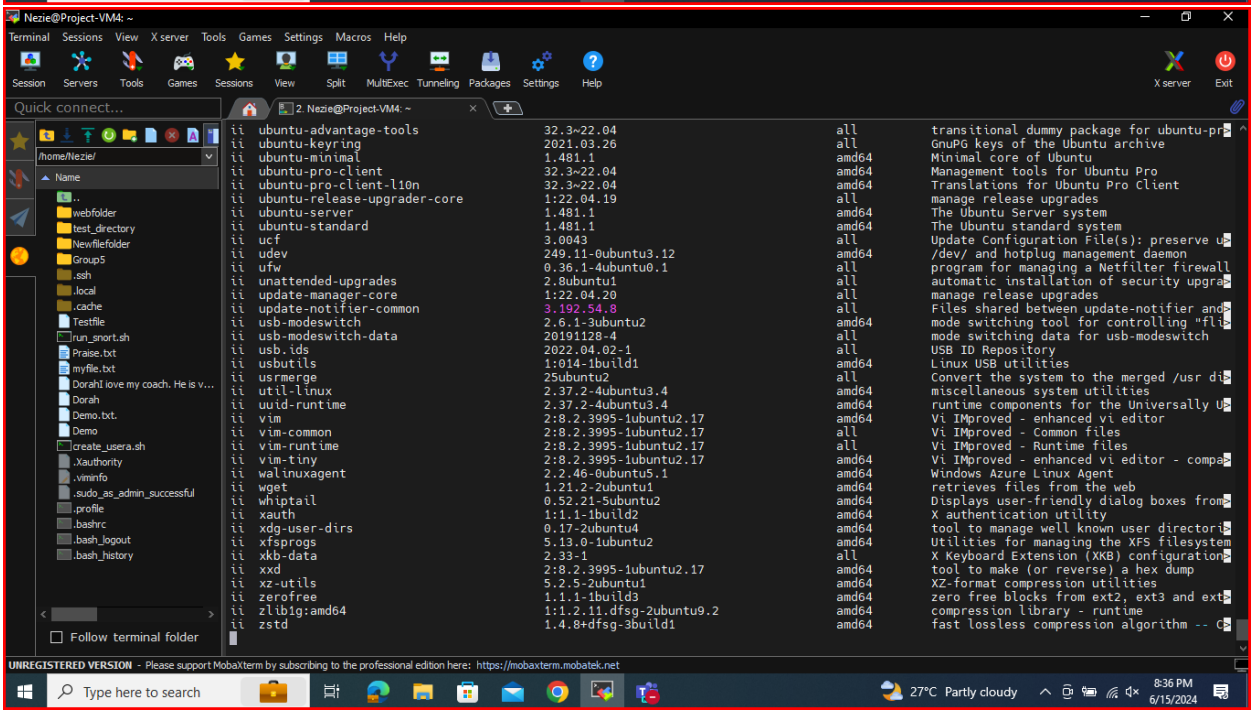
Step 1: Initial Security Audit

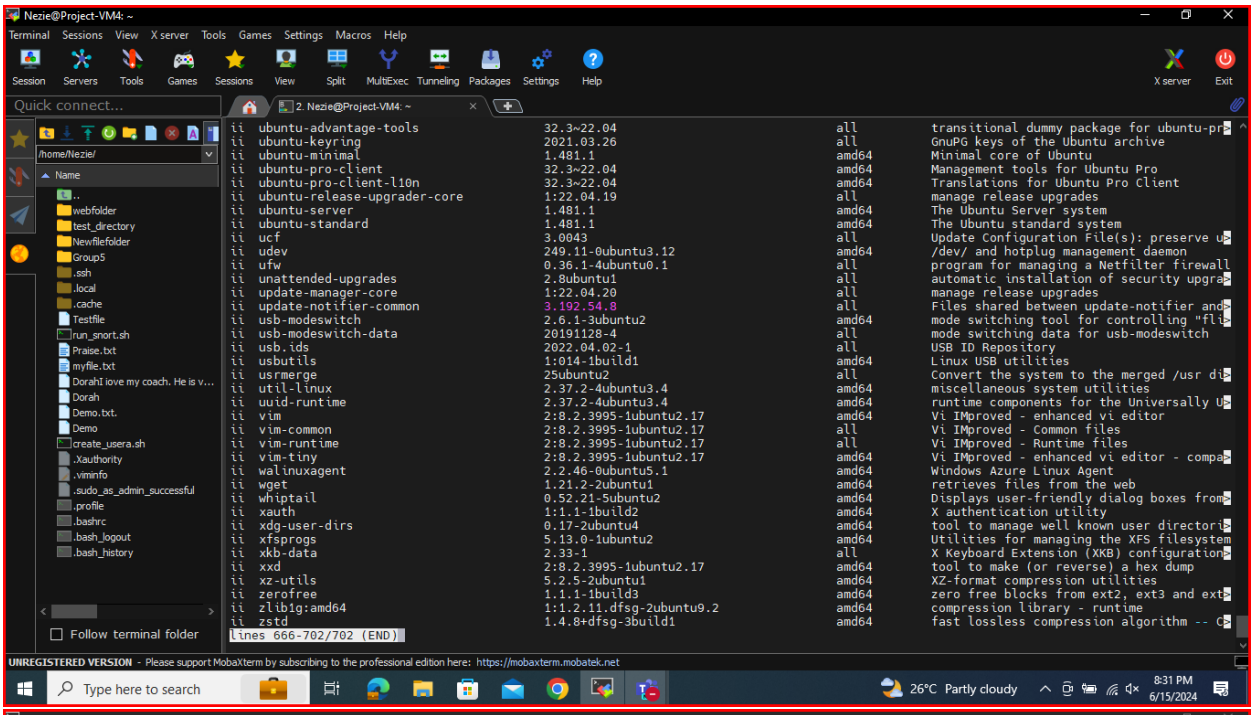
1. System Update was carried out to ensure the system is up-to-date with the latest patches and security by running this command
   Sudo apt update && sudo apt upgrade -y

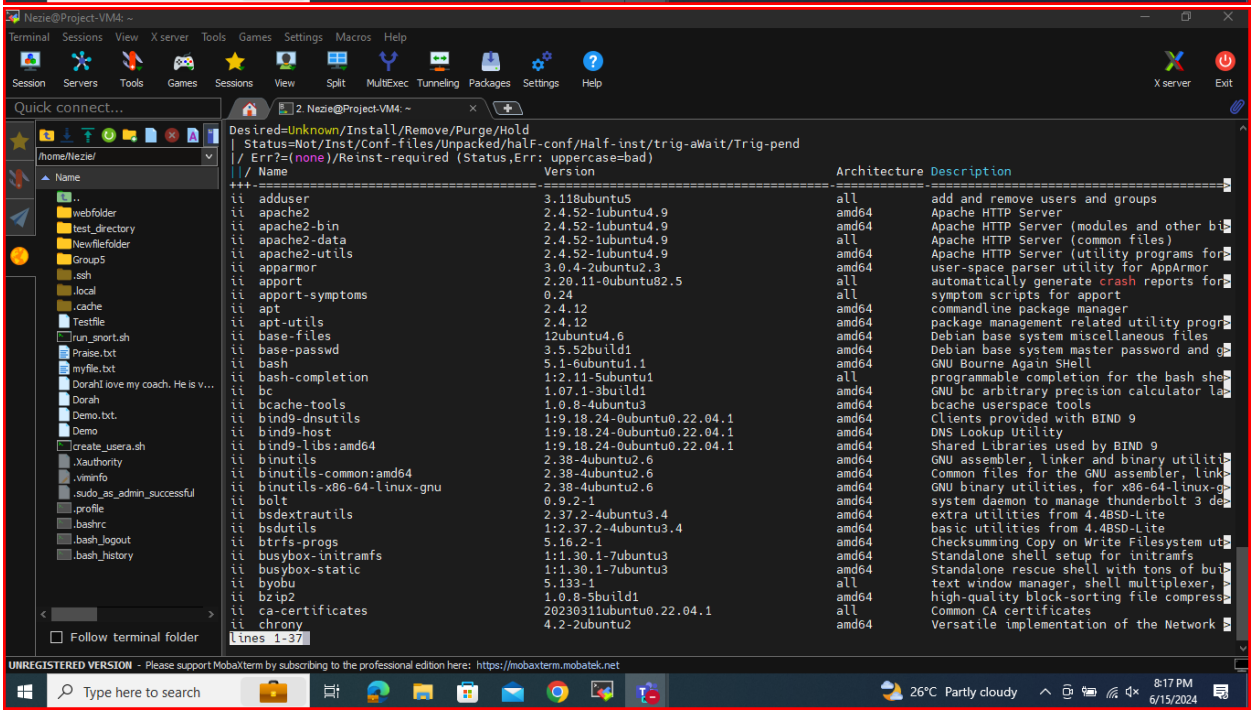


2. Review of installed Packages: We reviewed all installed packages in order to remove unnecessary ones with this command dpkg --list

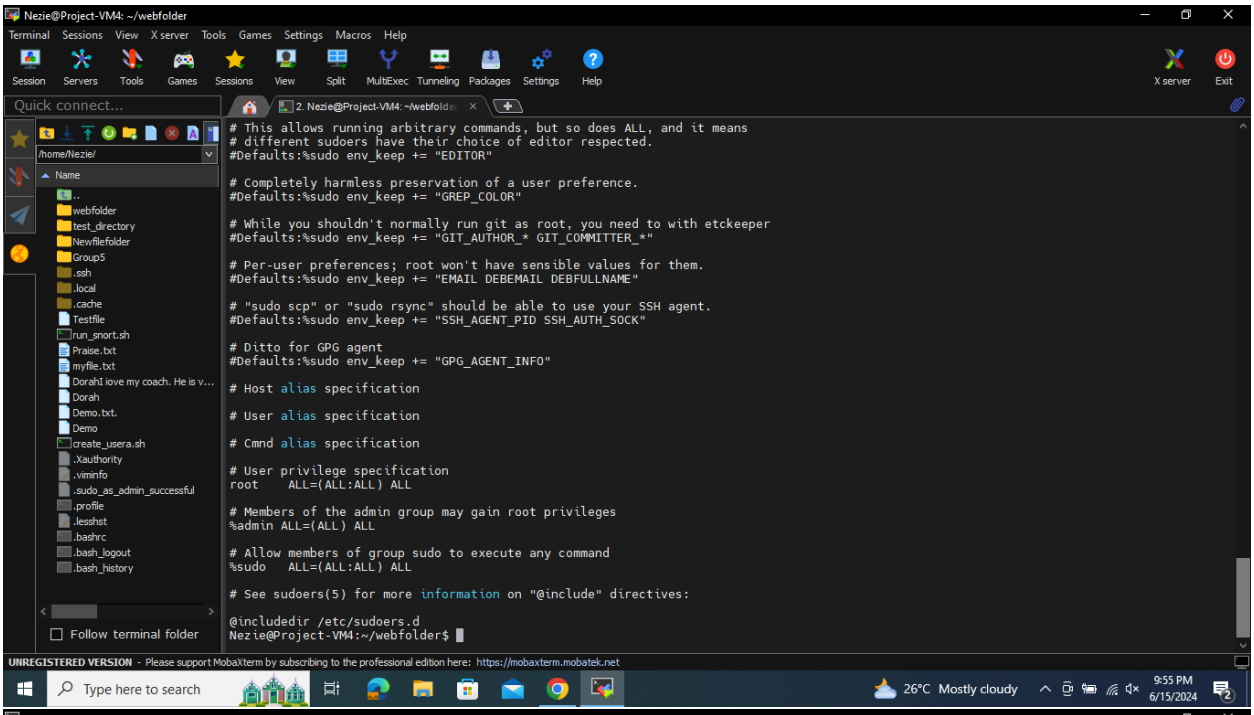

Nezie@Project-VM4: ~
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
Dorah‌I iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.bashrc
.bash_logout
.bash_history
Follow terminal folder
ii ubuntu-keyring 2021.03.26 all GnuPG keys of the Ubuntu archive
ii ubuntu-minimal 1.481.1 amd64 Minimal core of Ubuntu
ii ubuntu-pro-client 32.3~22.04 amd64 Management tools for Ubuntu Pro
ii ubuntu-pro-client-l10n 32.3~22.04 amd64 Translations for Ubuntu Pro Client
ii ubuntu-release-upgrader-core 1:22.04.19 all manage release upgrades
ii ubuntu-server 1.481.1 amd64 The Ubuntu Server system
ii ubuntu-standard 1.481.1 amd64 The Ubuntu standard system
ii ucf 3.0043 all Update Configuration File(s): preserve u
ii udev 249.11-0ubuntu3.12 amd64 /dev/ and hotplug management daemon
ii ufw 0.36.1-4ubuntu0.1 all program for managing a Netfilter firewall
ii unattended-upgrades 2.8ubuntu1 all automatic installation of security upgra
ii update-manager-core 1:22.04.20 all manage release upgrades
ii update-notifier-common 3.192.54.8 all Files shared between update-notifier and
ii usb-modeswitch 2.6.1-3ubuntu2 amd64 mode switching tool for controlling "fli
ii usb-modeswitch-data 20191128-4 all mode switching data for usb-modeswitch
ii usb.ids 2022.04.02-1 all USB ID Repository
ii usbutils 1:014-1build1 amd64 Linux USB utilities
ii usrmerge 25ubuntu2 all Convert the system to the merged /usr di
ii util-linux 2.37.2-4ubuntu3.4 amd64 miscellaneous system utilities
ii uuid-runtime 2.37.2-4ubuntu3.4 amd64 runtime components for the Universally U
ii vim 2:8.2.3995-1ubuntu2.17 amd64 Vi IMproved - enhanced vi editor
ii vim-common 2:8.2.3995-1ubuntu2.17 all Vi IMproved - Common files
ii vim-runtime 2:8.2.3995-1ubuntu2.17 all Vi IMproved - Runtime files
ii vim-tiny 2:8.2.3995-1ubuntu2.17 amd64 Vi IMproved - enhanced vi editor - compa
ii walinuxagent 2.2.46-0ubuntu5.1 amd64 Windows Azure Linux Agent
ii wget 1.21.2-2ubuntu1 amd64 retrieves files from the web
ii whiptail 0.52.21-5ubuntu2 amd64 Displays user-friendly dialog boxes from
ii xauth 1:1.1-1build2 amd64 X authentication utility
ii xdg-user-dirs 0.17-2ubuntu4 amd64 tool to manage well known user directori
ii xfsprogs 5.13.0-1ubuntu2 amd64 Utilities for managing the XFS filesystem
ii xkb-data 2.33-1 all X Keyboard Extension (XKB) configuration
ii xxd 2:8.2.3995-1ubuntu2.17 amd64 tool to make (or reverse) a hex dump
ii xz-utils 5.2.5-2ubuntu1 amd64 XZ-format compression utilities
ii zerofree 1.1.1-1build3 amd64 zero free blocks from ext2, ext3 and ext
ii zlib1g:amd64 1:1.2.11.dfsg-2ubuntu9.2 amd64 compression library - runtime
ii zstd 1.4.8+dfsg-3build1 amd64 fast lossless compression algorithm -- C
Nezie@Project-VM4:~$
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
27°C Partly cloudy
8:36 PM
6/15/2024

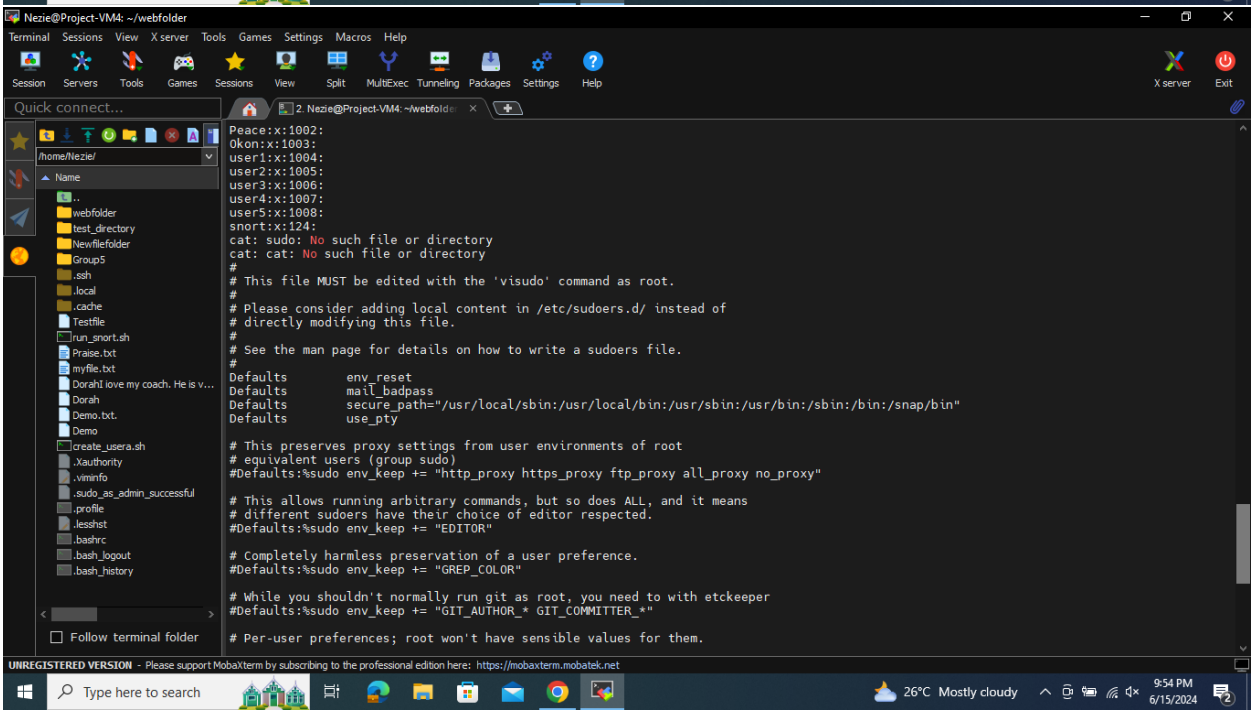

Nezie@Project-VM4: ~
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
Dorah‌I iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.bashrc
.bash_logout
.bash_history
Follow terminal folder
ii ubuntu-advantage-tools 32.3~22.04 all transitional dummy package for ubuntu-pr
ii ubuntu-keyring 2021.03.26 all GnuPG keys of the Ubuntu archive
ii ubuntu-minimal 1.481.1 amd64 Minimal core of Ubuntu
ii ubuntu-pro-client 32.3~22.04 amd64 Management tools for Ubuntu Pro
ii ubuntu-pro-client-l10n 32.3~22.04 amd64 Translations for Ubuntu Pro Client
ii ubuntu-release-upgrader-core 1:22.04.19 all manage release upgrades
ii ubuntu-server 1.481.1 amd64 The Ubuntu Server system
ii ubuntu-standard 1.481.1 amd64 The Ubuntu standard system
ii ucf 3.0043 all Update Configuration File(s): preserve u
ii udev 249.11-0ubuntu3.12 amd64 /dev/ and hotplug management daemon
ii ufw 0.36.1-4ubuntu0.1 all program for managing a Netfilter firewall
ii unattended-upgrades 2.8ubuntu1 all automatic installation of security upgra
ii update-manager-core 1:22.04.20 all manage release upgrades
ii update-notifier-common 3.192.54.8 all Files shared between update-notifier and
ii usb-modeswitch 2.6.1-3ubuntu2 amd64 mode switching tool for controlling "fli
ii usb-modeswitch-data 20191128-4 all mode switching data for usb-modeswitch
ii usb.ids 2022.04.02-1 all USB ID Repository
ii usbutils 1:014-1build1 amd64 Linux USB utilities
ii usrmerge 25ubuntu2 all Convert the system to the merged /usr di
ii util-linux 2.37.2-4ubuntu3.4 amd64 miscellaneous system utilities
ii uuid-runtime 2.37.2-4ubuntu3.4 amd64 runtime components for the Universally U
ii vim 2:8.2.3995-1ubuntu2.17 amd64 Vi IMproved - enhanced vi editor
ii vim-common 2:8.2.3995-1ubuntu2.17 all Vi IMproved - Common files
ii vim-runtime 2:8.2.3995-1ubuntu2.17 all Vi IMproved - Runtime files
ii vim-tiny 2:8.2.3995-1ubuntu2.17 amd64 Vi IMproved - enhanced vi editor - compa
ii walinuxagent 2.2.46-0ubuntu5.1 amd64 Windows Azure Linux Agent
ii wget 1.21.2-2ubuntu1 amd64 retrieves files from the web
ii whiptail 0.52.21-5ubuntu2 amd64 Displays user-friendly dialog boxes from
ii xauth 1:1.1-1build2 amd64 X authentication utility
ii xdg-user-dirs 0.17-2ubuntu4 amd64 tool to manage well known user directori
ii xfsprogs 5.13.0-1ubuntu2 amd64 Utilities for managing the XFS filesystem
ii xkb-data 2.33-1 all X Keyboard Extension (XKB) configuration
ii xxd 2:8.2.3995-1ubuntu2.17 amd64 tool to make (or reverse) a hex dump
ii xz-utils 5.2.5-2ubuntu1 amd64 XZ-format compression utilities
ii zerofree 1.1.1-1build3 amd64 zero free blocks from ext2, ext3 and ext
ii zlib1g:amd64 1:1.2.11.dfsg-2ubuntu9.2 amd64 compression library - runtime
ii zstd 1.4.8+dfsg-3build1 amd64 fast lossless compression algorithm -- C
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
27°C Partly cloudy
8:36 PM
6/15/2024

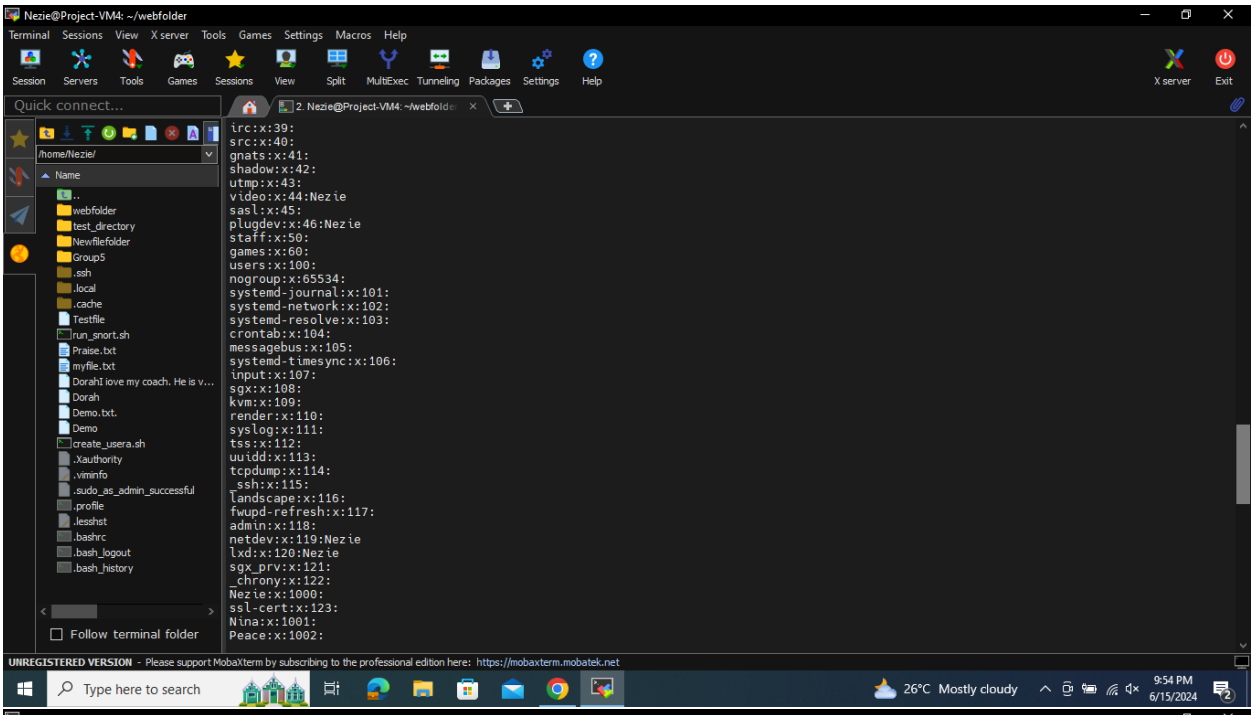


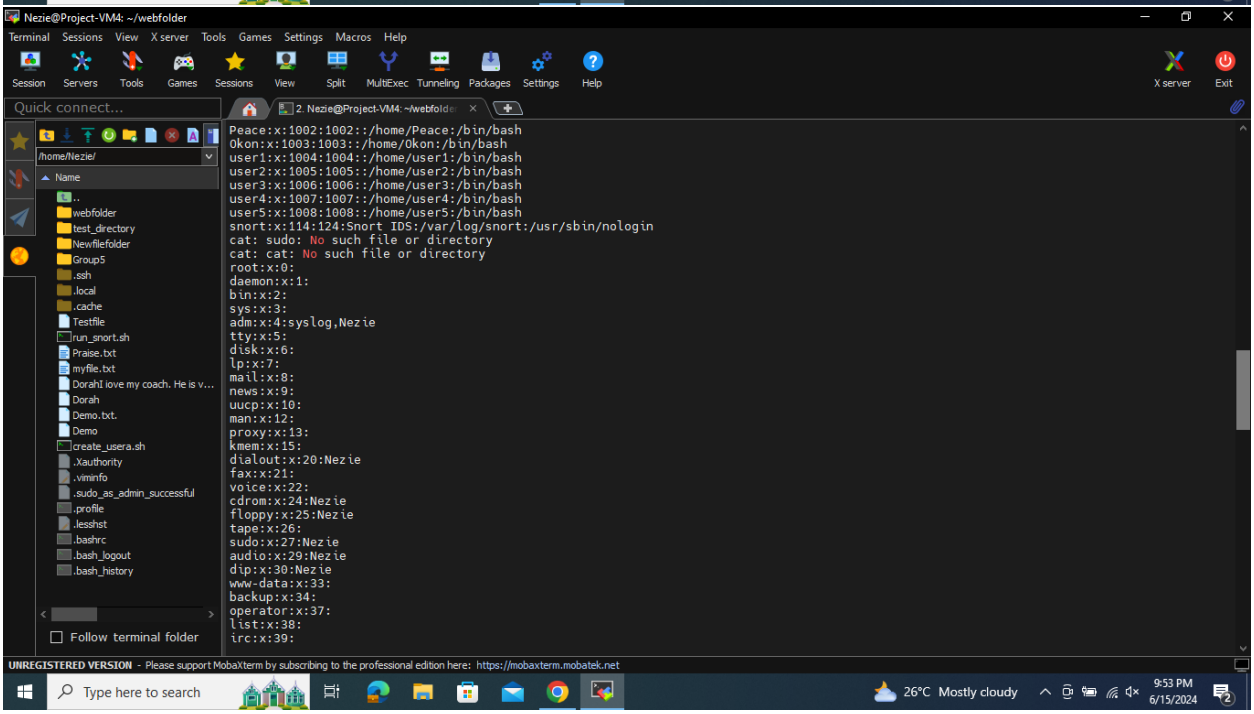


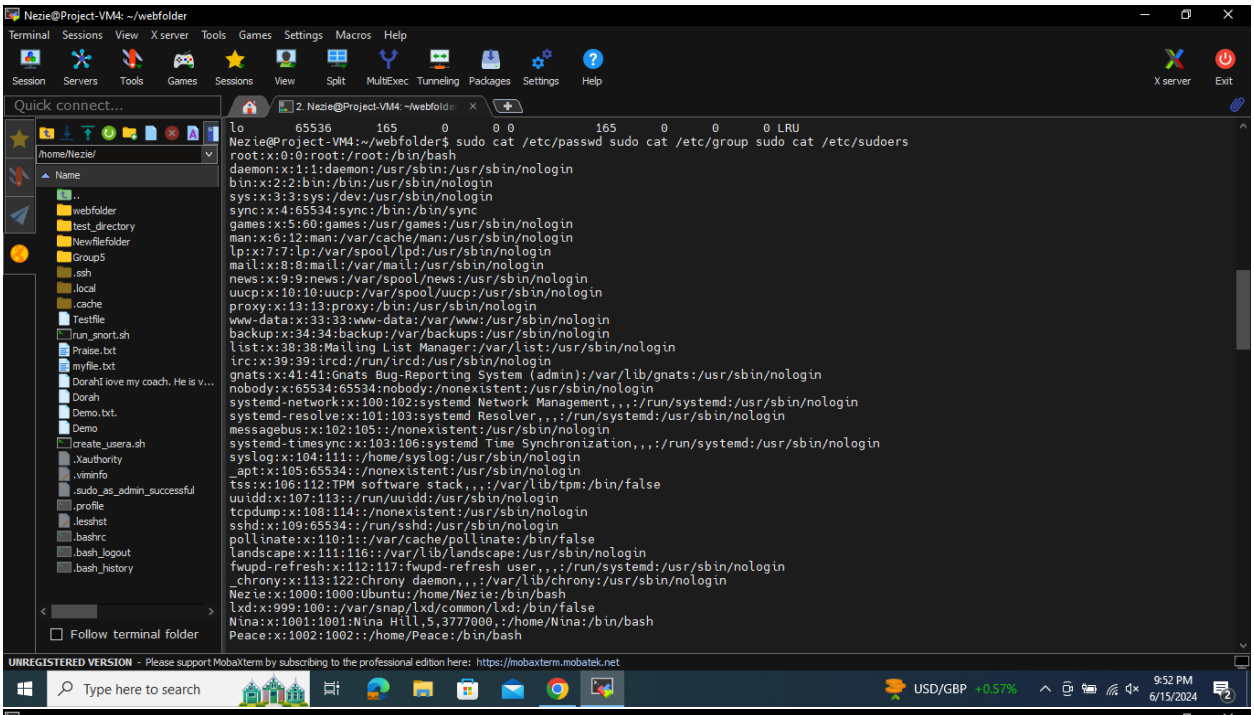
3. Checking for Open Ports: Open ports and associated services were identified by issuing these commands
   sudo netstat -tulnp
   sudo lsof -I -P -n


Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolder
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
This allows running arbitrary commands, but so does ALL, and it means
different sudoers have their choice of editor respected.
#Defaults:%sudo env_keep += "EDITOR"
Completely harmless preservation of a user preference.
#Defaults:%sudo env_keep += "GREP_COLOR"
While you shouldn't normally run git as root, you need to with etckeeper
#Defaults:%sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER_*"
Per-user preferences; root won't have sensible values for them.
#Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"
"sudo scp" or "sudo rsync" should be able to use your SSH agent.
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"
Ditto for GPG agent
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"
Host alias specification
User alias specification
Cmnd alias specification
User privilege specification
root ALL=(ALL:ALL) ALL
Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
Allow members of group sudo to execute any command
%sudo ALL=(ALL:ALL) ALL
See sudoers(5) for more information on "@include" directives:
@includedir /etc/sudoers.d
Nezie@Project-VM4:~/webfolder$
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
9:55 PM
6/15/2024

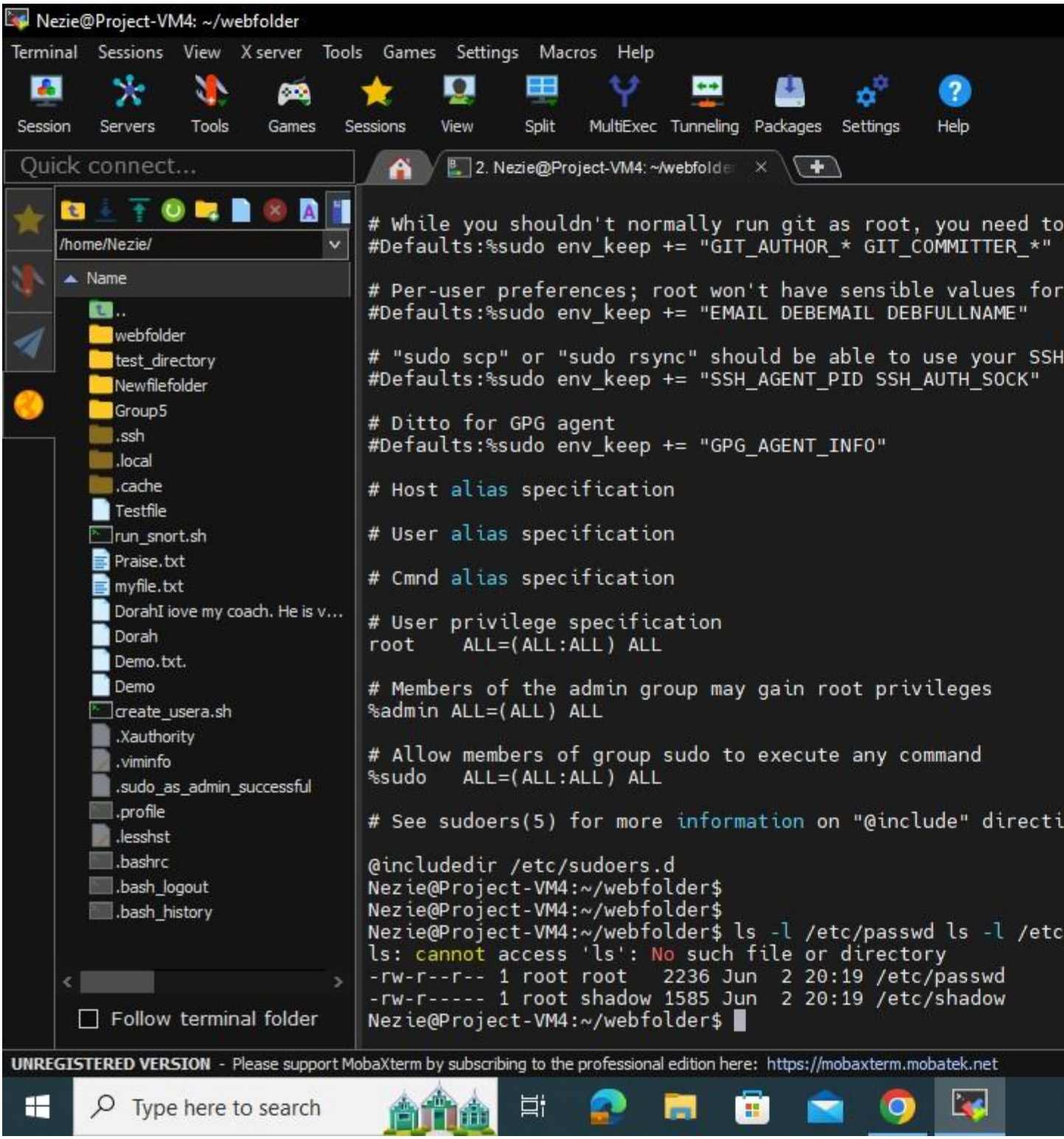

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolder
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Peace:x:1002:
Okon:x:1003:
user1:x:1004:
user2:x:1005:
user3:x:1006:
user4:x:1007:
user5:x:1008:
snort:x:124:
cat: sudo: No such file or directory
cat: cat: No such file or directory
#
This file MUST be edited with the 'visudo' command as root.
#
Please consider adding local content in /etc/sudoers.d/ instead of
directly modifying this file.
#
See the man page for details on how to write a sudoers file.
#
Defaults env_reset
Defaults mail_badpass
Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"
Defaults use_pty
This preserves proxy settings from user environments of root
equivalent users (group sudo)
#Defaults:%sudo env_keep += "http_proxy https_proxy ftp_proxy all_proxy no_proxy"
This allows running arbitrary commands, but so does ALL, and it means
different sudoers have their choice of editor respected.
#Defaults:%sudo env_keep += "EDITOR"
Completely harmless preservation of a user preference.
#Defaults:%sudo env_keep += "GREP_COLOR"
While you shouldn't normally run git as root, you need to with etckeeper
#Defaults:%sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER_*"
Per-user preferences; root won't have sensible values for them.
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
9:54 PM
6/15/2024


Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:Nezie
sasl:x:45:
plugdev:x:46:Nezie
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:101:
systemd-network:x:102:
systemd-resolve:x:103:
crontab:x:104:
messagebus:x:105:
systemd-timesync:x:106:
input:x:107:
sgx:x:108:
kvm:x:109:
render:x:110:
syslog:x:111:
tss:x:112:
uuidd:x:113:
tcpdump:x:114:
_ssh:x:115:
landscape:x:116:
fwupd-refresh:x:117:
admin:x:118:
netdev:x:119:Nezie
lxd:x:120:Nezie
sgx_prv:x:121:
_chrony:x:122:
Nezie:x:1000:
ssl-cert:x:123:
Nina:x:1001:
Peace:x:1002:
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
9:54 PM
6/15/2024

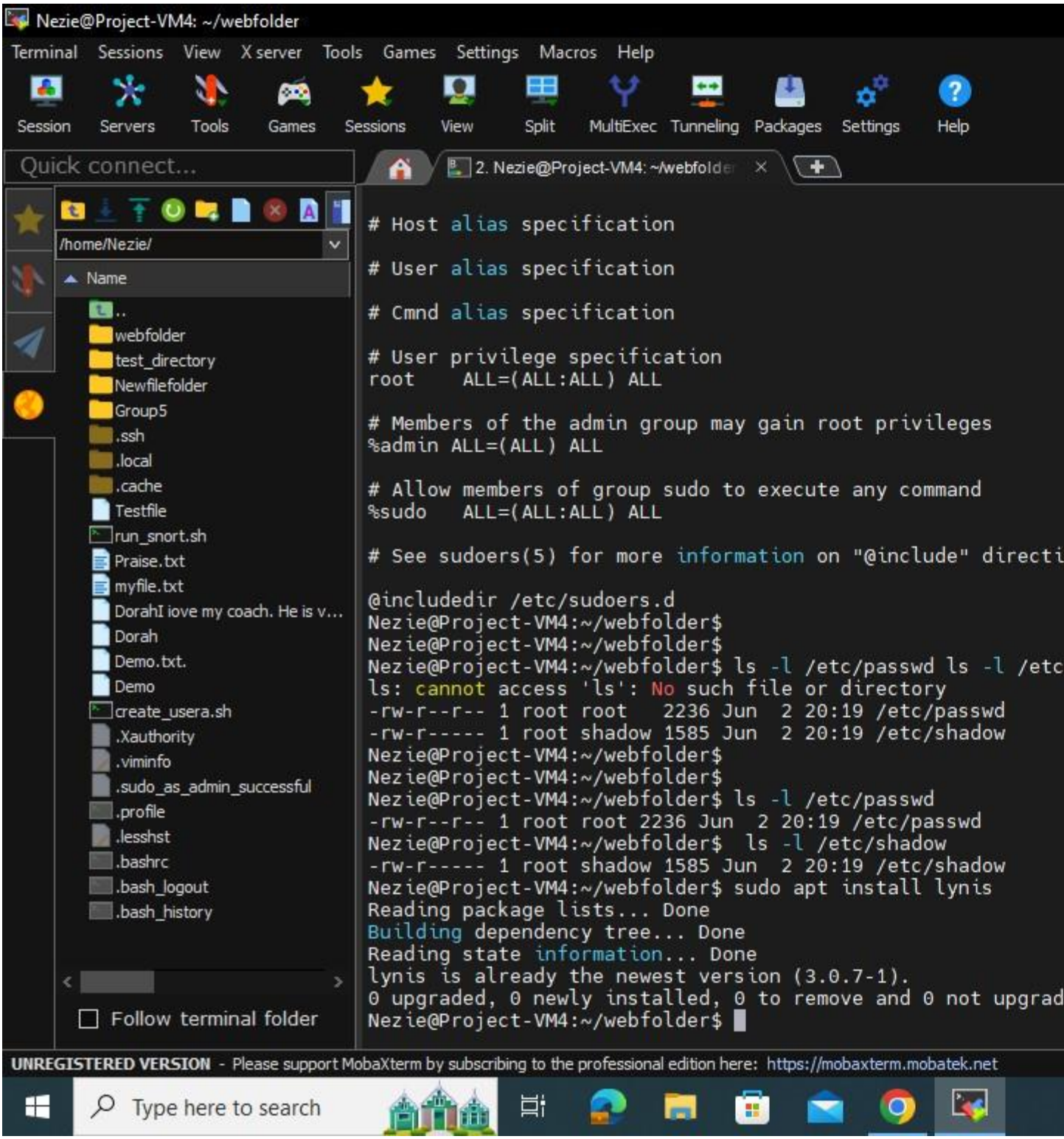

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Peace:x:1002:1002::/home/Peace:/bin/bash
Okon:x:1003:1003::/home/Okon:/bin/bash
user1:x:1004:1004::/home/user1:/bin/bash
user2:x:1005:1005::/home/user2:/bin/bash
user3:x:1006:1006::/home/user3:/bin/bash
user4:x:1007:1007::/home/user4:/bin/bash
user5:x:1008:1008::/home/user5:/bin/bash
snort:x:114:124:Snort IDS:/var/log/snort:/usr/sbin/nologin
cat: sudo: No such file or directory
cat: cat: No such file or directory
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,Nezie
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:Nezie
fax:x:21:
voice:x:22:
cdrom:x:24:Nezie
floppy:x:25:Nezie
tape:x:26:
sudo:x:27:Nezie
audio:x:29:Nezie
dip:x:30:Nezie
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
9:53 PM
6/15/2024



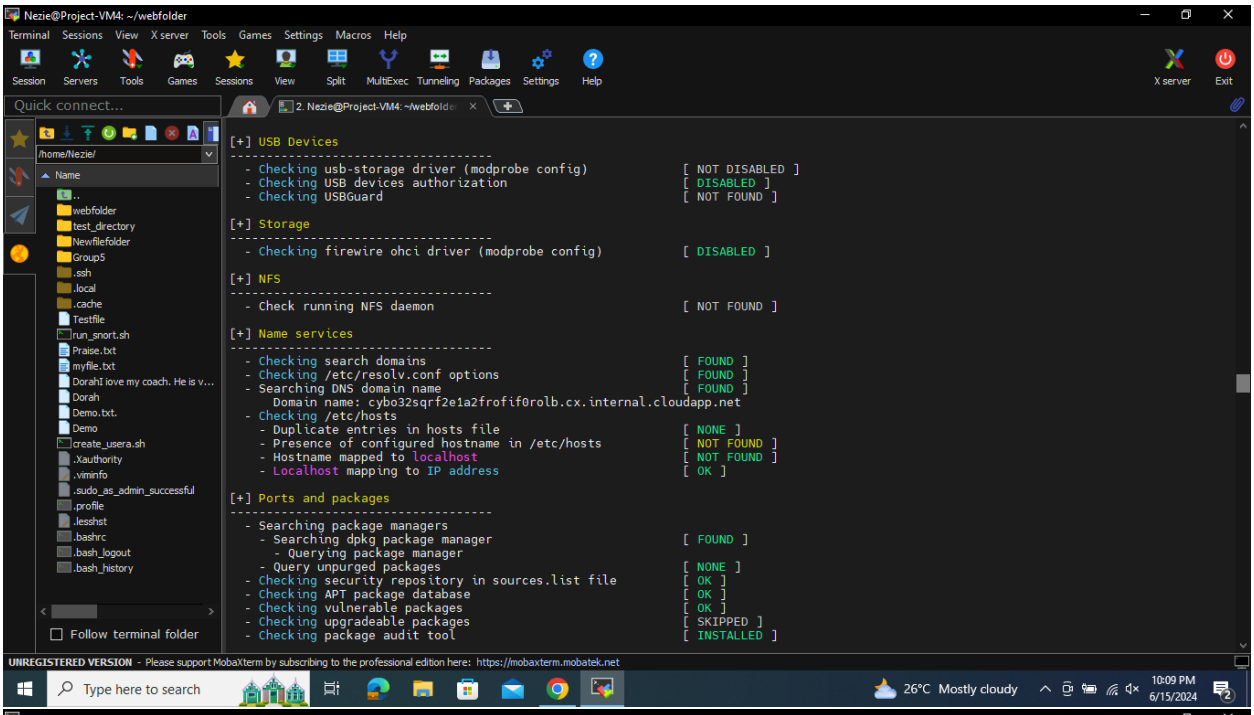
4. **Audit System Accounts:** Review all user accounts, especially those with root or sudo privileges
   Commands used: sudo cat /etc/passwd
   sudo cat /etc/group
   sudo cat /etc/sudoers

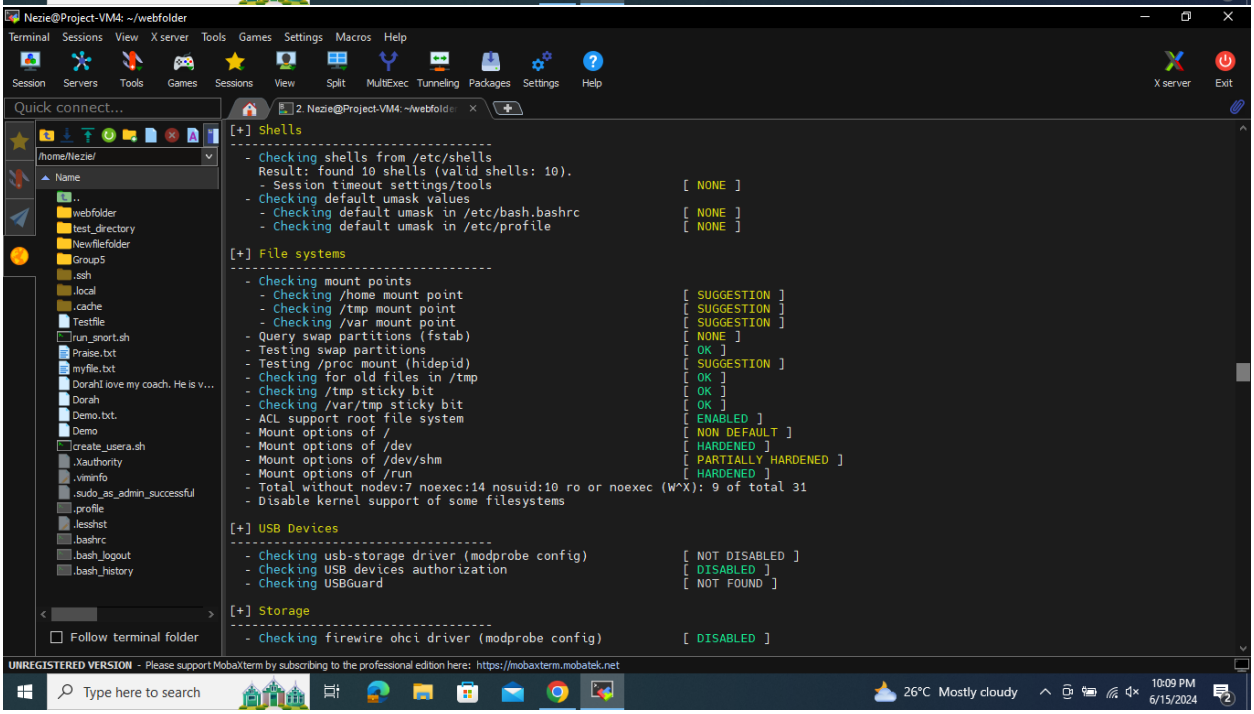


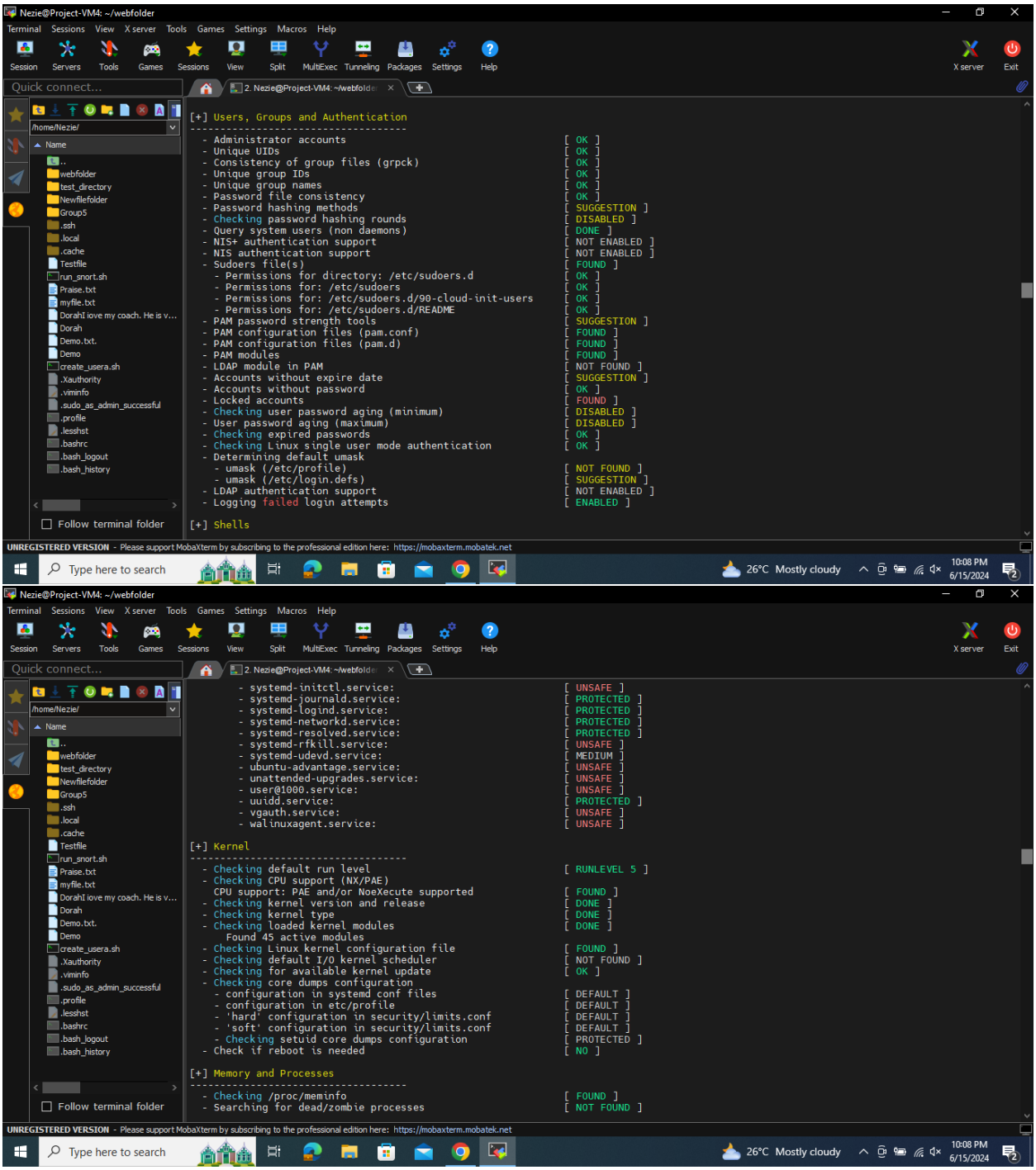
5. **Verify File Permissions:** Check permissions on sensitive files
   Command: ls -l /etc/passwd
   ls -l /etc/shadow

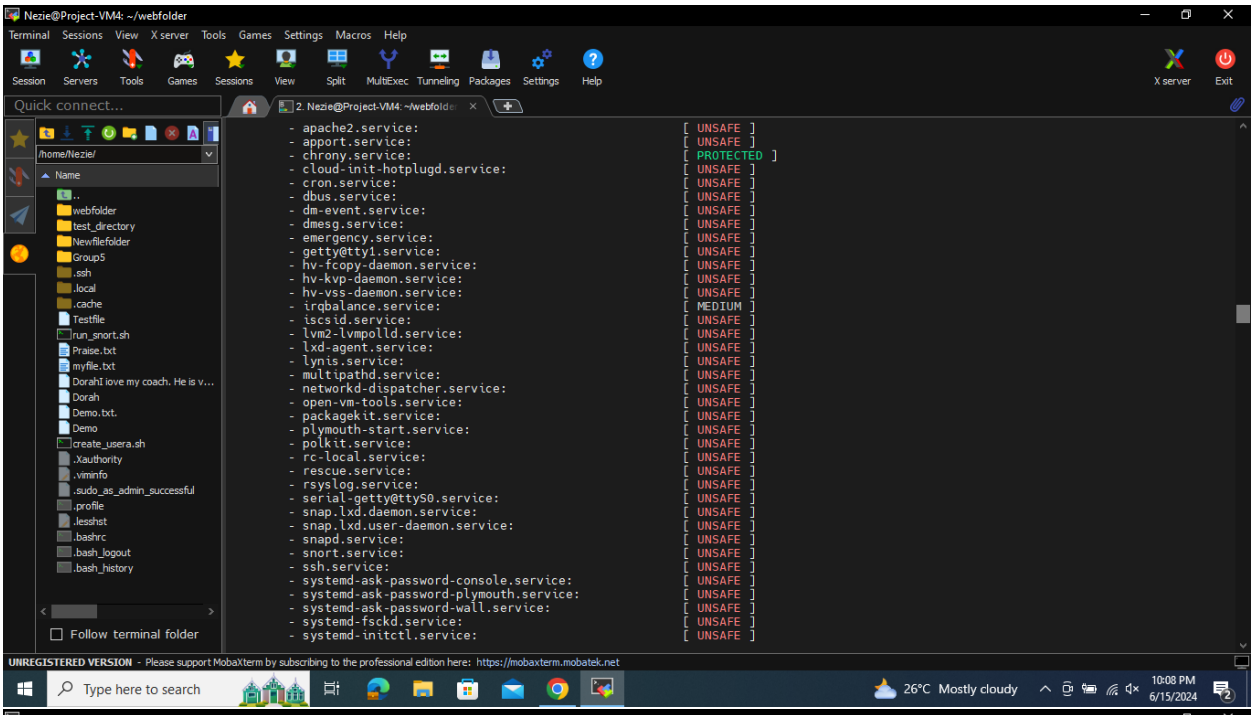


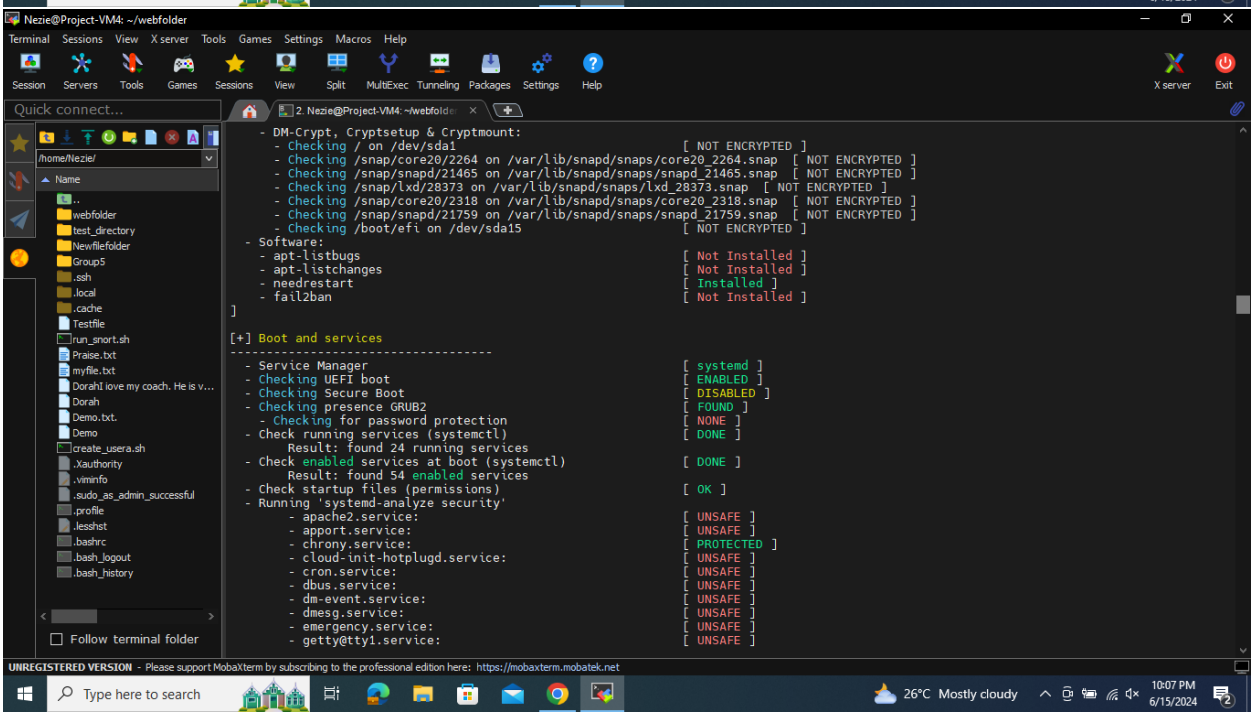
6. **Check for Vulnerabilities:** Use vulnerability scanners to identify known vulnerabilities.
   Commands: sudo apt install lynis
   sudo lynis audit system

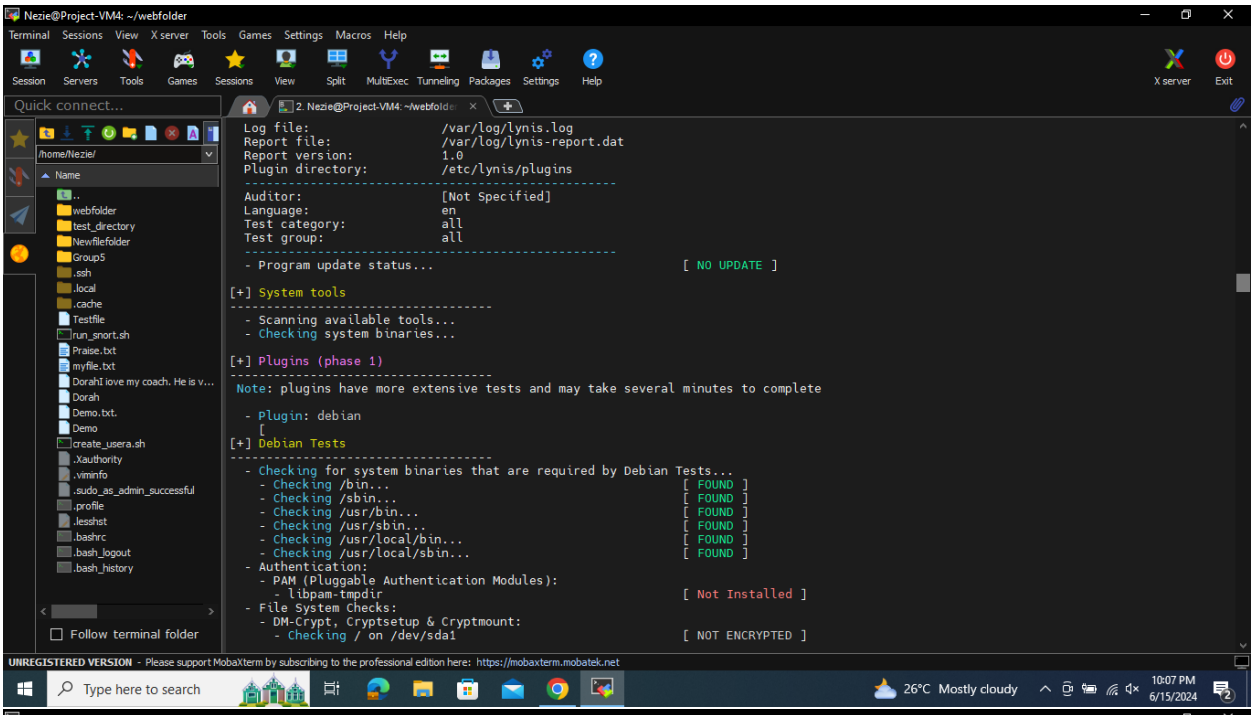

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolder
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
[+] USB Devices
- Checking usb-storage driver (modprobe config) [NOT DISABLED]
- Checking USB devices authorization [DISABLED]
- Checking USBGuard [NOT FOUND]
[+] Storage
- Checking firewire ohci driver (modprobe config) [DISABLED]
[+] NFS
- Check running NFS daemon [NOT FOUND]
[+] Name services
- Checking search domains [FOUND]
- Checking /etc/resolv.conf options [FOUND]
- Searching DNS domain name [FOUND]
Domain name: cybo32sqrf2e1a2frofif0rolb.cx.internal.cloudapp.net
- Checking /etc/hosts
- Duplicate entries in hosts file [NONE]
- Presence of configured hostname in /etc/hosts [NOT FOUND]
- Hostname mapped to localhost [NOT FOUND]
- Localhost mapping to IP address [OK]
[+] Ports and packages
- Searching package managers
- Searching dpkg package manager [FOUND]
- Querying package manager
- Query unpurged packages [NONE]
- Checking security repository in sources.list file [OK]
- Checking APT package database [OK]
- Checking vulnerable packages [OK]
- Checking upgradeable packages [SKIPPED]
- Checking package audit tool [INSTALLED]
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:09 PM
6/15/2024

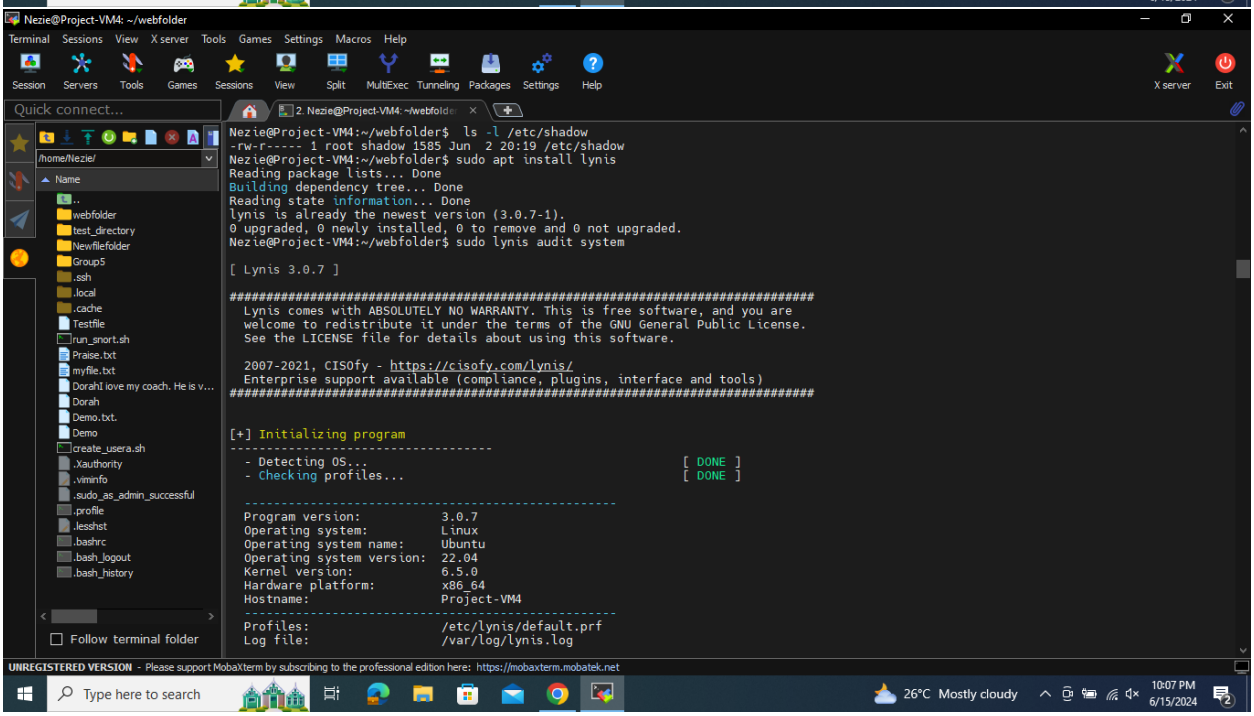

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolder
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
[+] Shells
- Checking shells from /etc/shells
Result: found 10 shells (valid shells: 10).
- Session timeout settings/tools [NONE]
- Checking default umask values
- Checking default umask in /etc/bash.bashrc [NONE]
- Checking default umask in /etc/profile [NONE]
[+] File systems
- Checking mount points
- Checking /home mount point [SUGGESTION]
- Checking /tmp mount point [SUGGESTION]
- Checking /var mount point [SUGGESTION]
- Query swap partitions (fstab) [NONE]
- Testing swap partitions [OK]
- Testing /proc mount (hidepid) [SUGGESTION]
- Checking for old files in /tmp [OK]
- Checking /tmp sticky bit [OK]
- Checking /var/tmp sticky bit [OK]
- ACL support root file system [ENABLED]
- Mount options of / [NON DEFAULT]
- Mount options of /dev [HARDENED]
- Mount options of /dev/shm [PARTIALLY HARDENED]
- Mount options of /run [HARDENED]
- Total without nodev:7 noexec:14 nosuid:10 ro or noexec (W^X): 9 of total 31
- Disable kernel support of some filesystems
[+] USB Devices
- Checking usb-storage driver (modprobe config) [NOT DISABLED]
- Checking USB devices authorization [DISABLED]
- Checking USBGuard [NOT FOUND]
[+] Storage
- Checking firewire ohci driver (modprobe config) [DISABLED]
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:09 PM
6/15/2024

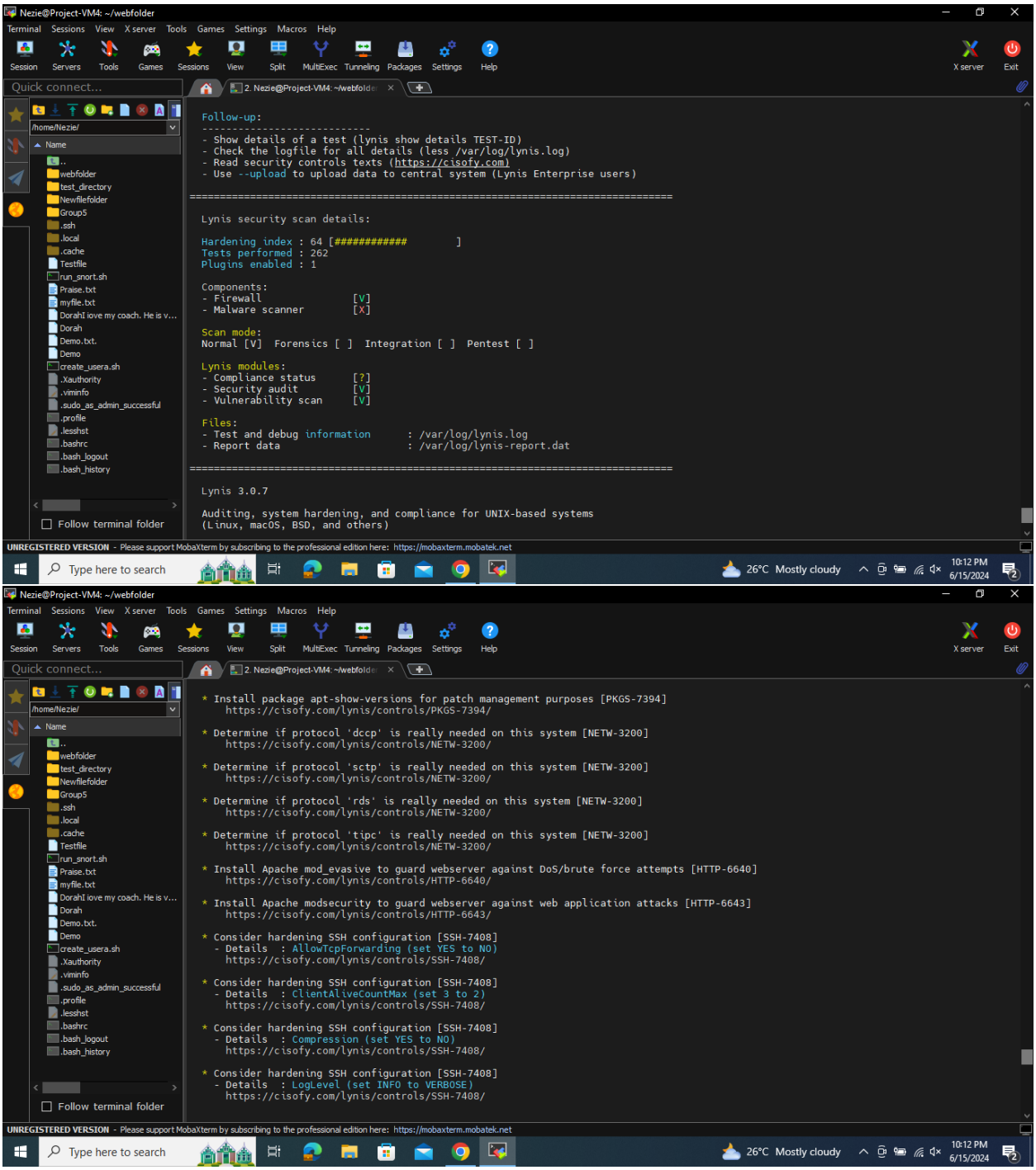

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
[+] Users, Groups and Authentication
- Administrator accounts [OK]
- Unique UIDs [OK]
- Consistency of group files (grpck) [OK]
- Unique group IDs [OK]
- Unique group names [OK]
- Password file consistency [OK]
- Password hashing methods [SUGGESTION]
- Checking password hashing rounds [DISABLED]
- Query system users (non daemons) [DONE]
- NIS+ authentication support [NOT ENABLED]
- NIS authentication support [NOT ENABLED]
- Sudoers file(s) [FOUND]
- Permissions for directory: /etc/sudoers.d [OK]
- Permissions for: /etc/sudoers [OK]
- Permissions for: /etc/sudoers.d/90-cloud-init-users [OK]
- Permissions for: /etc/sudoers.d/README [OK]
- PAM password strength tools [SUGGESTION]
- PAM configuration files (pam.conf) [FOUND]
- PAM configuration files (pam.d) [FOUND]
- PAM modules [FOUND]
- LDAP module in PAM [NOT FOUND]
- Accounts without expire date [SUGGESTION]
- Accounts without password [OK]
- Locked accounts [FOUND]
- Checking user password aging (minimum) [DISABLED]
- User password aging (maximum) [DISABLED]
- Checking expired passwords [OK]
- Checking Linux single user mode authentication [OK]
- Determining default umask
- umask (/etc/profile) [NOT FOUND]
- umask (/etc/login.defs) [SUGGESTION]
- LDAP authentication support [NOT ENABLED]
- Logging failed login attempts [ENABLED]
[+] Shells
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:08 PM
6/15/2024
Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
- systemd-initctl.service: [UNSAFE]
- systemd-journald.service: [PROTECTED]
- systemd-logind.service: [PROTECTED]
- systemd-networkd.service: [PROTECTED]
- systemd-resolved.service: [PROTECTED]
- systemd-rfkill.service: [UNSAFE]
- systemd-udevd.service: [MEDIUM]
- ubuntu-advantage.service: [UNSAFE]
- unattended-upgrades.service: [UNSAFE]
- user@1000.service: [UNSAFE]
- uuidd.service: [PROTECTED]
- vgauth.service: [UNSAFE]
- walinuxagent.service: [UNSAFE]
[+] Kernel
- Checking default run level [RUNLEVEL 5]
- Checking CPU support (NX/PAE)
CPU support: PAE and/or NoeXecute supported [FOUND]
- Checking kernel version and release [DONE]
- Checking kernel type [DONE]
- Checking loaded kernel modules [DONE]
Found 45 active modules
- Checking Linux kernel configuration file [FOUND]
- Checking default I/O kernel scheduler [NOT FOUND]
- Checking for available kernel update [OK]
- Checking core dumps configuration
- configuration in systemd conf files [DEFAULT]
- configuration in etc/profile [DEFAULT]
- 'hard' configuration in security/limits.conf [DEFAULT]
- 'soft' configuration in security/limits.conf [DEFAULT]
- Checking setuid core dumps configuration [PROTECTED]
- Check if reboot is needed [NO]
[+] Memory and Processes
- Checking /proc/meminfo [FOUND]
- Searching for dead/zombie processes [NOT FOUND]
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:08 PM
6/15/2024


Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
- apache2.service: [UNSAFE]
- apport.service: [UNSAFE]
- chrony.service: [PROTECTED]
- cloud-init-hotplugd.service: [UNSAFE]
- cron.service: [UNSAFE]
- dbus.service: [UNSAFE]
- dm-event.service: [UNSAFE]
- dmesg.service: [UNSAFE]
- emergency.service: [UNSAFE]
- getty@tty1.service: [UNSAFE]
- hv-fcopy-daemon.service: [UNSAFE]
- hv-kvp-daemon.service: [UNSAFE]
- hv-vss-daemon.service: [UNSAFE]
- irqbalance.service: [MEDIUM]
- iscsid.service: [UNSAFE]
- lvm2-lvmpolld.service: [UNSAFE]
- lxd-agent.service: [UNSAFE]
- lynis.service: [UNSAFE]
- multipathd.service: [UNSAFE]
- networkd-dispatcher.service: [UNSAFE]
- open-vm-tools.service: [UNSAFE]
- packagekit.service: [UNSAFE]
- plymouth-start.service: [UNSAFE]
- polkit.service: [UNSAFE]
- rc-local.service: [UNSAFE]
- rescue.service: [UNSAFE]
- rsyslog.service: [UNSAFE]
- serial-getty@ttyS0.service: [UNSAFE]
- snap.lxd.daemon.service: [UNSAFE]
- snap.lxd.user-daemon.service: [UNSAFE]
- snapd.service: [UNSAFE]
- snort.service: [UNSAFE]
- ssh.service: [UNSAFE]
- systemd-ask-password-console.service: [UNSAFE]
- systemd-ask-password-plymouth.service: [UNSAFE]
- systemd-ask-password-wall.service: [UNSAFE]
- systemd-fsckd.service: [UNSAFE]
- systemd-initctl.service: [UNSAFE]
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:08 PM
6/15/2024

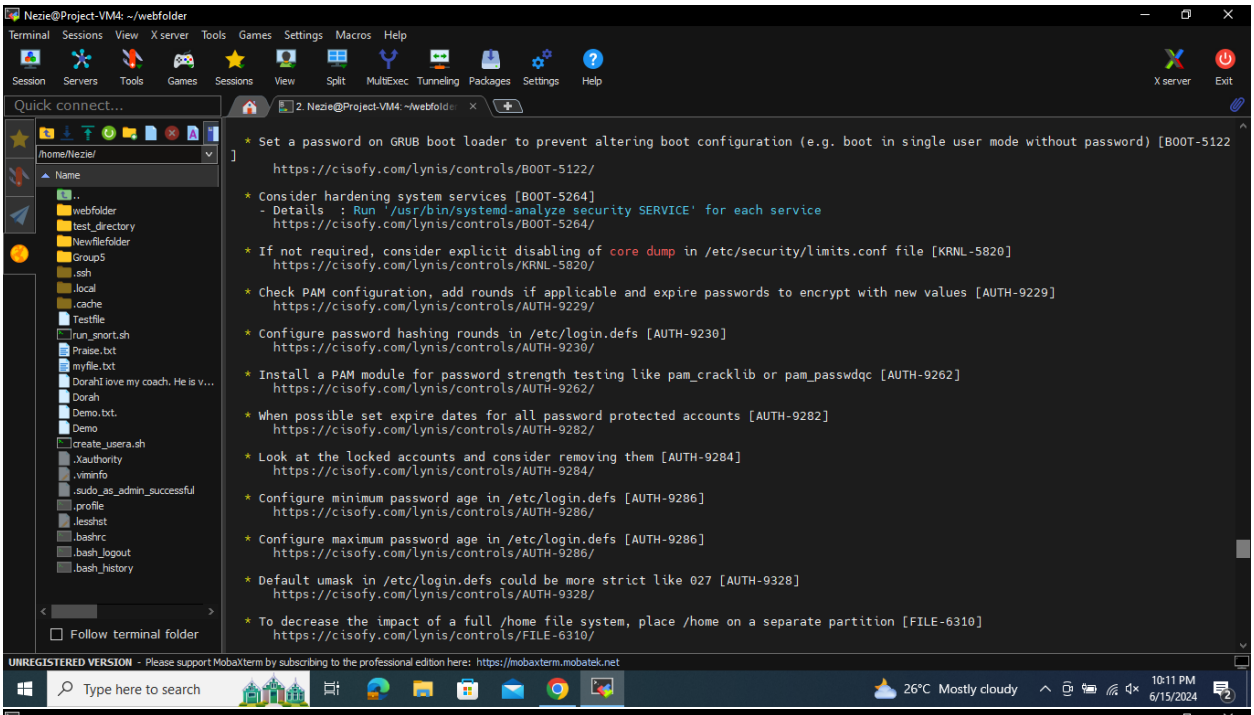

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
- DM-Crypt, Cryptsetup & Cryptmount:
- Checking / on /dev/sda1 [NOT ENCRYPTED]
- Checking /snap/core20/2264 on /var/lib/snapd/snaps/core20_2264.snap [NOT ENCRYPTED]
- Checking /snap/snapd/21465 on /var/lib/snapd/snaps/snapd_21465.snap [NOT ENCRYPTED]
- Checking /snap/lxd/28373 on /var/lib/snapd/snaps/lxd_28373.snap [NOT ENCRYPTED]
- Checking /snap/core20/2318 on /var/lib/snapd/snaps/core20_2318.snap [NOT ENCRYPTED]
- Checking /snap/snapd/21759 on /var/lib/snapd/snaps/snapd_21759.snap [NOT ENCRYPTED]
- Checking /boot/efi on /dev/sda15 [NOT ENCRYPTED]
- Software:
- apt-listbugs [Not Installed]
- apt-listchanges [Not Installed]
- needrestart [Installed]
- fail2ban [Not Installed]
]
[+] Boot and services
- Service Manager [systemd]
- Checking UEFI boot [ENABLED]
- Checking Secure Boot [DISABLED]
- Checking presence GRUB2 [FOUND]
- Checking for password protection [NONE]
- Check running services (systemctl) [DONE]
Result: found 24 running services
- Check enabled services at boot (systemctl) [DONE]
Result: found 54 enabled services
- Check startup files (permissions) [OK]
- Running 'systemd-analyze security'
- apache2.service: [UNSAFE]
- apport.service: [UNSAFE]
- chrony.service: [PROTECTED]
- cloud-init-hotplugd.service: [UNSAFE]
- cron.service: [UNSAFE]
- dbus.service: [UNSAFE]
- dm-event.service: [UNSAFE]
- dmesg.service: [UNSAFE]
- emergency.service: [UNSAFE]
- getty@tty1.service: [UNSAFE]
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:07 PM
6/15/2024

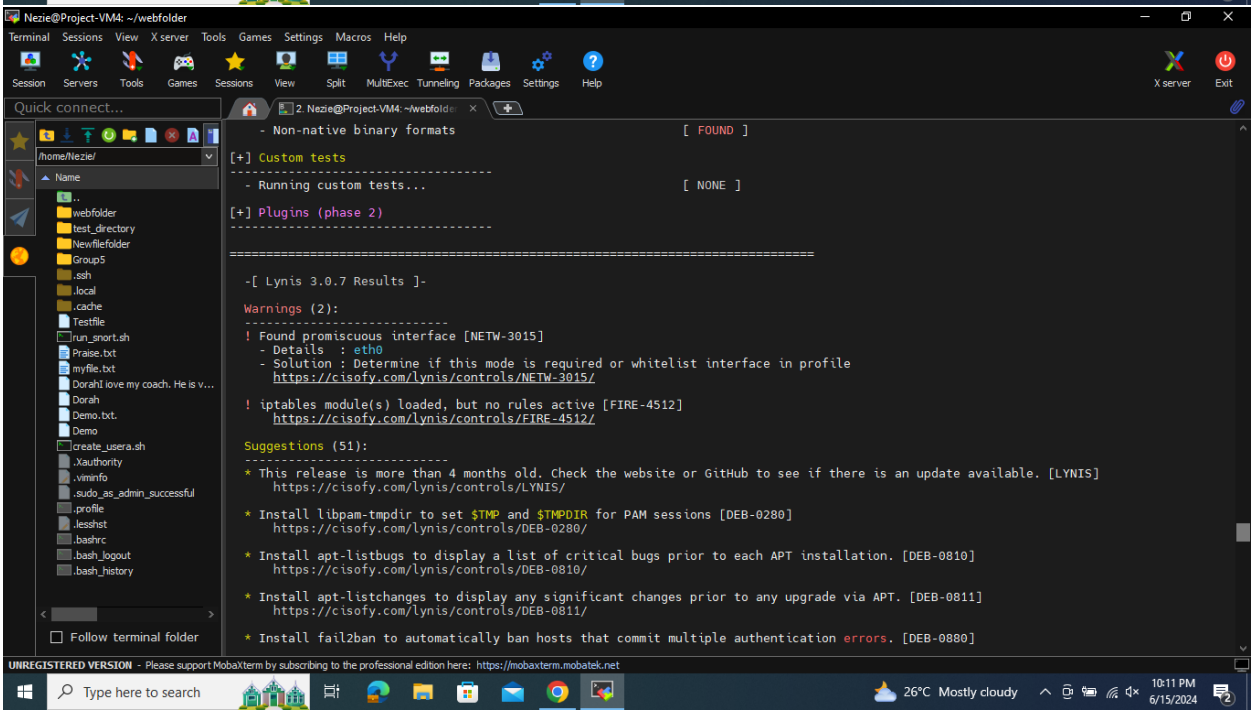

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
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]
- Checking /usr/bin... [FOUND]
- Checking /usr/sbin... [FOUND]
- Checking /usr/local/bin... [FOUND]
- Checking /usr/local/sbin... [FOUND]
- Authentication:
- PAM (Pluggable Authentication Modules):
- libpam-tmpdir [Not Installed]
- File System Checks:
- DM-Crypt, Cryptsetup & Cryptmount:
- Checking / on /dev/sda1 [NOT ENCRYPTED]
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:07 PM
6/15/2024

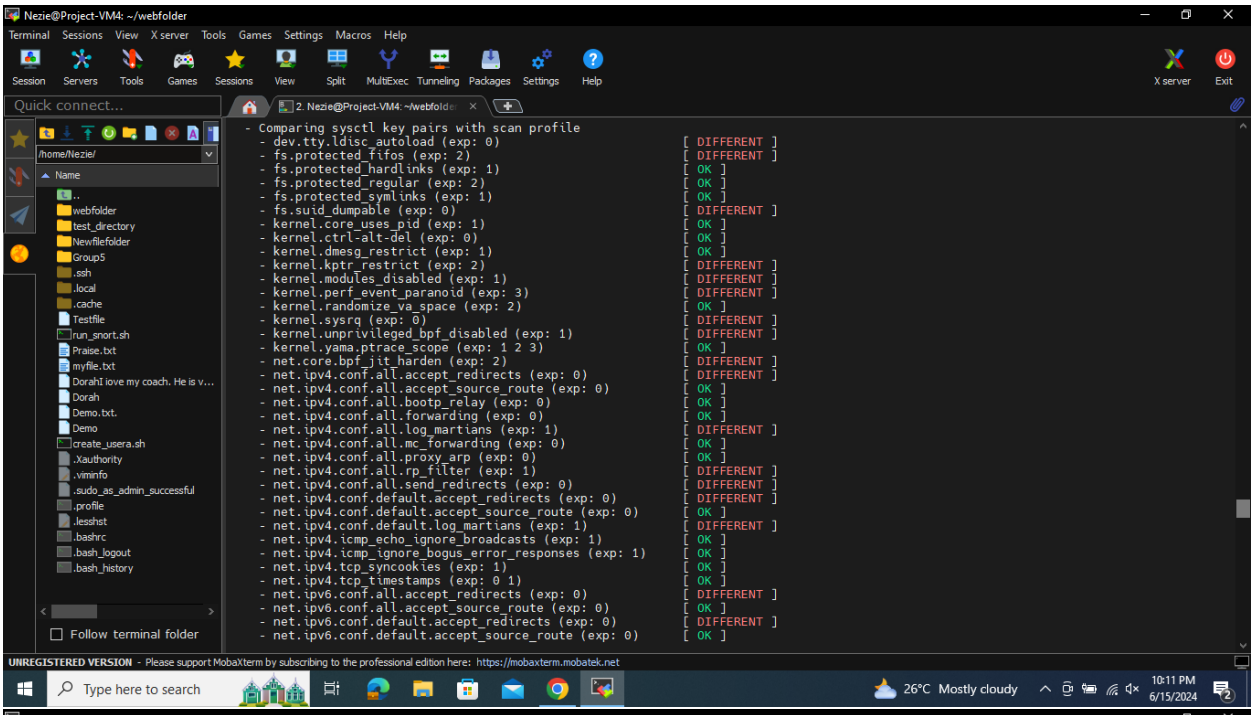

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Nezie@Project-VM4:~/webfolder$ ls -l /etc/shadow
-rw-r----- 1 root shadow 1585 Jun 2 20:19 /etc/shadow
Nezie@Project-VM4:~/webfolder$ sudo apt install lynis
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
lynis is already the newest version (3.0.7-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Nezie@Project-VM4:~/webfolder$ sudo lynis audit system
[Lynis 3.0.7]
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.
2007-2021, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
[+] Initializing program
- Detecting OS... [DONE]
- Checking profiles... [DONE]
Program version: 3.0.7
Operating system: Linux
Operating system name: Ubuntu
Operating system version: 22.04
Kernel version: 6.5.0
Hardware platform: x86_64
Hostname: Project-VM4
Profiles: /etc/lynis/default.prf
Log file: /var/log/lynis.log
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:07 PM
6/15/2024

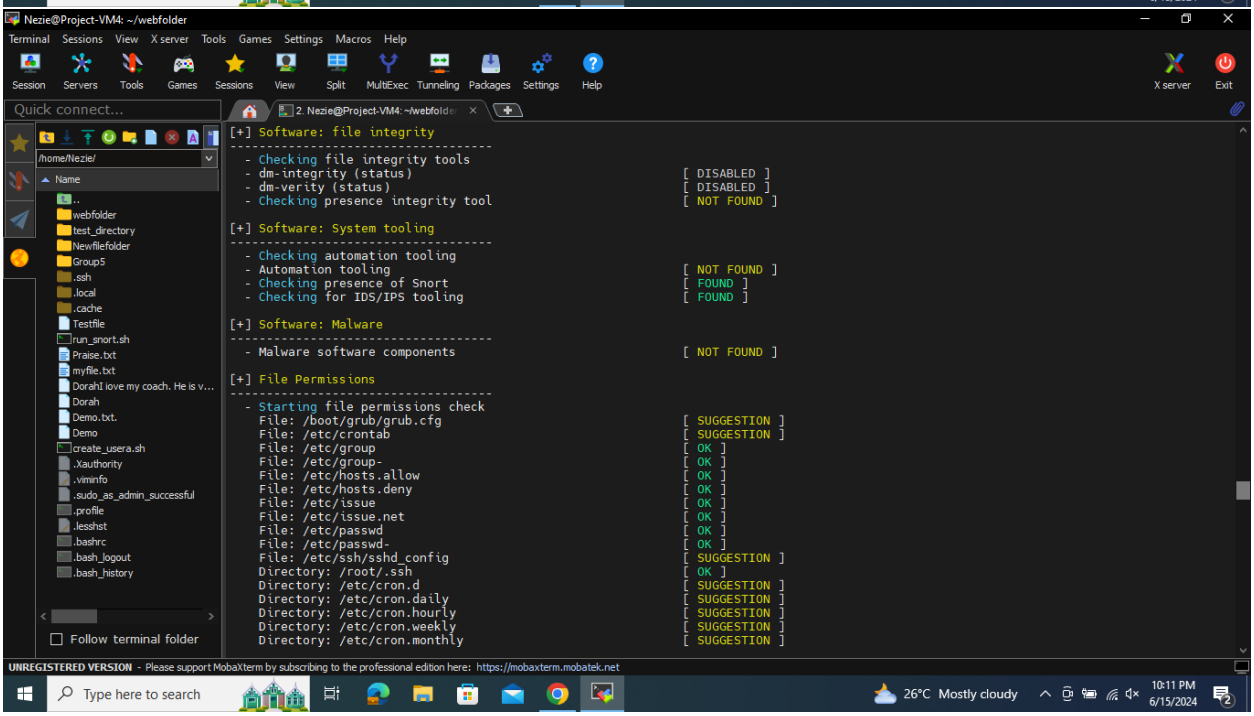

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolder
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Follow-up:
- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls texts (https://cisofy.com)
- Use --upload to upload data to central system (Lynis Enterprise users)
Lynis security scan details:
Hardening index : 64 [############]
Tests performed : 262
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 3.0.7
Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:12 PM
6/15/2024

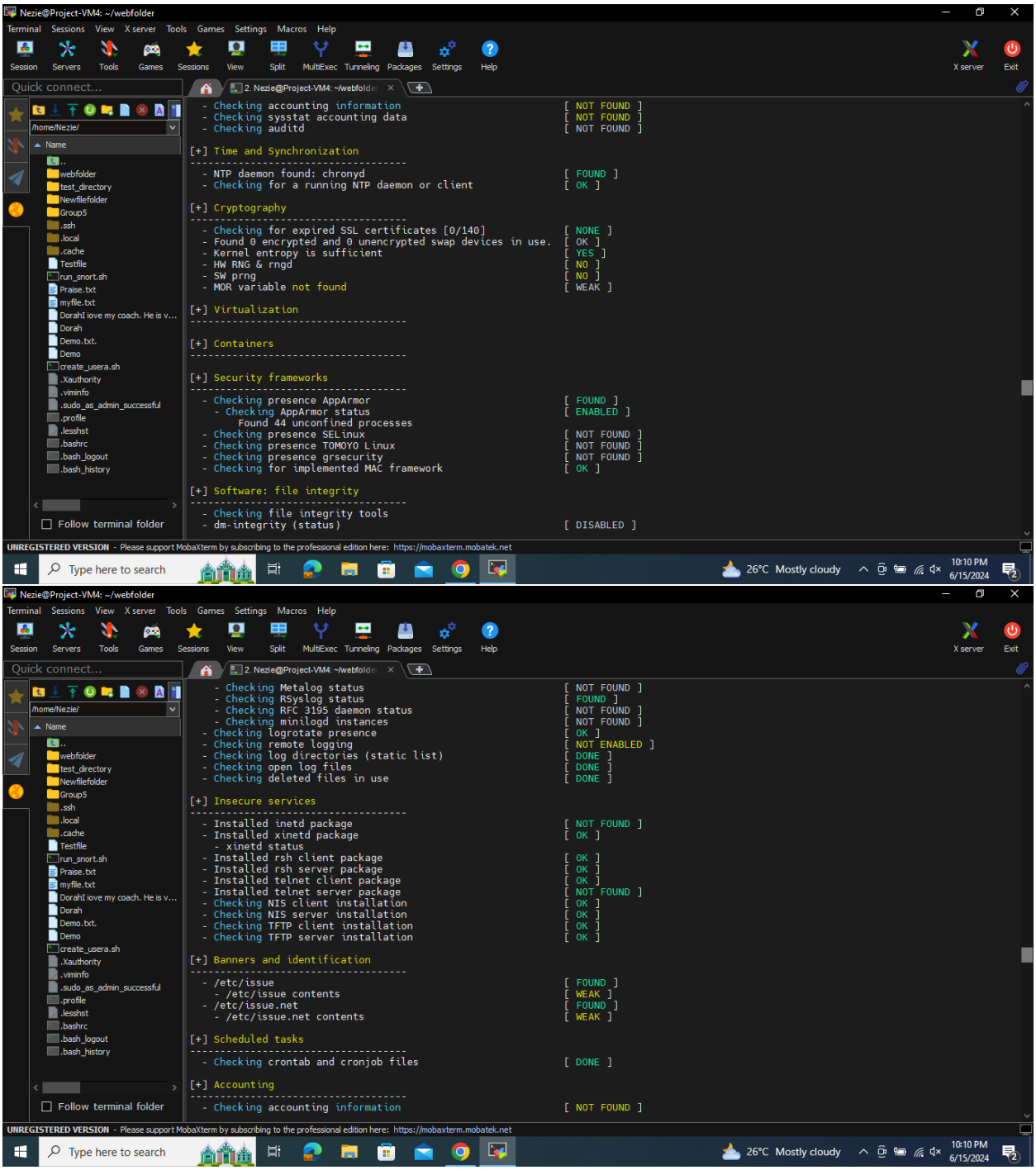
Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolder
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
* Install package apt-show-versions for patch management purposes [PKGS-7394]
https://cisofy.com/lynis/controls/PKGS-7394/
* Determine if protocol 'dccp' is really needed on this system [NETW-3200]
https://cisofy.com/lynis/controls/NETW-3200/
* Determine if protocol 'sctp' is really needed on this system [NETW-3200]
https://cisofy.com/lynis/controls/NETW-3200/
* Determine if protocol 'rds' is really needed on this system [NETW-3200]
https://cisofy.com/lynis/controls/NETW-3200/
* Determine if protocol 'tipc' is really needed on this system [NETW-3200]
https://cisofy.com/lynis/controls/NETW-3200/
* Install Apache mod_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]
https://cisofy.com/lynis/controls/HTTP-6640/
* Install Apache modsecurity to guard webserver against web application attacks [HTTP-6643]
https://cisofy.com/lynis/controls/HTTP-6643/
* Consider hardening SSH configuration [SSH-7408]
- Details : AllowTcpForwarding (set YES to NO)
https://cisofy.com/lynis/controls/SSH-7408/
* Consider hardening SSH configuration [SSH-7408]
- Details : ClientAliveCountMax (set 3 to 2)
https://cisofy.com/lynis/controls/SSH-7408/
* Consider hardening SSH configuration [SSH-7408]
- Details : Compression (set YES to NO)
https://cisofy.com/lynis/controls/SSH-7408/
* Consider hardening SSH configuration [SSH-7408]
- Details : LogLevel (set INFO to VERBOSE)
https://cisofy.com/lynis/controls/SSH-7408/
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:12 PM
6/15/2024

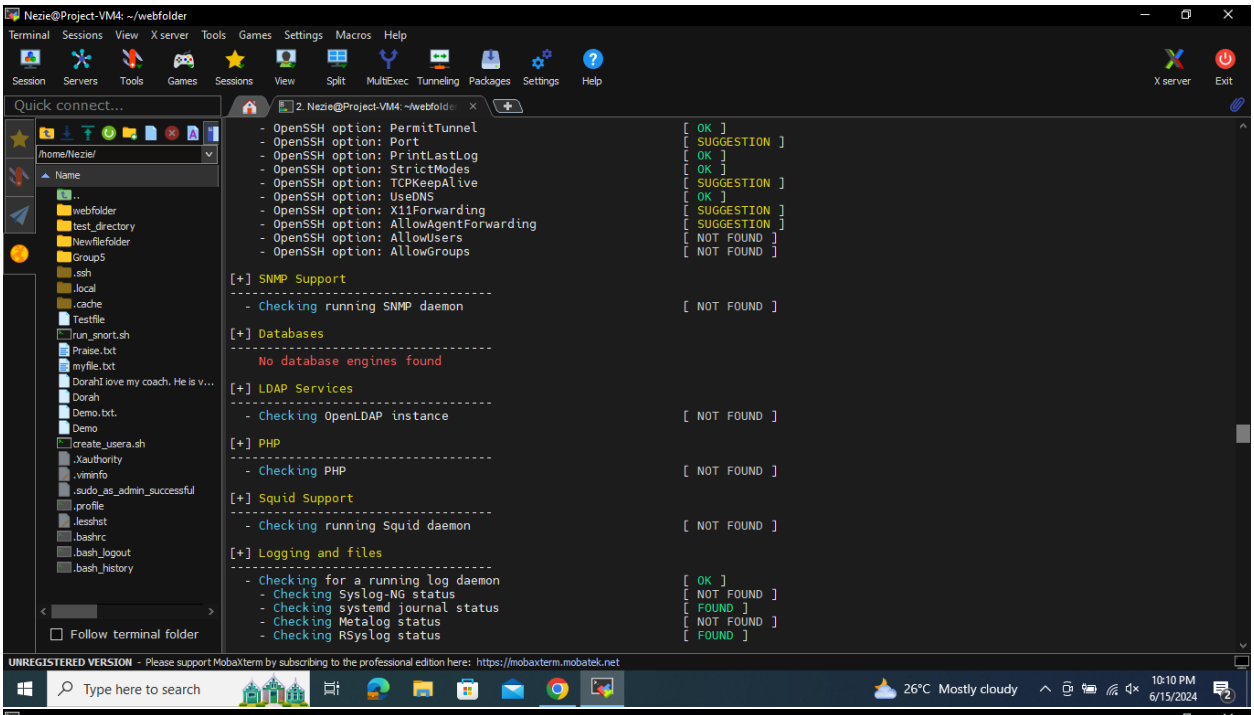

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
https://cisofy.com/lynis/controls/BOOT-5122/
* Consider hardening system services [BOOT-5264]
- Details : Run '/usr/bin/systemd-analyze security SERVICE' for each service
https://cisofy.com/lynis/controls/BOOT-5264/
* If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
https://cisofy.com/lynis/controls/KRNL-5820/
* Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new values [AUTH-9229]
https://cisofy.com/lynis/controls/AUTH-9229/
* Configure password hashing rounds in /etc/login.defs [AUTH-9230]
https://cisofy.com/lynis/controls/AUTH-9230/
* Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
https://cisofy.com/lynis/controls/AUTH-9262/
* When possible set expire dates for all password protected accounts [AUTH-9282]
https://cisofy.com/lynis/controls/AUTH-9282/
* Look at the locked accounts and consider removing them [AUTH-9284]
https://cisofy.com/lynis/controls/AUTH-9284/
* Configure minimum password age in /etc/login.defs [AUTH-9286]
https://cisofy.com/lynis/controls/AUTH-9286/
* Configure maximum password age in /etc/login.defs [AUTH-9286]
https://cisofy.com/lynis/controls/AUTH-9286/
* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
https://cisofy.com/lynis/controls/AUTH-9328/
* To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]
https://cisofy.com/lynis/controls/FILE-6310/
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:11 PM
6/15/2024

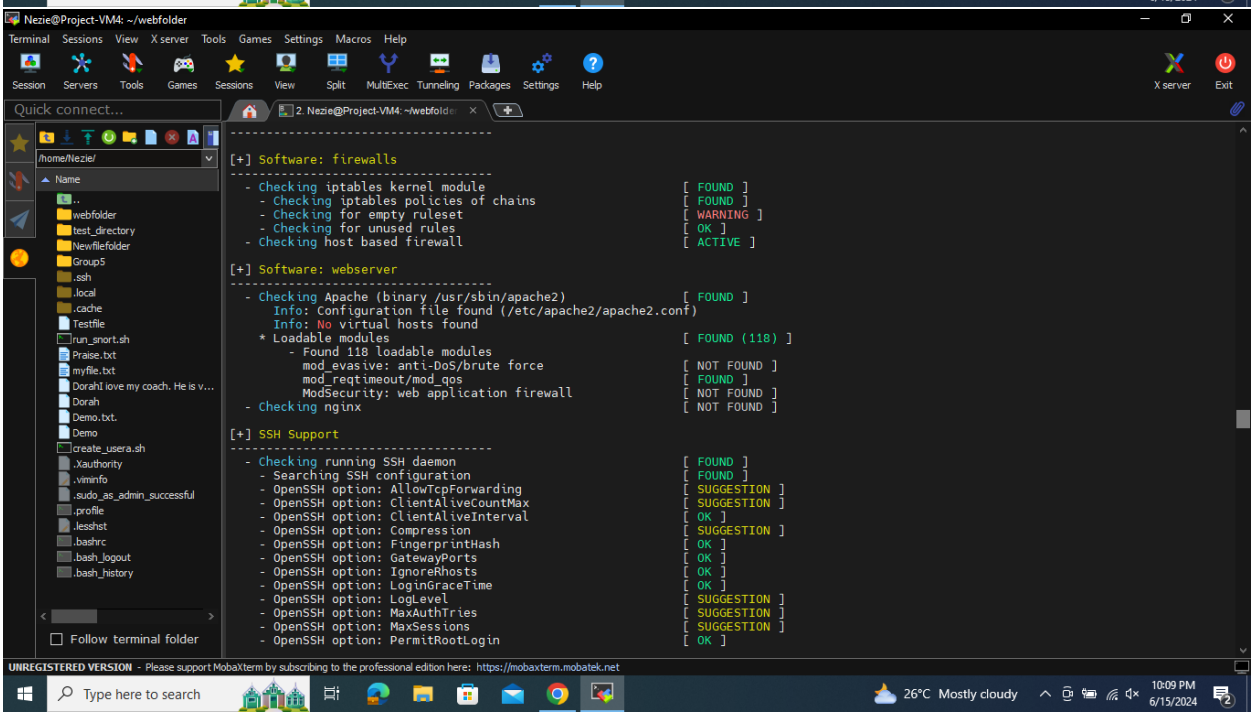

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
- Non-native binary formats [FOUND]
[+] Custom tests
- Running custom tests... [NONE]
[+] Plugins (phase 2)
-[Lynis 3.0.7 Results]-
Warnings (2):
! Found promiscuous interface [NETW-3015]
- Details : eth0
- Solution : Determine if this mode is required or whitelist interface in profile
https://cisofy.com/lynis/controls/NETW-3015/
! iptables module(s) loaded, but no rules active [FIRE-4512]
https://cisofy.com/lynis/controls/FIRE-4512/
Suggestions (51):
* This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]
https://cisofy.com/lynis/controls/LYNIS/
* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]
https://cisofy.com/lynis/controls/DEB-0280/
* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]
https://cisofy.com/lynis/controls/DEB-0810/
* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [DEB-0811]
https://cisofy.com/lynis/controls/DEB-0811/
* Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:11 PM
6/15/2024

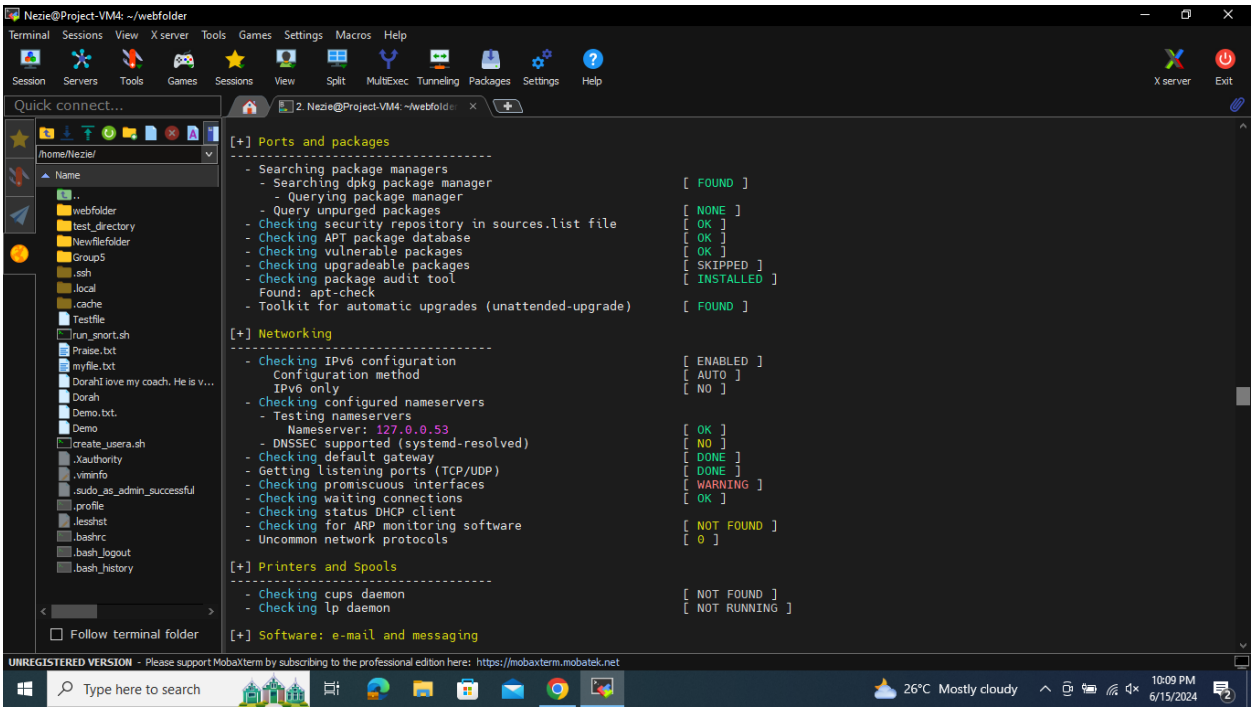

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
- Comparing sysctl key pairs with scan profile
- dev.tty.ldisc_autoload (exp: 0) [DIFFERENT]
- fs.protected_fifos (exp: 2) [DIFFERENT]
- fs.protected_hardlinks (exp: 1) [OK]
- fs.protected_regular (exp: 2) [OK]
- fs.protected_symlinks (exp: 1) [OK]
- fs.suid_dumpable (exp: 0) [DIFFERENT]
- kernel.core_uses_pid (exp: 1) [OK]
- kernel.ctrl-alt-del (exp: 0) [OK]
- kernel.dmesg_restrict (exp: 1) [OK]
- kernel.kptr_restrict (exp: 2) [DIFFERENT]
- kernel.modules_disabled (exp: 1) [DIFFERENT]
- kernel.perf_event_paranoid (exp: 3) [DIFFERENT]
- kernel.randomize_va_space (exp: 2) [OK]
- kernel.sysrq (exp: 0) [DIFFERENT]
- kernel.unprivileged_bpf_disabled (exp: 1) [DIFFERENT]
- kernel.yama.ptrace_scope (exp: 1 2 3) [OK]
- net.core.bpf_jit_harden (exp: 2) [DIFFERENT]
- net.ipv4.conf.all.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv4.conf.all.accept_source_route (exp: 0) [OK]
- net.ipv4.conf.all.bootp_relay (exp: 0) [OK]
- net.ipv4.conf.all.forwarding (exp: 0) [OK]
- net.ipv4.conf.all.log_martians (exp: 1) [DIFFERENT]
- net.ipv4.conf.all.mc_forwarding (exp: 0) [OK]
- net.ipv4.conf.all.proxy_arp (exp: 0) [OK]
- net.ipv4.conf.all.rp_filter (exp: 1) [DIFFERENT]
- net.ipv4.conf.all.send_redirects (exp: 0) [DIFFERENT]
- net.ipv4.conf.default.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv4.conf.default.accept_source_route (exp: 0) [OK]
- net.ipv4.conf.default.log_martians (exp: 1) [DIFFERENT]
- net.ipv4.icmp_echo_ignore_broadcasts (exp: 1) [OK]
- net.ipv4.icmp_ignore_bogus_error_responses (exp: 1) [OK]
- net.ipv4.tcp_syncookies (exp: 1) [OK]
- net.ipv4.tcp_timestamps (exp: 0 1) [OK]
- net.ipv6.conf.all.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv6.conf.all.accept_source_route (exp: 0) [OK]
- net.ipv6.conf.default.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv6.conf.default.accept_source_route (exp: 0) [OK]
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:11 PM
6/15/2024


Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
[+] Software: file integrity
- Checking file integrity tools
- dm-integrity (status) [DISABLED]
- dm-verity (status) [DISABLED]
- Checking presence integrity tool [NOT FOUND]
[+] Software: System tooling
- Checking automation tooling
- Automation tooling [NOT FOUND]
- Checking presence of Snort [FOUND]
- Checking for IDS/IPS tooling [FOUND]
[+] Software: Malware
- Malware software components [NOT FOUND]
[+] File Permissions
- Starting file permissions check
File: /boot/grub/grub.cfg [SUGGESTION]
File: /etc/crontab [SUGGESTION]
File: /etc/group [OK]
File: /etc/group- [OK]
File: /etc/hosts.allow [OK]
File: /etc/hosts.deny [OK]
File: /etc/issue [OK]
File: /etc/issue.net [OK]
File: /etc/passwd [OK]
File: /etc/passwd- [OK]
File: /etc/ssh/sshd_config [SUGGESTION]
Directory: /root/.ssh [OK]
Directory: /etc/cron.d [SUGGESTION]
Directory: /etc/cron.daily [SUGGESTION]
Directory: /etc/cron.hourly [SUGGESTION]
Directory: /etc/cron.weekly [SUGGESTION]
Directory: /etc/cron.monthly [SUGGESTION]
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:11 PM
6/15/2024


Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
- Checking accounting information [NOT FOUND]
- Checking sysstat accounting data [NOT FOUND]
- Checking auditd [NOT FOUND]
[+] Time and Synchronization
- NTP daemon found: chronyd [FOUND]
- Checking for a running NTP daemon or client [OK]
[+] Cryptography
- Checking for expired SSL certificates [0/140] [NONE]
- Found 0 encrypted and 0 unencrypted swap devices in use. [OK]
- Kernel entropy is sufficient [YES]
- HW RNG & rngd [NO]
- SW prng [NO]
- MOR variable not found [WEAK]
[+] Virtualization
[+] Containers
[+] Security frameworks
- Checking presence AppArmor [FOUND]
- Checking AppArmor status [ENABLED]
Found 44 unconfined processes
- Checking presence SELinux [NOT FOUND]
- Checking presence TOMOYO Linux [NOT FOUND]
- Checking presence grsecurity [NOT FOUND]
- Checking for implemented MAC framework [OK]
[+] Software: file integrity
- Checking file integrity tools
- dm-integrity (status) [DISABLED]
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:10 PM
6/15/2024
Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
- Checking Metalog status [NOT FOUND]
- Checking RSyslog status [FOUND]
- Checking RFC 3195 daemon status [NOT FOUND]
- Checking minilogd instances [NOT FOUND]
- Checking logrotate presence [OK]
- Checking remote logging [NOT ENABLED]
- Checking log directories (static list) [DONE]
- Checking open log files [DONE]
- Checking deleted files in use [DONE]
[+] Insecure services
- Installed inetd package [NOT FOUND]
- Installed xinetd package [OK]
- xinetd status
- Installed rsh client package [OK]
- Installed rsh server package [OK]
- Installed telnet client package [OK]
- Installed telnet server package [NOT FOUND]
- Checking NIS client installation [OK]
- Checking NIS server installation [OK]
- Checking TFTP client installation [OK]
- Checking TFTP server installation [OK]
[+] Banners and identification
- /etc/issue [FOUND]
- /etc/issue contents [WEAK]
- /etc/issue.net [FOUND]
- /etc/issue.net contents [WEAK]
[+] Scheduled tasks
- Checking crontab and cronjob files [DONE]
[+] Accounting
- Checking accounting information [NOT FOUND]
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:10 PM
6/15/2024


Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
- OpenSSH option: PermitTunnel [OK]
- OpenSSH option: Port [SUGGESTION]
- OpenSSH option: PrintLastLog [OK]
- OpenSSH option: StrictModes [OK]
- OpenSSH option: TCPKeepAlive [SUGGESTION]
- OpenSSH option: UseDNS [OK]
- OpenSSH option: X11Forwarding [SUGGESTION]
- OpenSSH option: AllowAgentForwarding [SUGGESTION]
- OpenSSH option: AllowUsers [NOT FOUND]
- OpenSSH option: AllowGroups [NOT FOUND]
[+] SNMP Support
- Checking running SNMP daemon [NOT FOUND]
[+] Databases
No database engines found
[+] LDAP Services
- Checking OpenLDAP instance [NOT FOUND]
[+] PHP
- Checking PHP [NOT FOUND]
[+] Squid Support
- Checking running Squid daemon [NOT FOUND]
[+] Logging and files
- Checking for a running log daemon [OK]
- Checking Syslog-NG status [NOT FOUND]
- Checking systemd journal status [FOUND]
- Checking Metalog status [NOT FOUND]
- Checking RSyslog status [FOUND]
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:10 PM
6/15/2024


Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
[+] Software: firewalls
- Checking iptables kernel module [FOUND]
- Checking iptables policies of chains [FOUND]
- Checking for empty ruleset [WARNING]
- Checking for unused rules [OK]
- Checking host based firewall [ACTIVE]
[+] Software: webserver
- Checking Apache (binary /usr/sbin/apache2) [FOUND]
Info: Configuration file found (/etc/apache2/apache2.conf)
Info: No virtual hosts found
* Loadable modules [FOUND (118)]
- Found 118 loadable modules
mod_evasive: anti-DoS/brute force [NOT FOUND]
mod_reqtimeout/mod_qos [FOUND]
ModSecurity: web application firewall [NOT FOUND]
- Checking nginx [NOT FOUND]
[+] SSH Support
- Checking running SSH daemon [FOUND]
- Searching SSH configuration [FOUND]
- OpenSSH option: AllowTcpForwarding [SUGGESTION]
- OpenSSH option: ClientAliveCountMax [SUGGESTION]
- OpenSSH option: ClientAliveInterval [OK]
- OpenSSH option: Compression [SUGGESTION]
- OpenSSH option: FingerprintHash [OK]
- OpenSSH option: GatewayPorts [OK]
- OpenSSH option: IgnoreRhosts [OK]
- OpenSSH option: LoginGraceTime [OK]
- OpenSSH option: LogLevel [SUGGESTION]
- OpenSSH option: MaxAuthTries [SUGGESTION]
- OpenSSH option: MaxSessions [SUGGESTION]
- OpenSSH option: PermitRootLogin [OK]
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:09 PM
6/15/2024



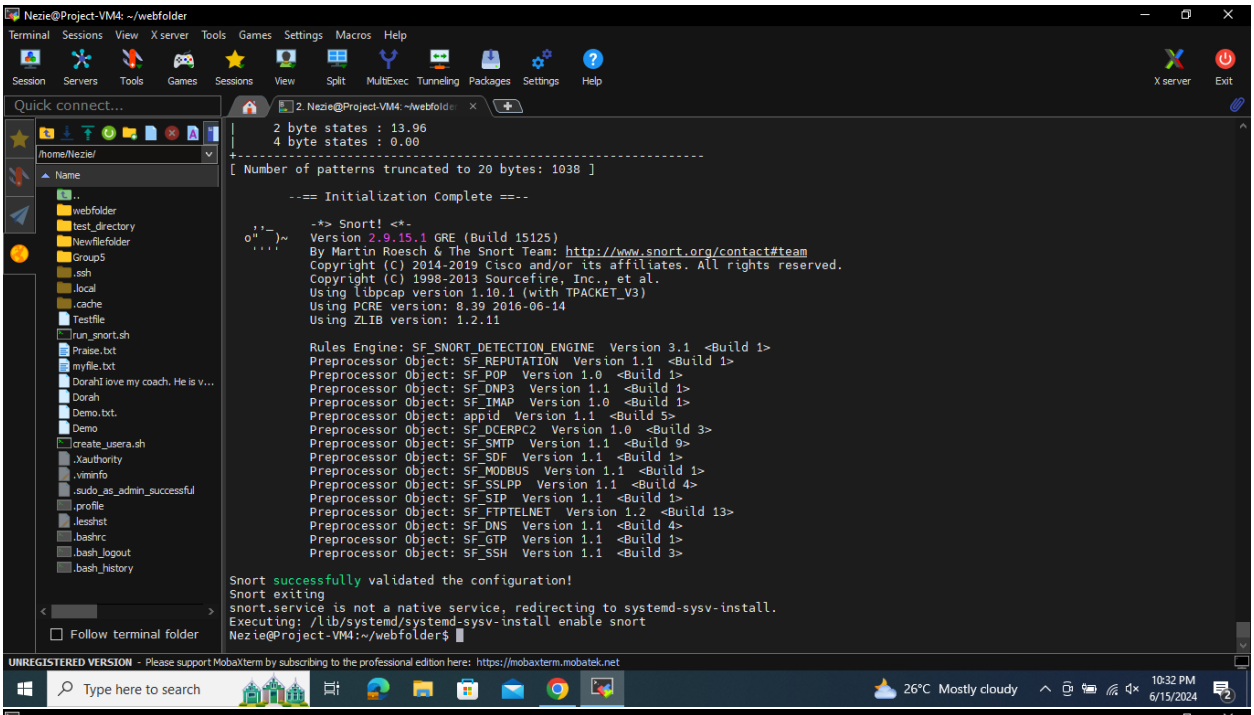
Step 2: Enable Intrusion Detection and Prevention

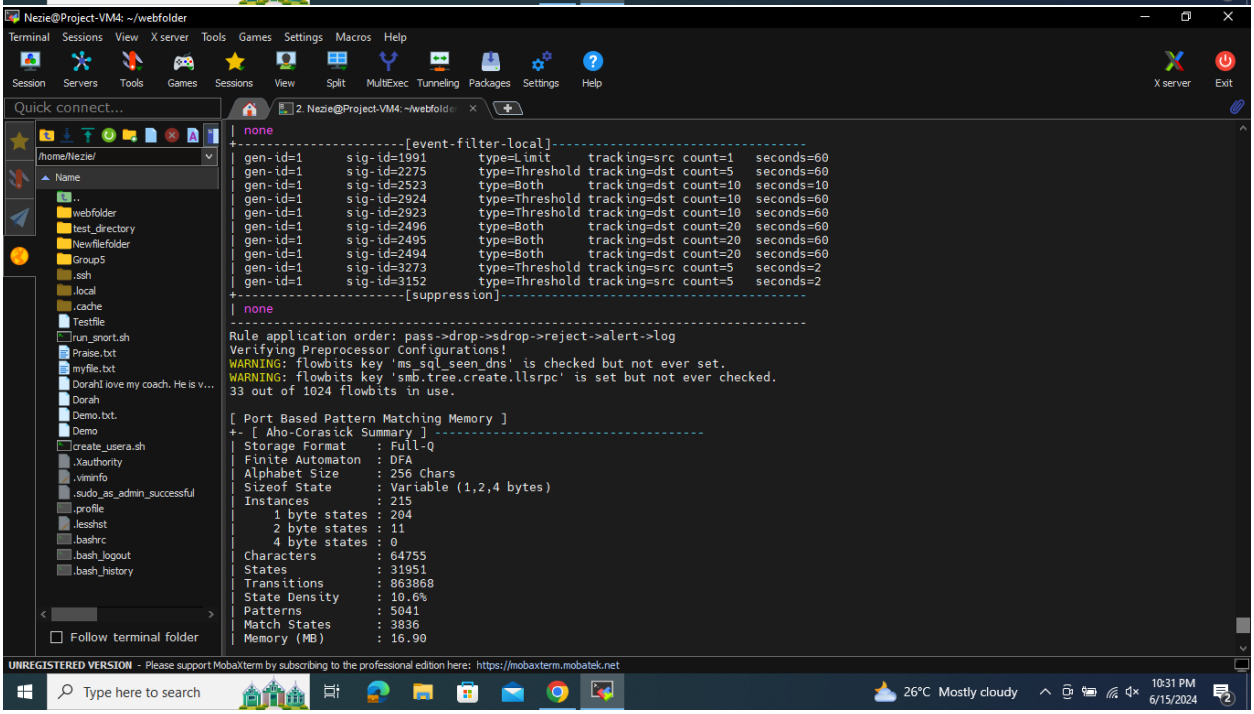
1. **Install and Configure an IDS/IPS:**

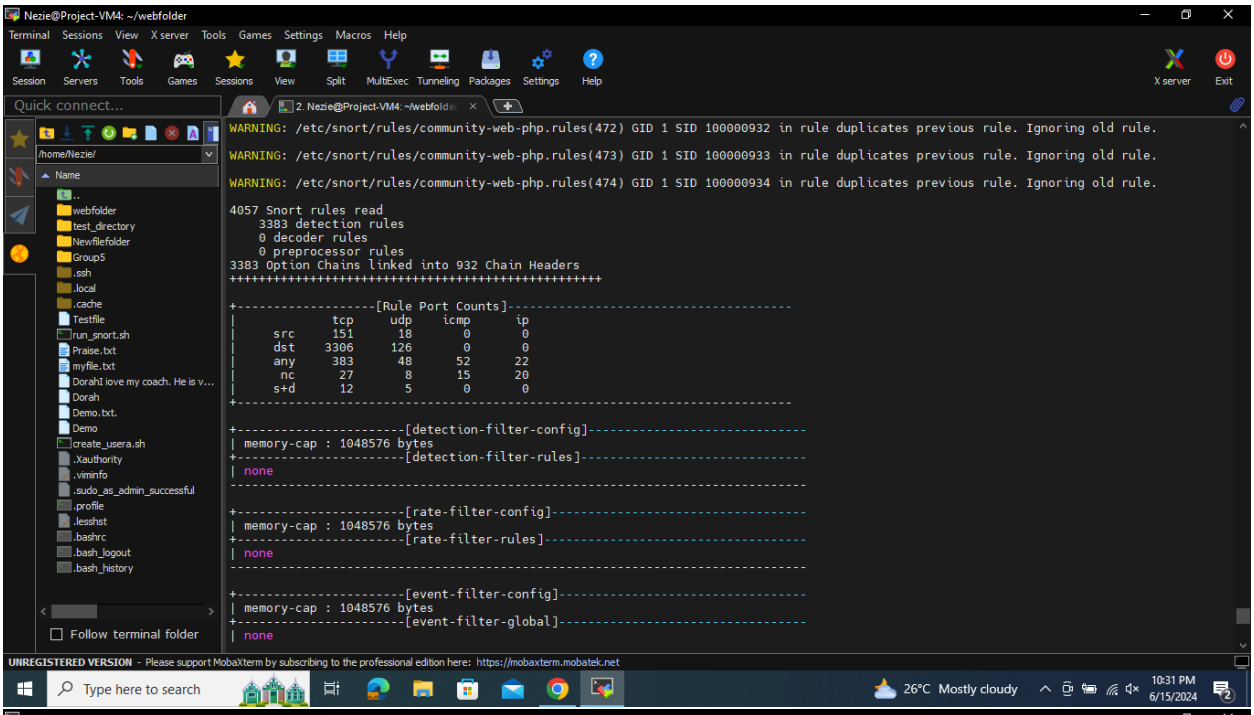
Snort: Snort is an open-source IDS/IPS.

Commands:

sudo apt install snort
sudo snort -T -c /etc/snort/snort.conf
sudo systemctl start snort
sudo systemctl enable snort

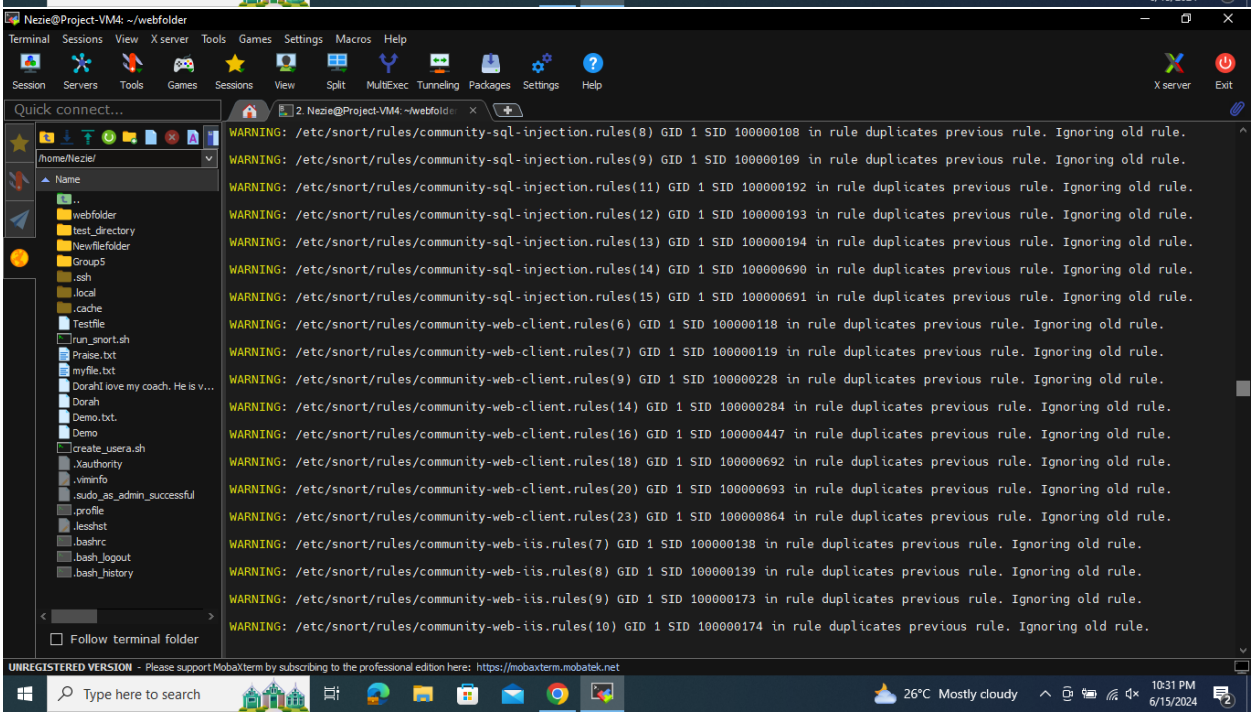

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolder
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
Dorah I love my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
2 byte states : 13.96
4 byte states : 0.00
[Number of patterns truncated to 20 bytes: 1038]
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Snort successfully validated the configuration!
Snort exiting
snort.service is not a native service, redirecting to systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable snort
Nezie@Project-VM4:~/webfolder$
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:32 PM
6/15/2024

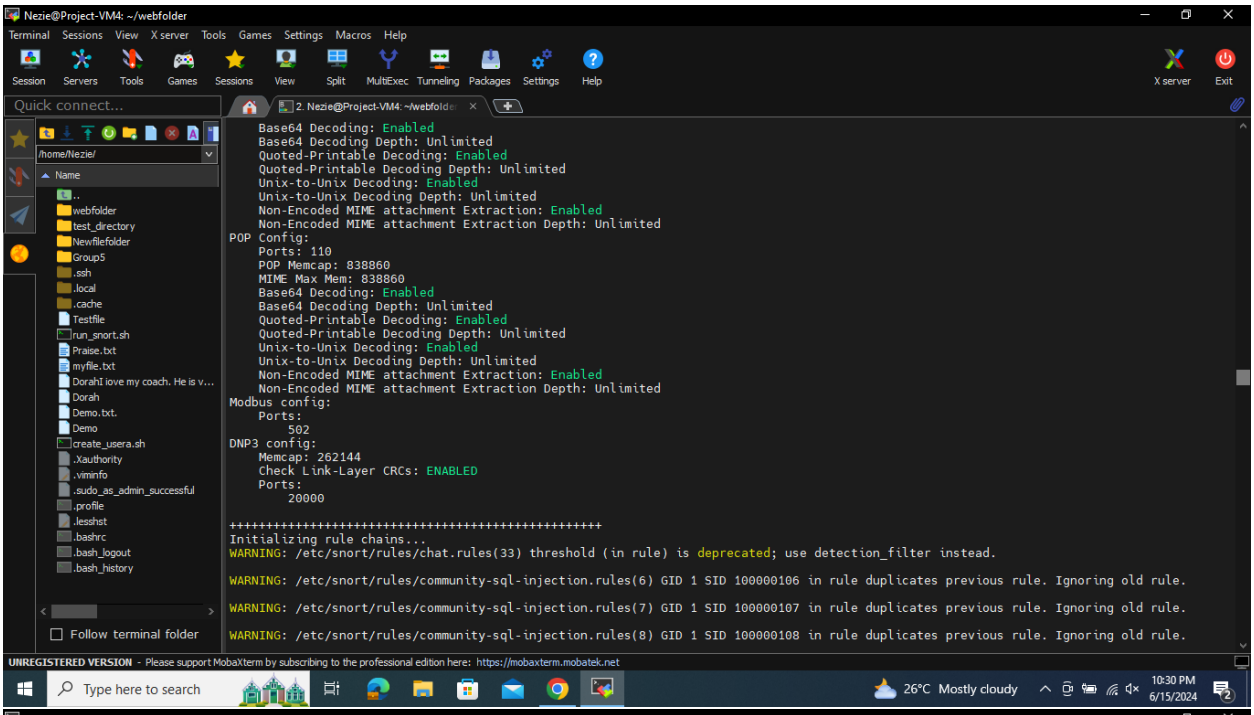

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolder
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
Dorah I love my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
none
+----------[event-filter-local]----------
| gen-id=1 sig-id=1991 type=Limit tracking=src count=1 seconds=60
| gen-id=1 sig-id=2275 type=Threshold tracking=dst count=5 seconds=60
| gen-id=1 sig-id=2523 type=Both tracking=dst count=10 seconds=10
| gen-id=1 sig-id=2924 type=Threshold tracking=dst count=10 seconds=60
| gen-id=1 sig-id=2923 type=Threshold tracking=dst count=10 seconds=60
| gen-id=1 sig-id=2496 type=Both tracking=dst count=20 seconds=60
| gen-id=1 sig-id=2495 type=Both tracking=dst count=20 seconds=60
| gen-id=1 sig-id=2494 type=Both tracking=dst count=20 seconds=60
| gen-id=1 sig-id=3273 type=Threshold tracking=src count=5 seconds=2
| gen-id=1 sig-id=3152 type=Threshold tracking=src count=5 seconds=2
+----------[suppression]----------
| none
Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!
WARNING: flowbits key 'ms_sql_seen_dns' is checked but not ever set.
WARNING: flowbits key 'smb.tree.create.llsrpc' is set but not ever checked.
33 out of 1024 flowbits in use.
[Port Based Pattern Matching Memory]
+- [Aho-Corasick Summary] ----------
| Storage Format : Full-Q
| Finite Automaton : DFA
| Alphabet Size : 256 Chars
| Sizeof State : Variable (1,2,4 bytes)
| Instances : 215
| 1 byte states : 204
| 2 byte states : 11
| 4 byte states : 0
| Characters : 64755
| States : 31951
| Transitions : 863868
| State Density : 10.6%
| Patterns : 5041
| Match States : 3836
| Memory (MB) : 16.90
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:31 PM
6/15/2024

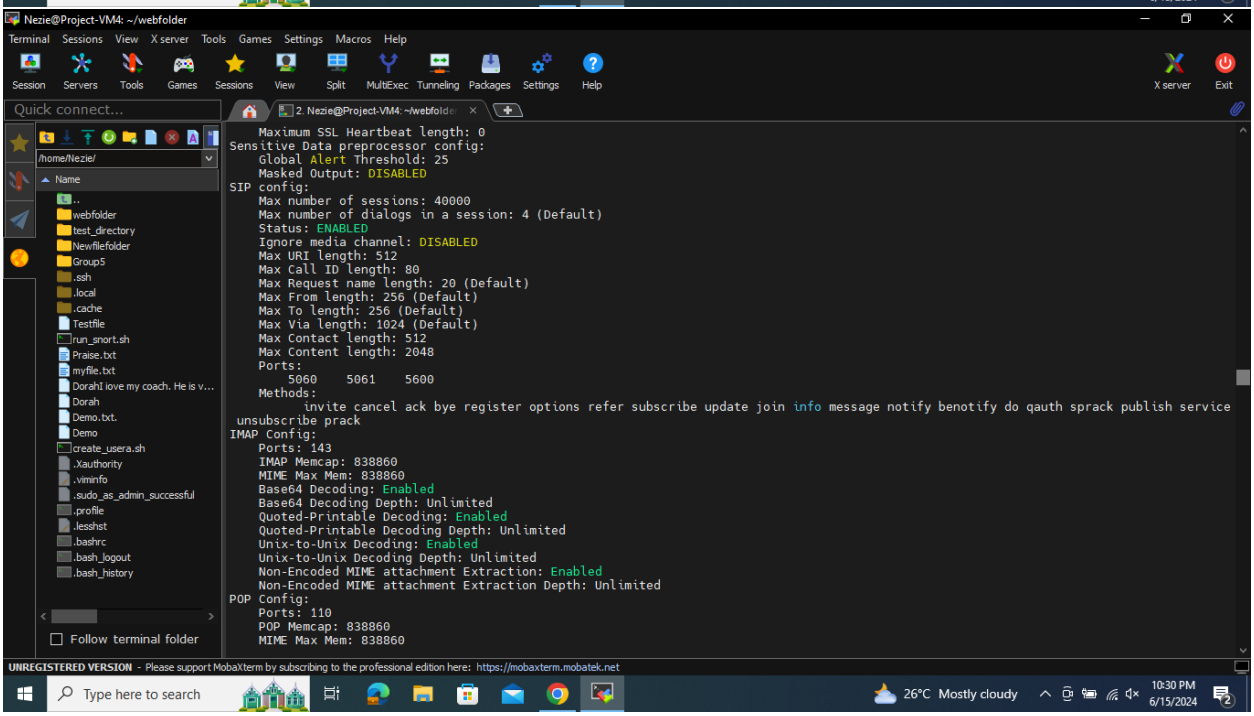

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
WARNING: /etc/snort/rules/community-web-php.rules(472) GID 1 SID 100000932 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-php.rules(473) GID 1 SID 100000933 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-php.rules(474) GID 1 SID 100000934 in rule duplicates previous rule. Ignoring old rule.
4057 Snort rules read
3383 detection rules
0 decoder rules
0 preprocessor rules
3383 Option Chains linked into 932 Chain Headers
+-------------------[Rule Port Counts]-------------------------------------
| tcp udp icmp ip
| src 151 18 0 0
| dst 3306 126 0 0
| any 383 48 52 22
| nc 27 8 15 20
| s+d 12 5 0 0
+--
+----------------------[detection-filter-config]---------------------------
| memory-cap : 1048576 bytes
+----------------------[detection-filter-rules]----------------------------
| none

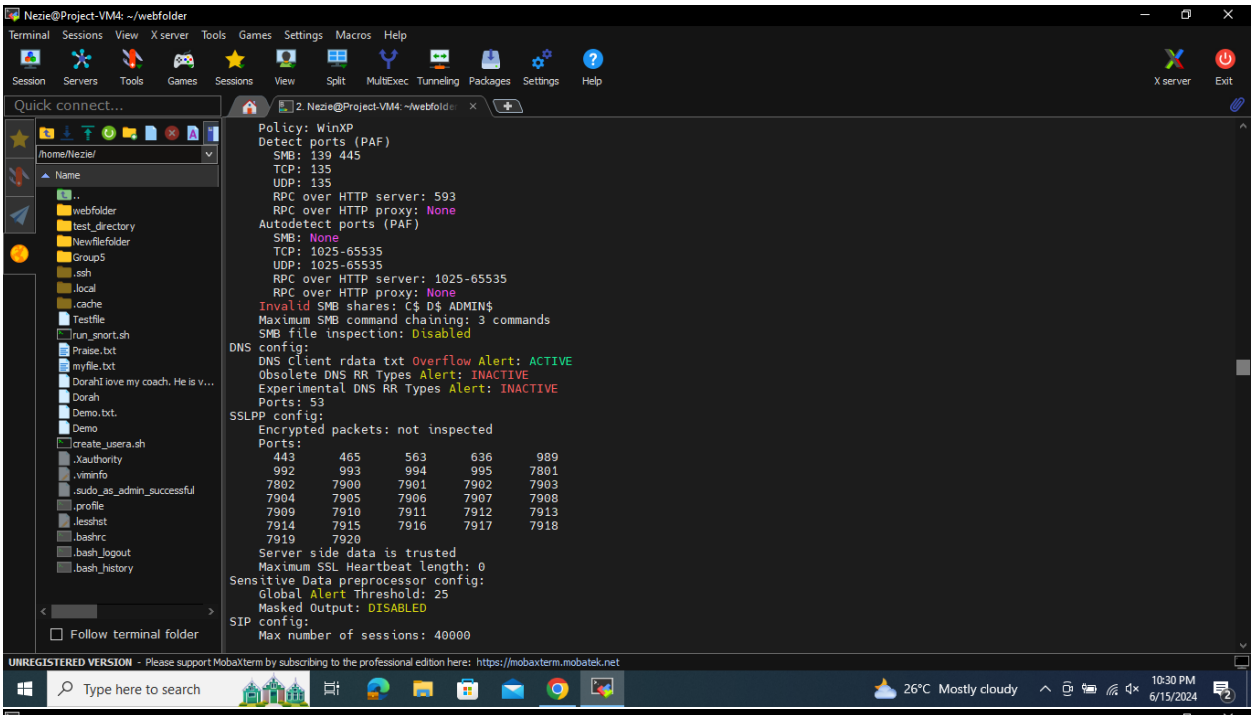
+----------------------[rate-filter-config]--------------------------------
| memory-cap : 1048576 bytes
+----------------------[rate-filter-rules]---------------------------------
| none

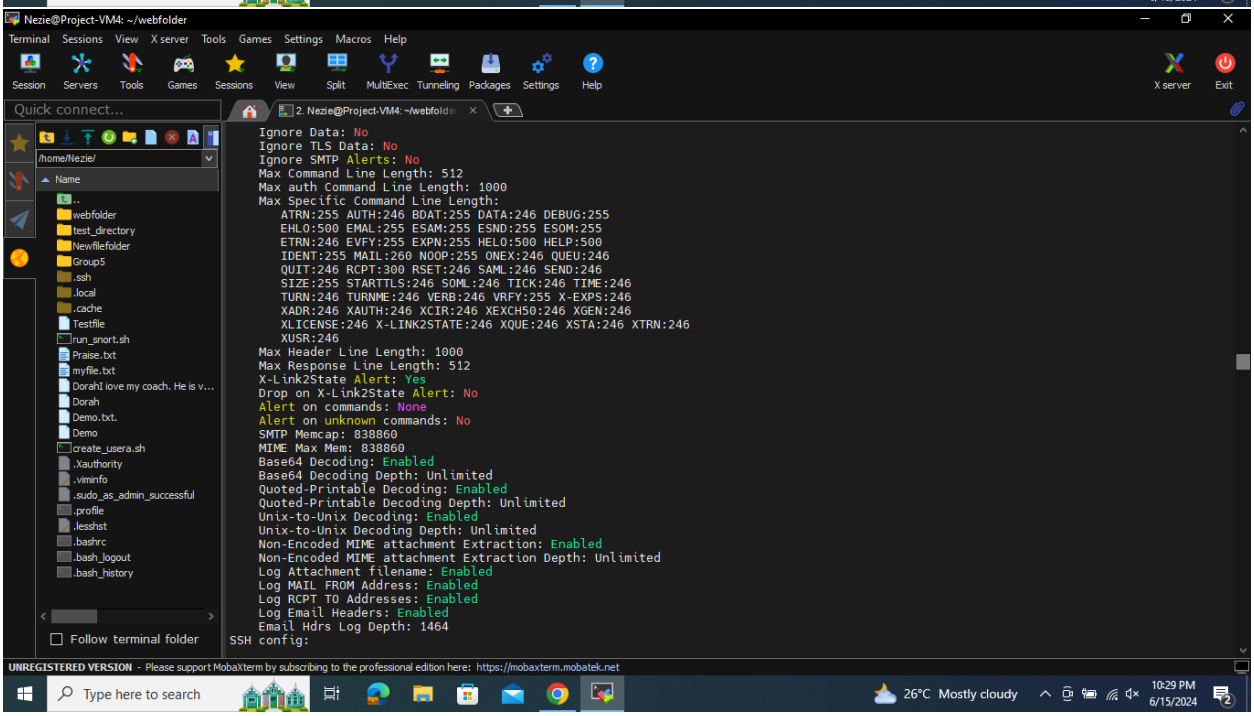
+----------------------[event-filter-config]-------------------------------
| memory-cap : 1048576 bytes
+----------------------[event-filter-global]-------------------------------
| none
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:31 PM
6/15/2024

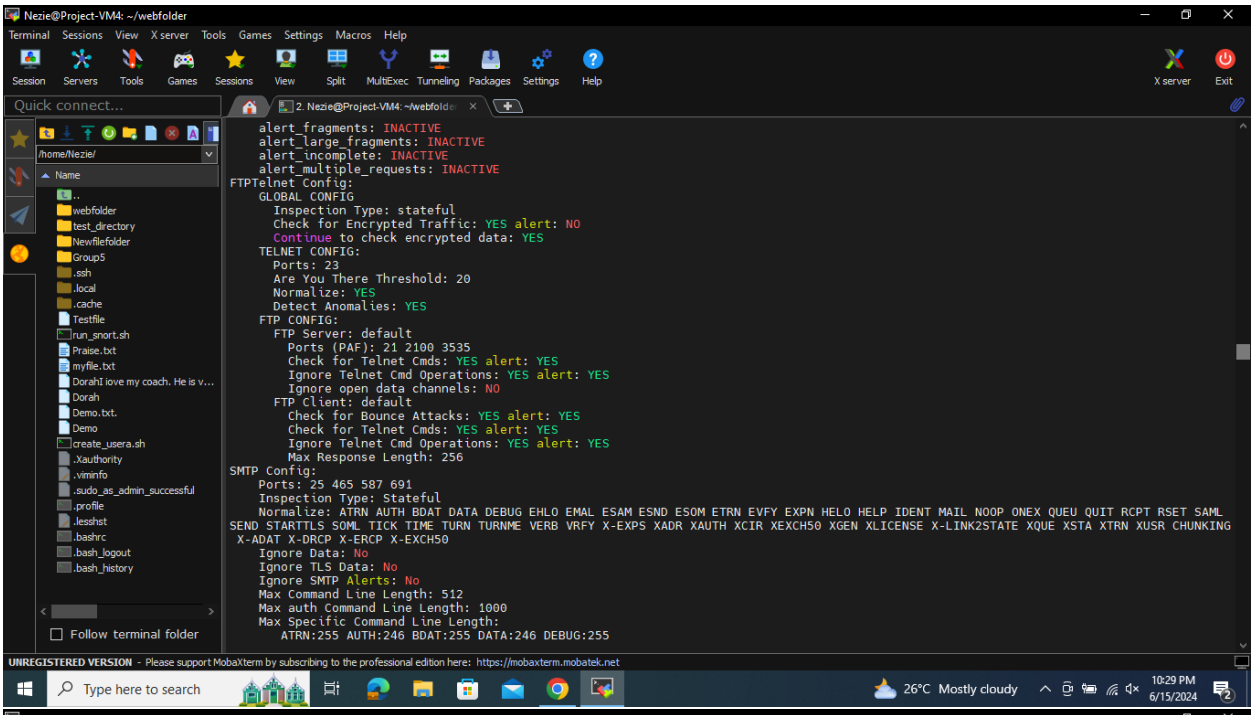

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
WARNING: /etc/snort/rules/community-sql-injection.rules(8) GID 1 SID 100000108 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-sql-injection.rules(9) GID 1 SID 100000109 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-sql-injection.rules(11) GID 1 SID 100000192 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-sql-injection.rules(12) GID 1 SID 100000193 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-sql-injection.rules(13) GID 1 SID 100000194 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-sql-injection.rules(14) GID 1 SID 100000690 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-sql-injection.rules(15) GID 1 SID 100000691 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-client.rules(6) GID 1 SID 100000118 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-client.rules(7) GID 1 SID 100000119 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-client.rules(9) GID 1 SID 100000228 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-client.rules(14) GID 1 SID 100000284 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-client.rules(16) GID 1 SID 100000447 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-client.rules(18) GID 1 SID 100000692 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-client.rules(20) GID 1 SID 100000693 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-client.rules(23) GID 1 SID 100000864 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-iis.rules(7) GID 1 SID 100000138 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-iis.rules(8) GID 1 SID 100000139 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-iis.rules(9) GID 1 SID 100000173 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-iis.rules(10) GID 1 SID 100000174 in rule duplicates previous rule. Ignoring old rule.
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:31 PM
6/15/2024

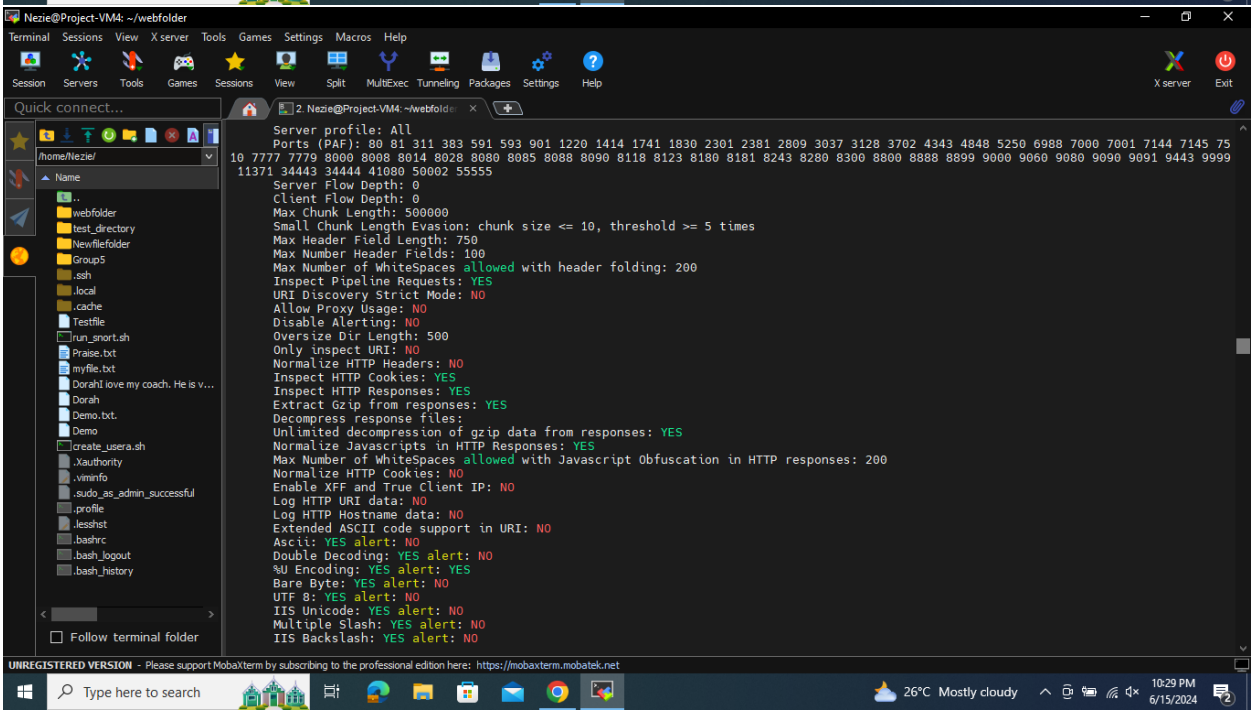

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Base64 Decoding: Enabled
Base64 Decoding Depth: Unlimited
Quoted-Printable Decoding: Enabled
Quoted-Printable Decoding Depth: Unlimited
Unix-to-Unix Decoding: Enabled
Unix-to-Unix Decoding Depth: Unlimited
Non-Encoded MIME attachment Extraction: Enabled
Non-Encoded MIME attachment Extraction Depth: Unlimited
POP Config:
Ports: 110
POP Memcap: 838860
MIME Max Mem: 838860
Base64 Decoding: Enabled
Base64 Decoding Depth: Unlimited
Quoted-Printable Decoding: Enabled
Quoted-Printable Decoding Depth: Unlimited
Unix-to-Unix Decoding: Enabled
Unix-to-Unix Decoding Depth: Unlimited
Non-Encoded MIME attachment Extraction: Enabled
Non-Encoded MIME attachment Extraction Depth: Unlimited
Modbus config:
Ports:
502
DNP3 config:
Memcap: 262144
Check Link-Layer CRCs: ENABLED
Ports:
20000
++
Initializing rule chains...
WARNING: /etc/snort/rules/chat.rules(33) threshold (in rule) is deprecated; use detection_filter instead.
WARNING: /etc/snort/rules/community-sql-injection.rules(6) GID 1 SID 100000106 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-sql-injection.rules(7) GID 1 SID 100000107 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-sql-injection.rules(8) GID 1 SID 100000108 in rule duplicates previous rule. Ignoring old rule.
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:30 PM
6/15/2024

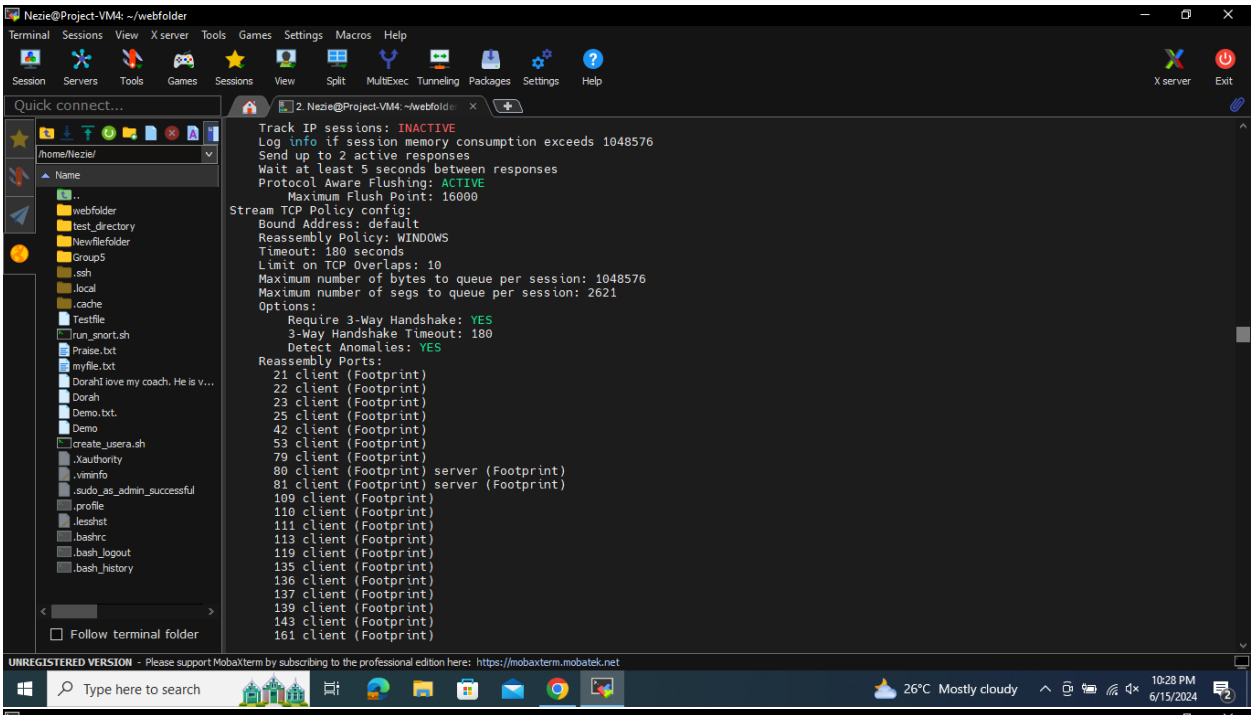

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Maximum SSL Heartbeat length: 0
Sensitive Data preprocessor config:
Global Alert Threshold: 25
Masked Output: DISABLED
SIP config:
Max number of sessions: 40000
Max number of dialogs in a session: 4 (Default)
Status: ENABLED
Ignore media channel: DISABLED
Max URI length: 512
Max Call ID length: 80
Max Request name length: 20 (Default)
Max From length: 256 (Default)
Max To length: 256 (Default)
Max Via length: 1024 (Default)
Max Contact length: 512
Max Content length: 2048
Ports:
5060 5061 5600
Methods:
invite cancel ack bye register options refer subscribe update join info message notify benotify do qauth sprack publish service
unsubscribe prack
IMAP Config:
Ports: 143
IMAP Memcap: 838860
MIME Max Mem: 838860
Base64 Decoding: Enabled
Base64 Decoding Depth: Unlimited
Quoted-Printable Decoding: Enabled
Quoted-Printable Decoding Depth: Unlimited
Unix-to-Unix Decoding: Enabled
Unix-to-Unix Decoding Depth: Unlimited
Non-Encoded MIME attachment Extraction: Enabled
Non-Encoded MIME attachment Extraction Depth: Unlimited
POP Config:
Ports: 110
POP Memcap: 838860
MIME Max Mem: 838860
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:30 PM
6/15/2024

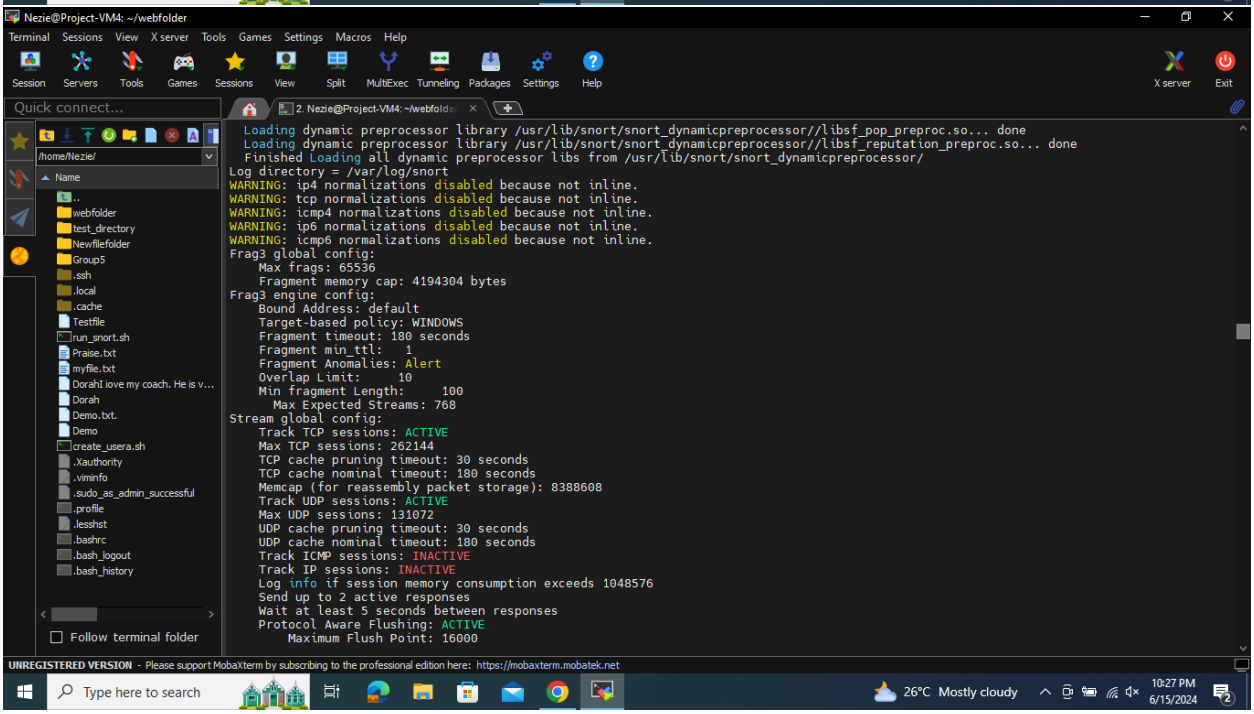

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolder
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Policy: WinXP
Detect ports (PAF)
SMB: 139 445
TCP: 135
UDP: 135
RPC over HTTP server: 593
RPC over HTTP proxy: None
Autodetect ports (PAF)
SMB: None
TCP: 1025-65535
UDP: 1025-65535
RPC over HTTP server: 1025-65535
RPC over HTTP proxy: None
Invalid SMB shares: C$ D$ ADMIN$
Maximum SMB command chaining: 3 commands
SMB file inspection: Disabled
DNS config:
DNS Client rdata txt Overflow Alert: ACTIVE
Obsolete DNS RR Types Alert: INACTIVE
Experimental DNS RR Types Alert: INACTIVE
Ports: 53
SSLPP config:
Encrypted packets: not inspected
Ports:
443 465 563 636 989
992 993 994 995 7801
7802 7900 7901 7902 7903
7904 7905 7906 7907 7908
7909 7910 7911 7912 7913
7914 7915 7916 7917 7918
7919 7920
Server side data is trusted
Maximum SSL Heartbeat length: 0
Sensitive Data preprocessor config:
Global Alert Threshold: 25
Masked Output: DISABLED
SIP config:
Max number of sessions: 40000
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:30 PM
6/15/2024

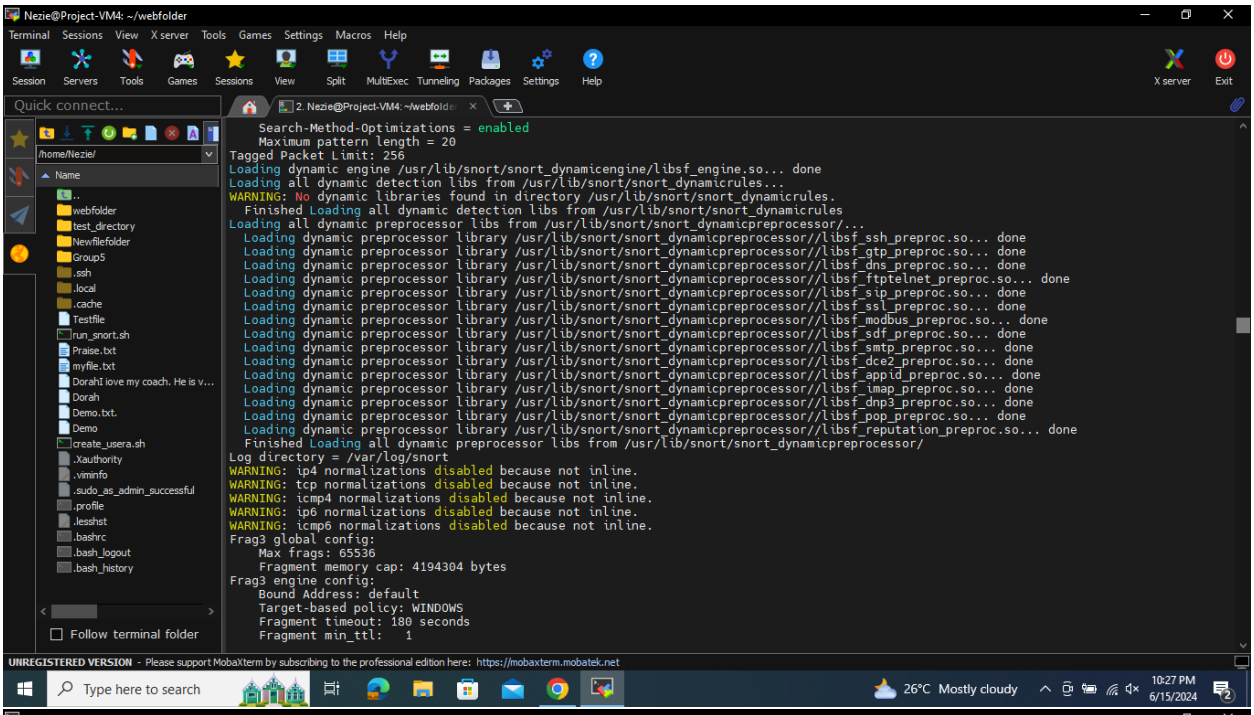

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolder
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Ignore Data: No
Ignore TLS Data: No
Ignore SMTP Alerts: No
Max Command Line Length: 512
Max auth Command Line Length: 1000
Max Specific Command Line Length:
ATRN:255 AUTH:246 BDAT:255 DATA:246 DEBUG:255
EHLO:500 EMAL:255 ESAM:255 ESND:255 ESOM:255
ETRN:246 EVFY:255 EXPN:255 HELO:500 HELP:500
IDENT:255 MAIL:260 NOOP:255 ONEX:246 QUEU:246
QUIT:246 RCPT:300 RSET:246 SAML:246 SEND:246
SIZE:255 STARTTLS:246 SOML:246 TICK:246 TIME:246
TURN:246 TURNME:246 VERB:246 VRFY:255 X-EXPS:246
XADR:246 XAUTH:246 XCIR:246 XEXCH50:246 XGEN:246
XLICENSE:246 X-LINK2STATE:246 XQUE:246 XSTA:246 XTRN:246
XUSR:246
Max Header Line Length: 1000
Max Response Line Length: 512
X-Link2State Alert: Yes
Drop on X-Link2State Alert: No
Alert on commands: None
Alert on unknown commands: No
SMTP Memcap: 838860
MIME Max Mem: 838860
Base64 Decoding: Enabled
Base64 Decoding Depth: Unlimited
Quoted-Printable Decoding: Enabled
Quoted-Printable Decoding Depth: Unlimited
Unix-to-Unix Decoding: Enabled
Unix-to-Unix Decoding Depth: Unlimited
Non-Encoded MIME attachment Extraction: Enabled
Non-Encoded MIME attachment Extraction Depth: Unlimited
Log Attachment filename: Enabled
Log MAIL FROM Address: Enabled
Log RCPT TO Addresses: Enabled
Log Email Headers: Enabled
Email Hdrs Log Depth: 1464
SSH config:
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:29 PM
6/15/2024

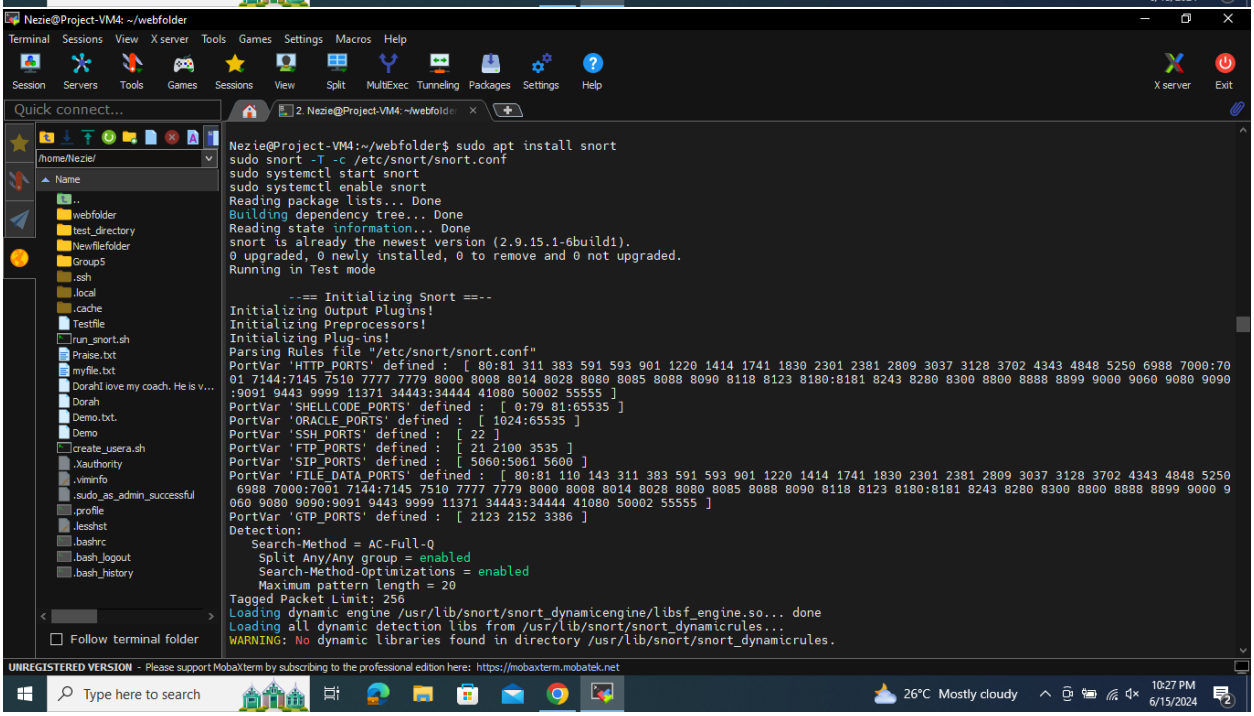

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
alert_fragments: INACTIVE
alert_large_fragments: INACTIVE
alert_incomplete: INACTIVE
alert_multiple_requests: INACTIVE
FTPTelnet Config:
GLOBAL CONFIG
Inspection Type: stateful
Check for Encrypted Traffic: YES alert: NO
Continue to check encrypted data: YES
TELNET CONFIG:
Ports: 23
Are You There Threshold: 20
Normalize: YES
Detect Anomalies: YES
FTP CONFIG:
FTP Server: default
Ports (PAF): 21 2100 3535
Check for Telnet Cmds: YES alert: YES
Ignore Telnet Cmd Operations: YES alert: YES
Ignore open data channels: NO
FTP Client: default
Check for Bounce Attacks: YES alert: YES
Check for Telnet Cmds: YES alert: YES
Ignore Telnet Cmd Operations: YES alert: YES
Max Response Length: 256
SMTP Config:
Ports: 25 465 587 691
Inspection Type: Stateful
Normalize: ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML
SEND STARTTLS SOML TICK TIME TURN TURNME VERB VRFY X-EXPS XADR XAUTH XCIR XEXCH50 XGEN XLICENSE X-LINK2STATE XQUE XSTA XTRN XUSR CHUNKING
X-ADAT X-DRCP X-ERCP X-EXCH50
Ignore Data: No
Ignore TLS Data: No
Ignore SMTP Alerts: No
Max Command Line Length: 512
Max auth Command Line Length: 1000
Max Specific Command Line Length:
ATRN:255 AUTH:246 BDAT:255 DATA:246 DEBUG:255
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:29 PM
6/15/2024

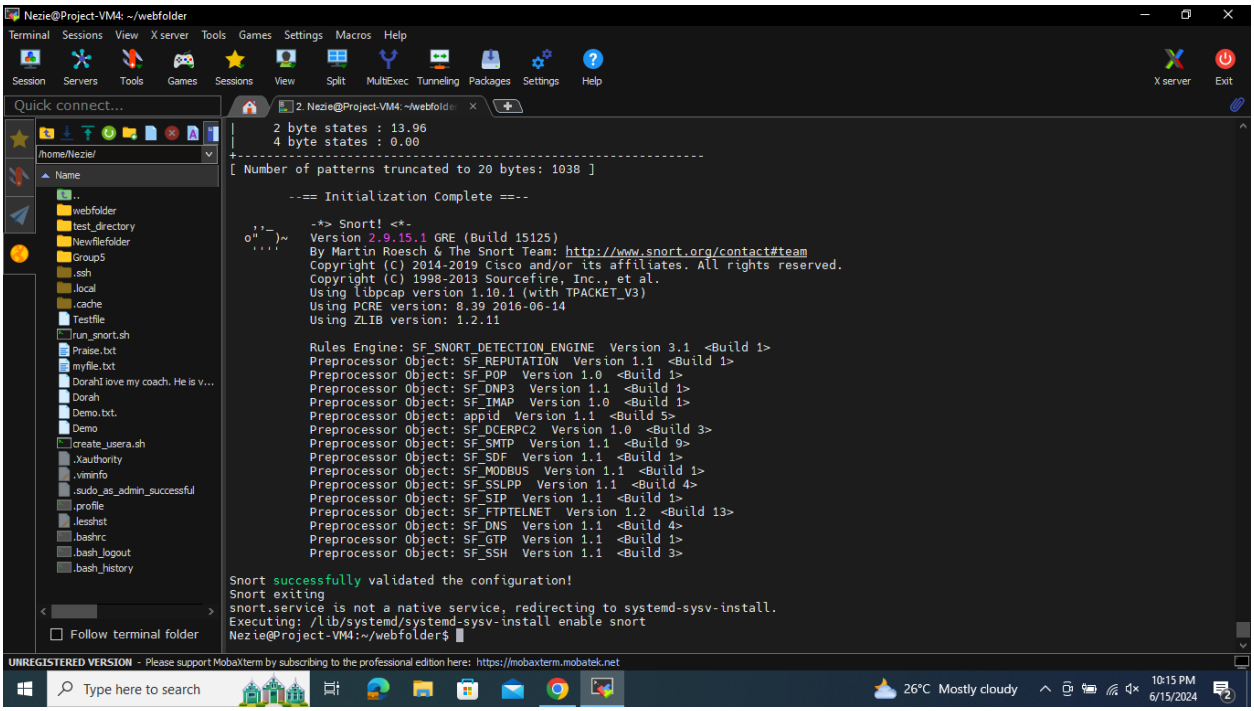

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Server profile: All
Ports (PAF): 80 81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000 7001 7144 7145 75
10 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180 8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090 9091 9443 9999
11371 34443 34444 41080 50002 55555
Server Flow Depth: 0
Client Flow Depth: 0
Max Chunk Length: 500000
Small Chunk Length Evasion: chunk size <= 10, threshold >= 5 times
Max Header Field Length: 750
Max Number Header Fields: 100
Max Number of WhiteSpaces allowed with header folding: 200
Inspect Pipeline Requests: YES
URI Discovery Strict Mode: NO
Allow Proxy Usage: NO
Disable Alerting: NO
Oversize Dir Length: 500
Only inspect URI: NO
Normalize HTTP Headers: NO
Inspect HTTP Cookies: YES
Inspect HTTP Responses: YES
Extract Gzip from responses: YES
Decompress response files:
Unlimited decompression of gzip data from responses: YES
Normalize Javascripts in HTTP Responses: YES
Max Number of WhiteSpaces allowed with Javascript Obfuscation in HTTP responses: 200
Normalize HTTP Cookies: NO
Enable XFF and True Client IP: NO
Log HTTP URI data: NO
Log HTTP Hostname data: NO
Extended ASCII code support in URI: NO
Ascii: YES alert: NO
Double Decoding: YES alert: NO
%U Encoding: YES alert: YES
Bare Byte: YES alert: NO
UTF 8: YES alert: NO
IIS Unicode: YES alert: NO
Multiple Slash: YES alert: NO
IIS Backslash: YES alert: NO
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:29 PM
6/15/2024


Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Track IP sessions: INACTIVE
Log info if session memory consumption exceeds 1048576
Send up to 2 active responses
Wait at least 5 seconds between responses
Protocol Aware Flushing: ACTIVE
Maximum Flush Point: 16000
Stream TCP Policy config:
Bound Address: default
Reassembly Policy: WINDOWS
Timeout: 180 seconds
Limit on TCP Overlaps: 10
Maximum number of bytes to queue per session: 1048576
Maximum number of segs to queue per session: 2621
Options:
Require 3-Way Handshake: YES
3-Way Handshake Timeout: 180
Detect Anomalies: YES
Reassembly Ports:
21 client (Footprint)
22 client (Footprint)
23 client (Footprint)
25 client (Footprint)
42 client (Footprint)
53 client (Footprint)
79 client (Footprint)
80 client (Footprint) server (Footprint)
81 client (Footprint) server (Footprint)
109 client (Footprint)
110 client (Footprint)
111 client (Footprint)
113 client (Footprint)
119 client (Footprint)
135 client (Footprint)
136 client (Footprint)
137 client (Footprint)
139 client (Footprint)
143 client (Footprint)
161 client (Footprint)
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:28 PM
6/15/2024

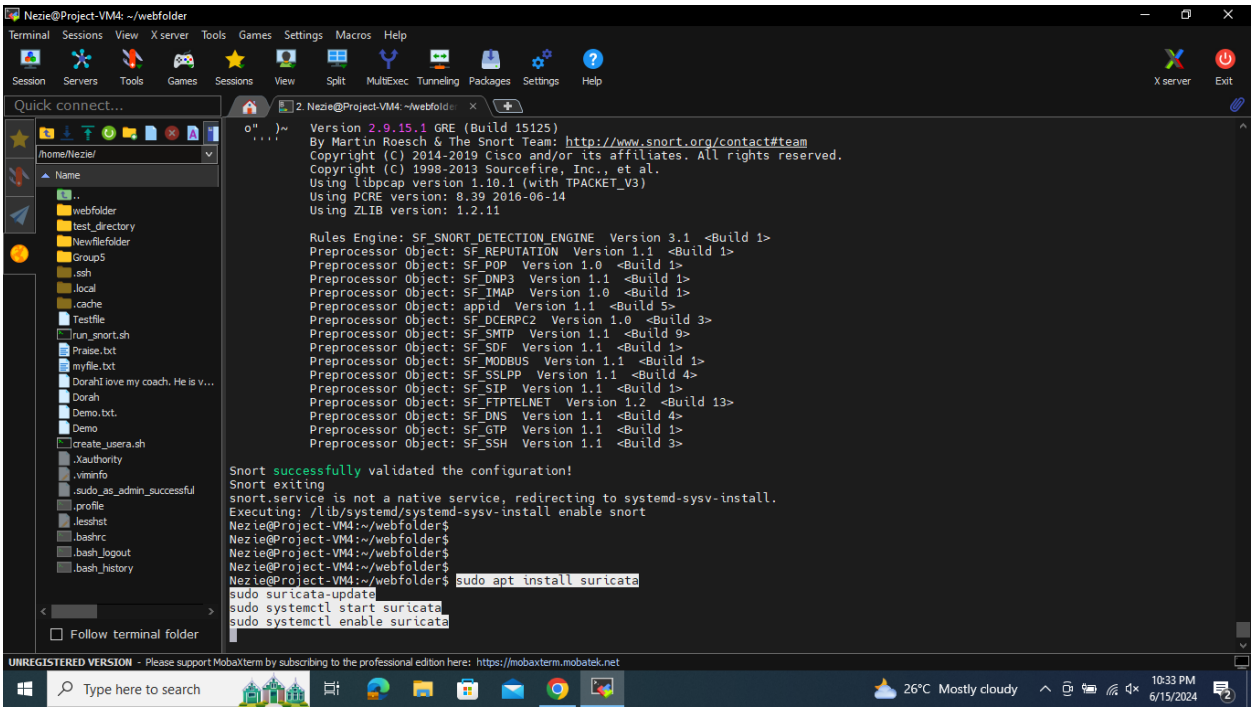

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_pop_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_reputation_preproc.so... done
Finished Loading all dynamic preprocessor libs from /usr/lib/snort/snort_dynamicpreprocessor/
Log directory = /var/log/snort
WARNING: ip4 normalizations disabled because not inline.
WARNING: tcp normalizations disabled because not inline.
WARNING: icmp4 normalizations disabled because not inline.
WARNING: ip6 normalizations disabled because not inline.
WARNING: icmp6 normalizations disabled because not inline.
Frag3 global config:
Max frags: 65536
Fragment memory cap: 4194304 bytes
Frag3 engine config:
Bound Address: default
Target-based policy: WINDOWS
Fragment timeout: 180 seconds
Fragment min_ttl: 1
Fragment Anomalies: Alert
Overlap Limit: 10
Min fragment Length: 100
Max Expected Streams: 768
Stream global config:
Track TCP sessions: ACTIVE
Max TCP sessions: 262144
TCP cache pruning timeout: 30 seconds
TCP cache nominal timeout: 180 seconds
Memcap (for reassembly packet storage): 8388608
Track UDP sessions: ACTIVE
Max UDP sessions: 131072
UDP cache pruning timeout: 30 seconds
UDP cache nominal timeout: 180 seconds
Track ICMP sessions: INACTIVE
Track IP sessions: INACTIVE
Log info if session memory consumption exceeds 1048576
Send up to 2 active responses
Wait at least 5 seconds between responses
Protocol Aware Flushing: ACTIVE
Maximum Flush Point: 16000
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:27 PM
6/15/2024

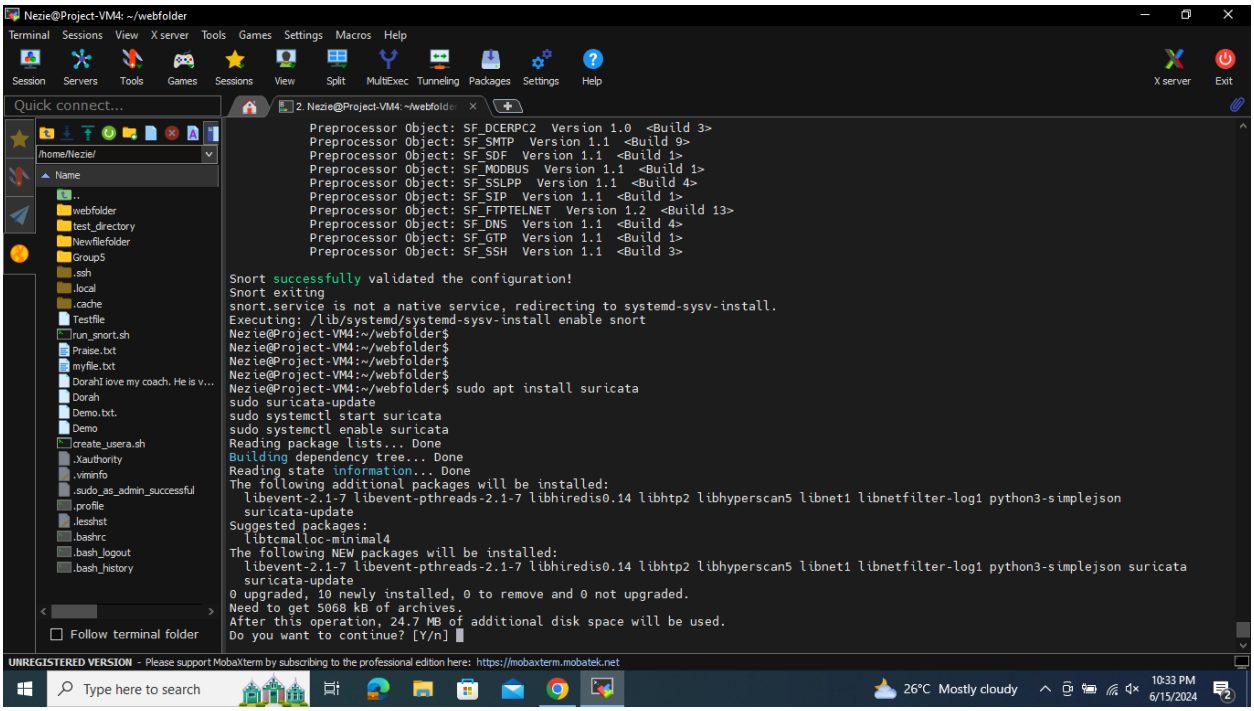

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolder
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Search-Method-Optimizations = enabled
Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/lib/snort/snort_dynamicrules.
Finished Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules
Loading all dynamic preprocessor libs from /usr/lib/snort/snort_dynamicpreprocessor/...
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_ssh_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_gtp_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_dns_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_ftptelnet_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_sip_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_ssl_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_modbus_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_sdf_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_smtp_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_dce2_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_appid_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_imap_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_dnp3_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_pop_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_reputation_preproc.so... done
Finished Loading all dynamic preprocessor libs from /usr/lib/snort/snort_dynamicpreprocessor/
Log directory = /var/log/snort
WARNING: ip4 normalizations disabled because not inline.
WARNING: tcp normalizations disabled because not inline.
WARNING: icmp4 normalizations disabled because not inline.
WARNING: ip6 normalizations disabled because not inline.
WARNING: icmp6 normalizations disabled because not inline.
Frag3 global config:
Max frags: 65536
Fragment memory cap: 4194304 bytes
Frag3 engine config:
Bound Address: default
Target-based policy: WINDOWS
Fragment timeout: 180 seconds
Fragment min_ttl: 1
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:27 PM
6/15/2024

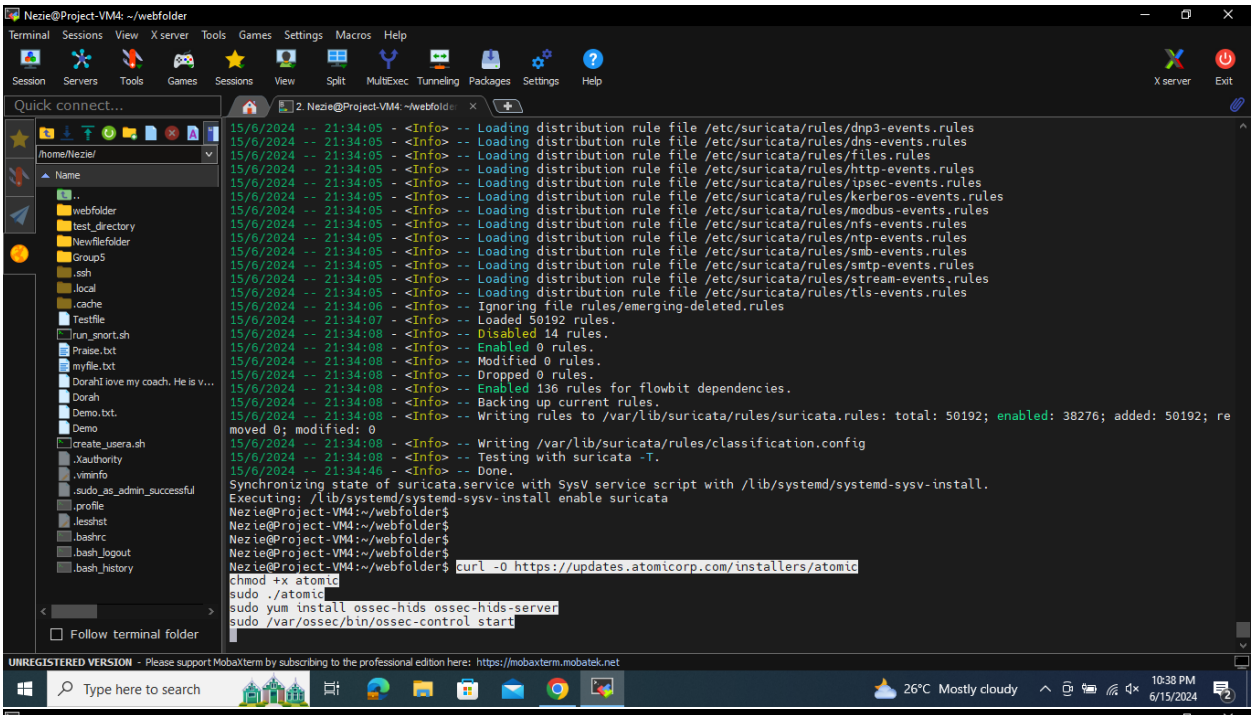

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolder
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Nezie@Project-VM4:~/webfolder$ sudo apt install snort
sudo snort -T -c /etc/snort/snort.conf
sudo systemctl start snort
sudo systemctl enable snort
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
snort is already the newest version (2.9.15.1-6build1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Running in Test mode
--== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555]
PortVar 'SHELLCODE_PORTS' defined : [0:79 81:65535]
PortVar 'ORACLE_PORTS' defined : [1024:65535]
PortVar 'SSH_PORTS' defined : [22]
PortVar 'FTP_PORTS' defined : [21 2100 3535]
PortVar 'SIP_PORTS' defined : [5060:5061 5600]
PortVar 'FILE_DATA_PORTS' defined : [80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555]
PortVar 'GTP_PORTS' defined : [2123 2152 3386]
Detection:
Search-Method = AC-Full-Q
Split Any/Any group = enabled
Search-Method-Optimizations = enabled
Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/lib/snort/snort_dynamicrules.
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:27 PM
6/15/2024

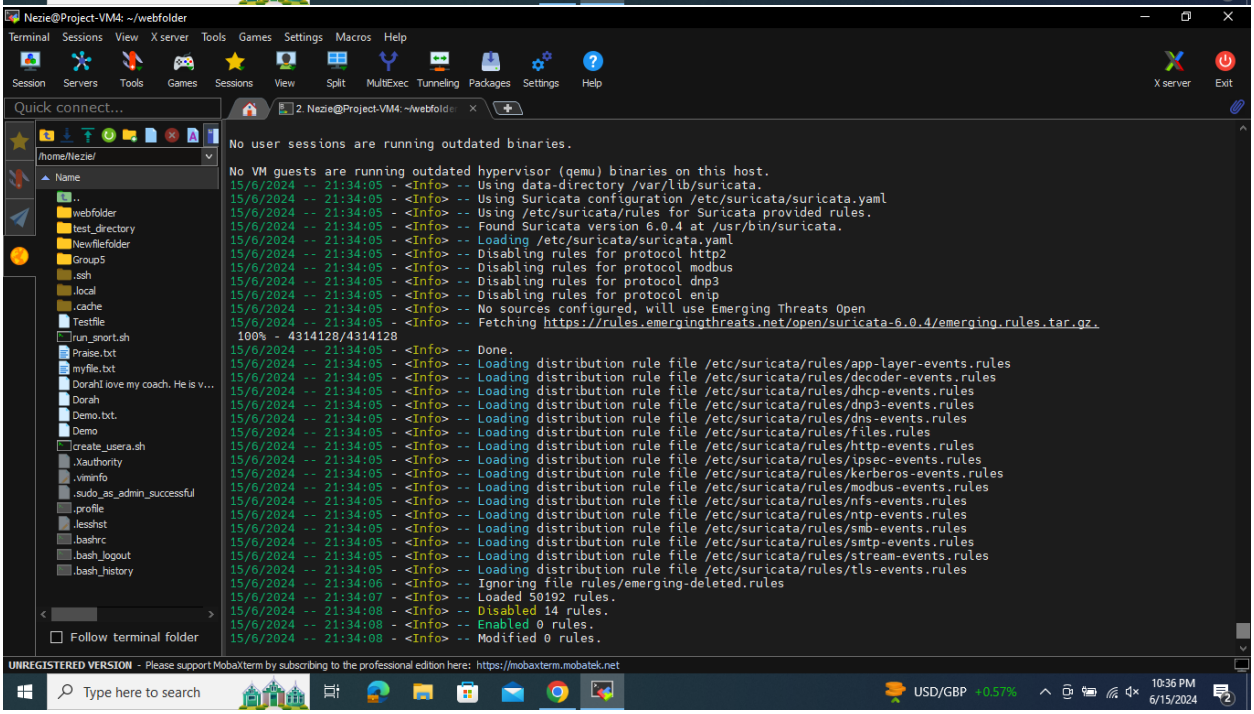


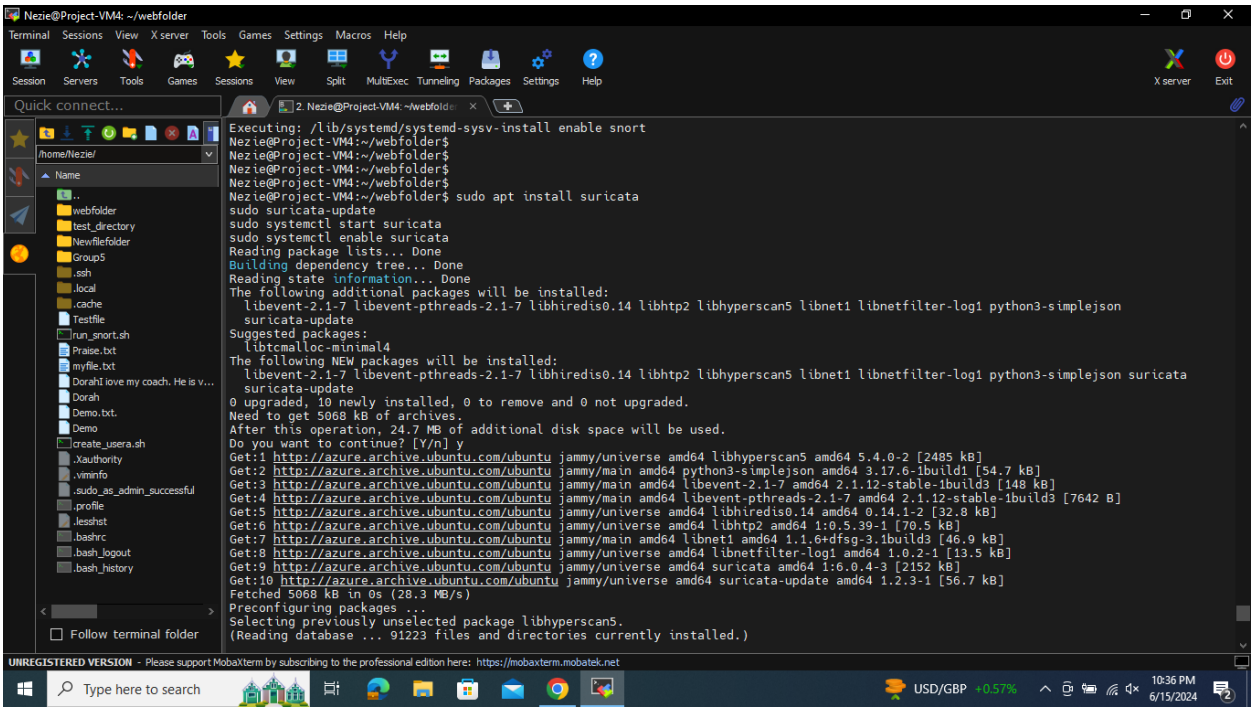
Suricata was installed: Suricata is an advanced IDS/IPS.
Commands: sudo apt install suricata
sudo suricata-update
sudo systemctl start suricata
sudo systemctl enable suricata




Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Snort successfully validated the configuration!
Snort exiting
snort.service is not a native service, redirecting to systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable snort
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo apt install suricata
sudo suricata-update
sudo systemctl start suricata
sudo systemctl enable suricata
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libevent-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhtp2 libhyperscan5 libnet1 libnetfilter-log1 python3-simplejson
suricata-update
Suggested packages:
libtcmalloc-minimal4
The following NEW packages will be installed:
libevent-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhtp2 libhyperscan5 libnet1 libnetfilter-log1 python3-simplejson suricata
suricata-update
0 upgraded, 10 newly installed, 0 to remove and 0 not upgraded.
Need to get 5068 kB of archives.
After this operation, 24.7 MB of additional disk space will be used.
Do you want to continue? [Y/n]
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:33 PM
6/15/2024

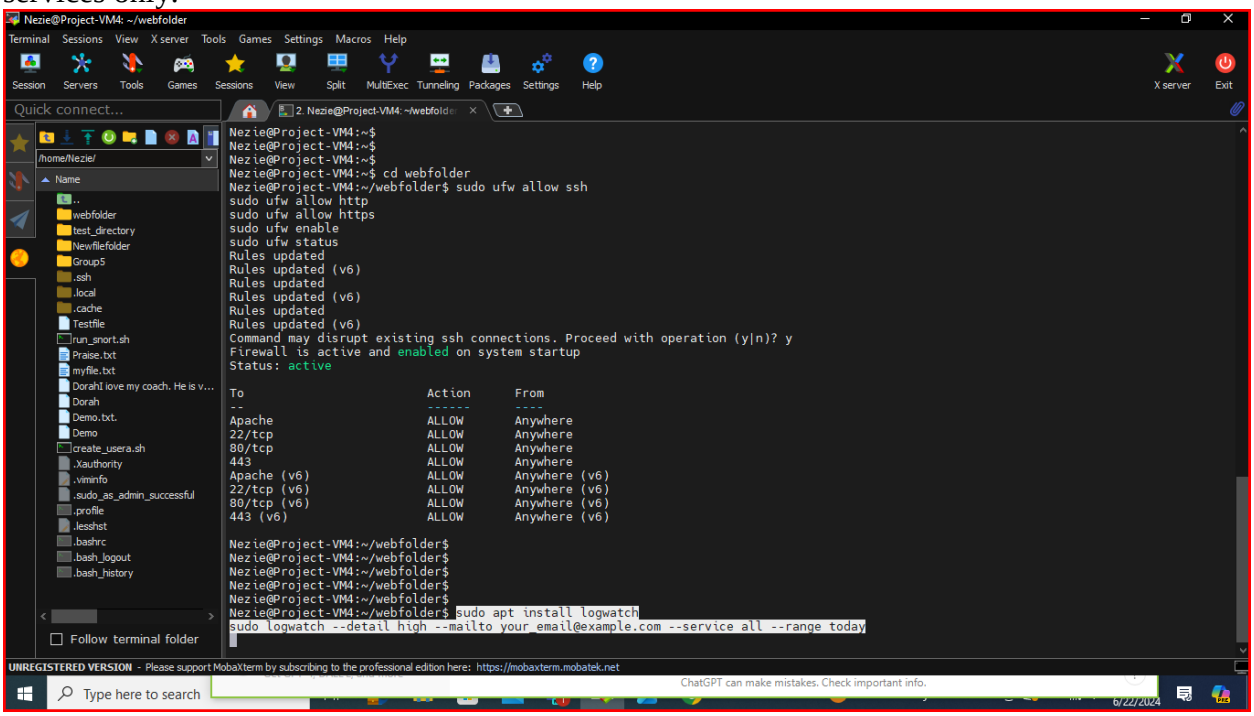

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolder
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/dnp3-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/dns-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/files.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/http-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/ipsec-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/kerberos-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/modbus-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/nfs-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/ntp-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/smb-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/smtp-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/stream-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/tls-events.rules
15/6/2024 -- 21:34:06 - <Info> -- Ignoring file rules/emerging-deleted.rules
15/6/2024 -- 21:34:07 - <Info> -- Loaded 50192 rules.
15/6/2024 -- 21:34:08 - <Info> -- Disabled 14 rules.
15/6/2024 -- 21:34:08 - <Info> -- Enabled 0 rules.
15/6/2024 -- 21:34:08 - <Info> -- Modified 0 rules.
15/6/2024 -- 21:34:08 - <Info> -- Dropped 0 rules.
15/6/2024 -- 21:34:08 - <Info> -- Enabled 136 rules for flowbit dependencies.
15/6/2024 -- 21:34:08 - <Info> -- Backing up current rules.
15/6/2024 -- 21:34:08 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 50192; enabled: 38276; added: 50192; re
moved 0; modified: 0
15/6/2024 -- 21:34:08 - <Info> -- Writing /var/lib/suricata/rules/classification.config
15/6/2024 -- 21:34:08 - <Info> -- Testing with suricata -T.
15/6/2024 -- 21:34:46 - <Info> -- Done.
Synchronizing state of suricata.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable suricata
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ curl -O https://updates.atomicorp.com/installers/atomic
chmod +x atomic
sudo ./atomic
sudo yum install ossec-hids ossec-hids-server
sudo /var/ossec/bin/ossec-control start
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
26°C Mostly cloudy
10:38 PM
6/15/2024

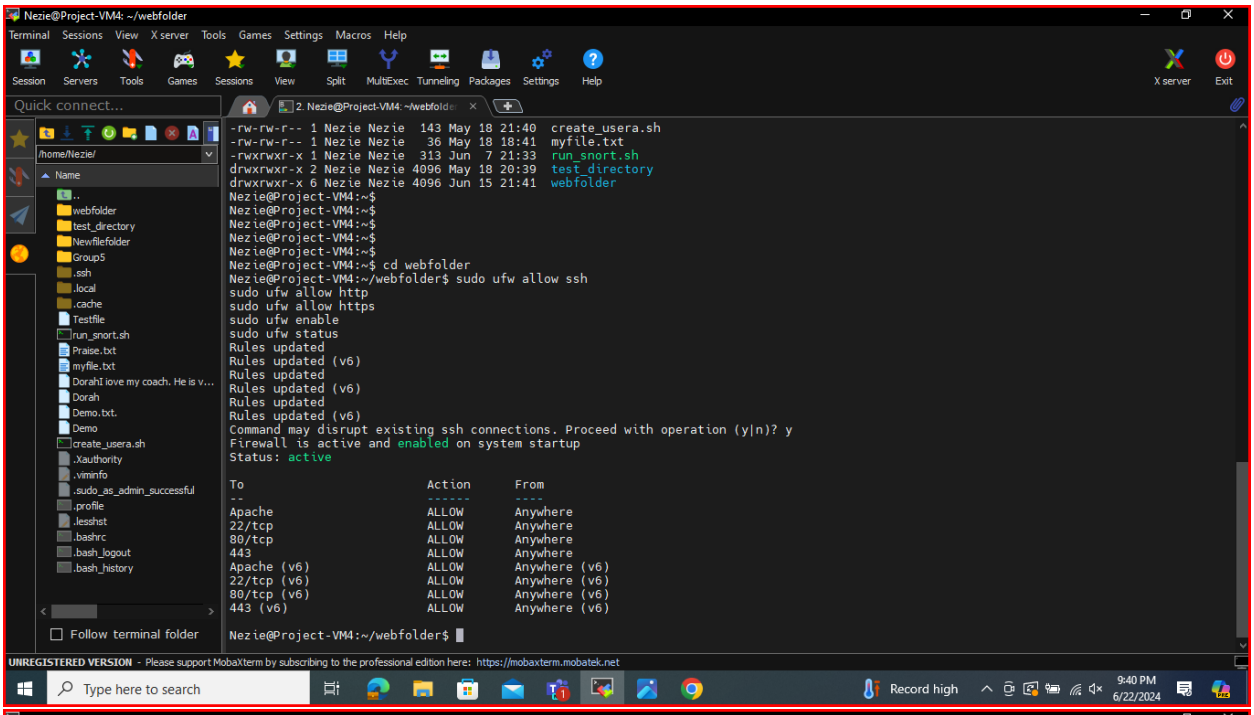

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolder
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
15/6/2024 -- 21:34:05 - <Info> -- Using data-directory /var/lib/suricata.
15/6/2024 -- 21:34:05 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
15/6/2024 -- 21:34:05 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
15/6/2024 -- 21:34:05 - <Info> -- Found Suricata version 6.0.4 at /usr/bin/suricata.
15/6/2024 -- 21:34:05 - <Info> -- Loading /etc/suricata/suricata.yaml
15/6/2024 -- 21:34:05 - <Info> -- Disabling rules for protocol http2
15/6/2024 -- 21:34:05 - <Info> -- Disabling rules for protocol modbus
15/6/2024 -- 21:34:05 - <Info> -- Disabling rules for protocol dnp3
15/6/2024 -- 21:34:05 - <Info> -- Disabling rules for protocol enip
15/6/2024 -- 21:34:05 - <Info> -- No sources configured, will use Emerging Threats Open
15/6/2024 -- 21:34:05 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-6.0.4/emerging.rules.tar.gz.
100% - 4314128/4314128
15/6/2024 -- 21:34:05 - <Info> -- Done.
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/app-layer-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/decoder-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/dhcp-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/dnp3-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/dns-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/files.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/http-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/ipsec-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/kerberos-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/modbus-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/nfs-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/ntp-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/smb-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/smtp-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/stream-events.rules
15/6/2024 -- 21:34:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/tls-events.rules
15/6/2024 -- 21:34:06 - <Info> -- Ignoring file rules/emerging-deleted.rules
15/6/2024 -- 21:34:07 - <Info> -- Loaded 50192 rules.
15/6/2024 -- 21:34:08 - <Info> -- Disabled 14 rules.
15/6/2024 -- 21:34:08 - <Info> -- Enabled 0 rules.
15/6/2024 -- 21:34:08 - <Info> -- Modified 0 rules.
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
USD/GBP +0.57%
10:36 PM
6/15/2024

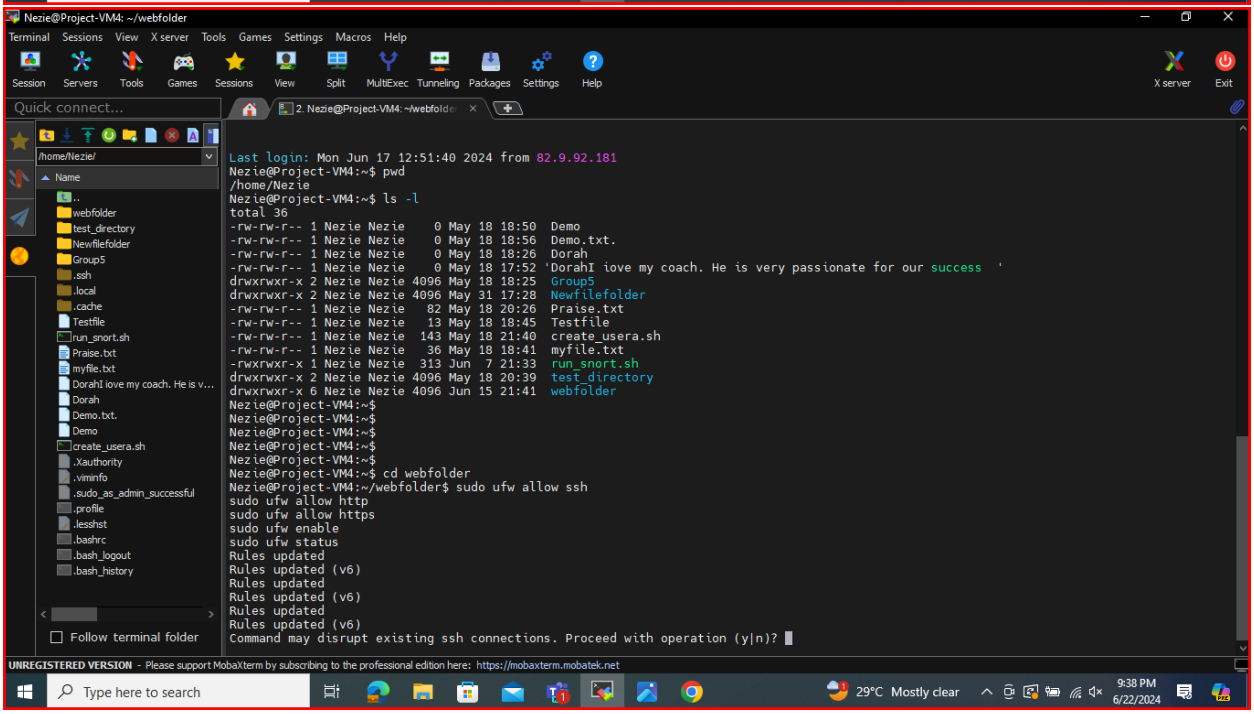


2. **Configure Alerts and Notifications:** Configure your IDS/IPS to send alerts via email or other notification methods.

3. **Enable and Configure a Firewall:** Set up firewall rules to restrict access to necessary services only.



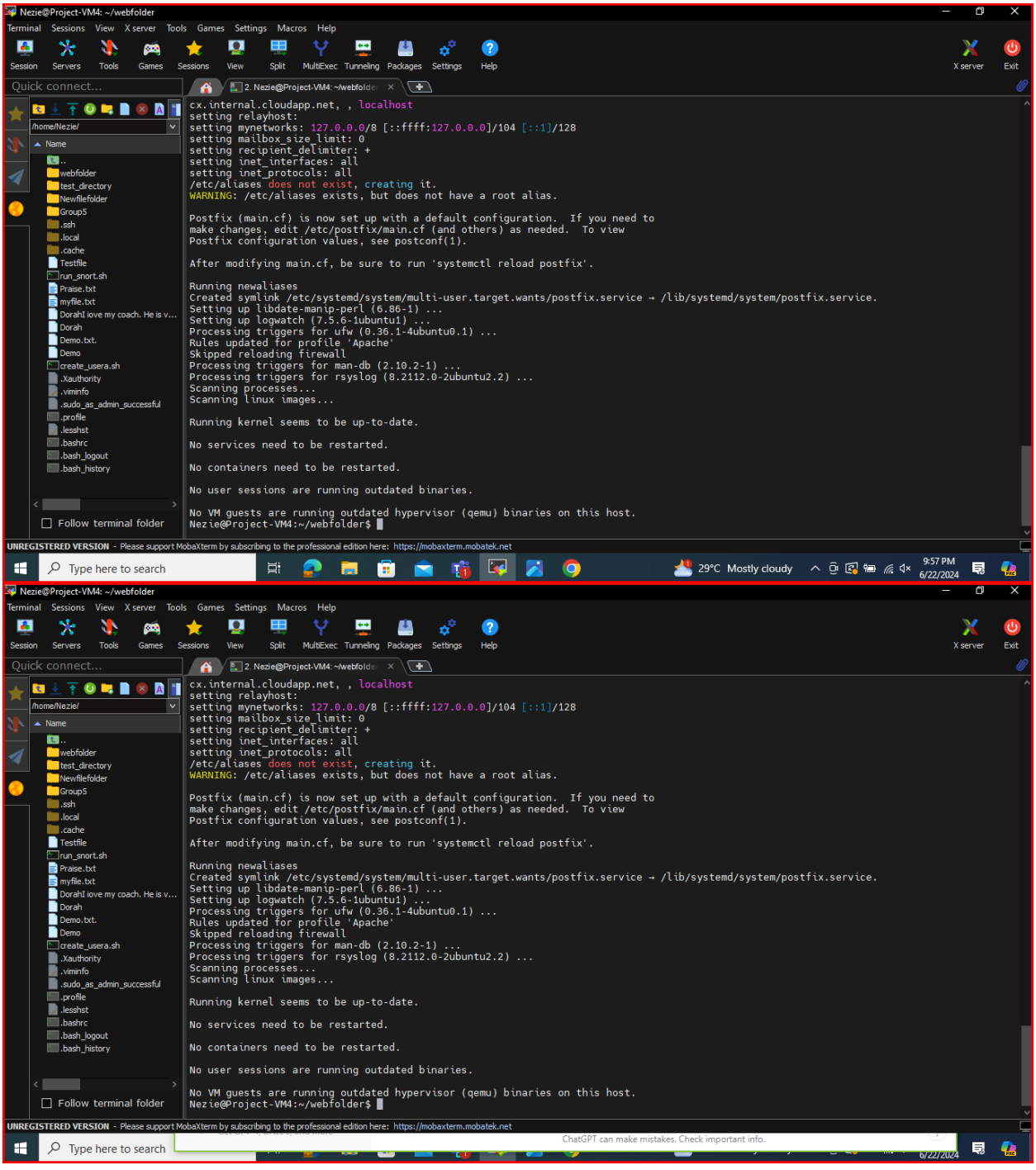


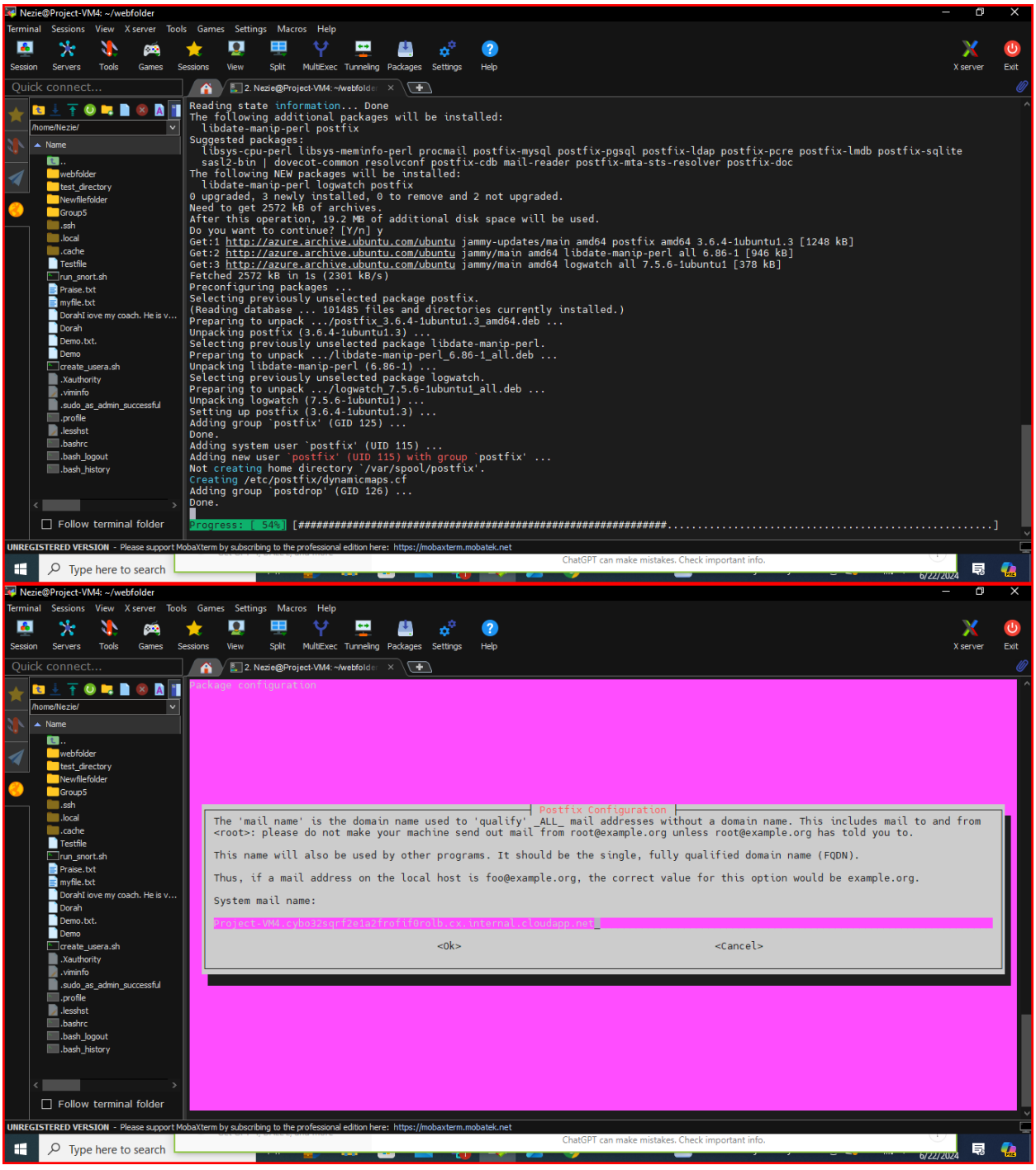


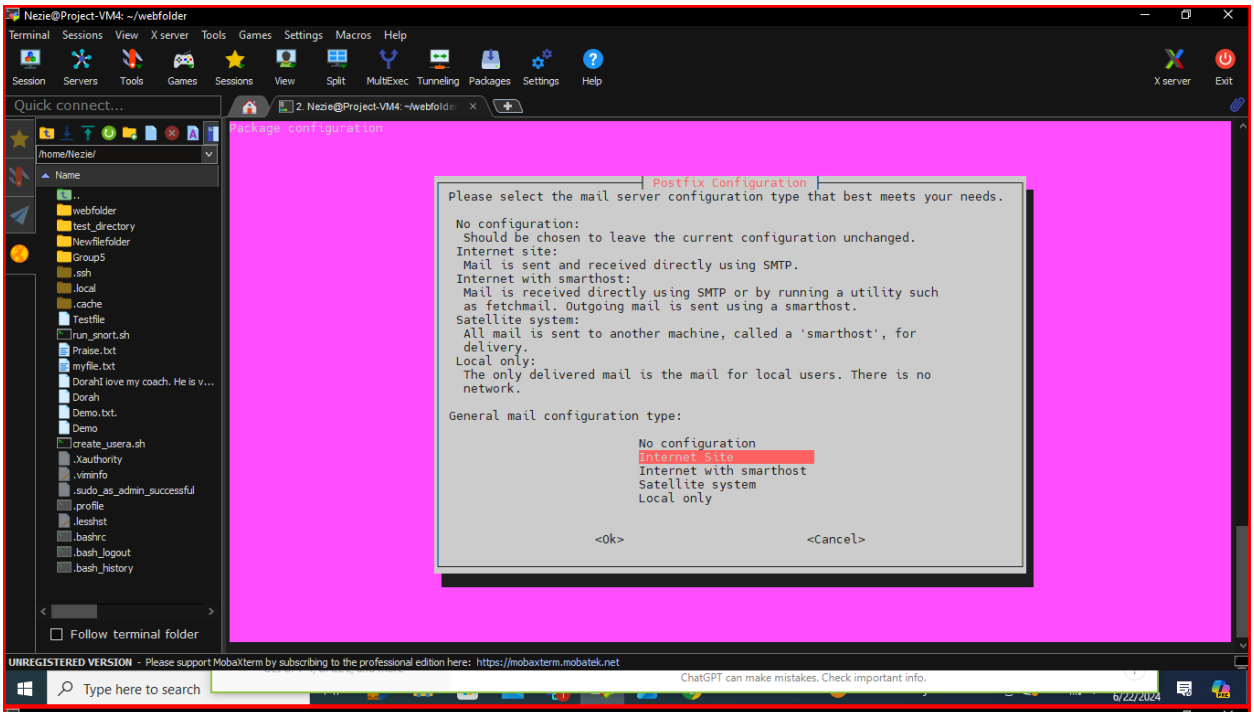
4. Log Management and Monitoring:

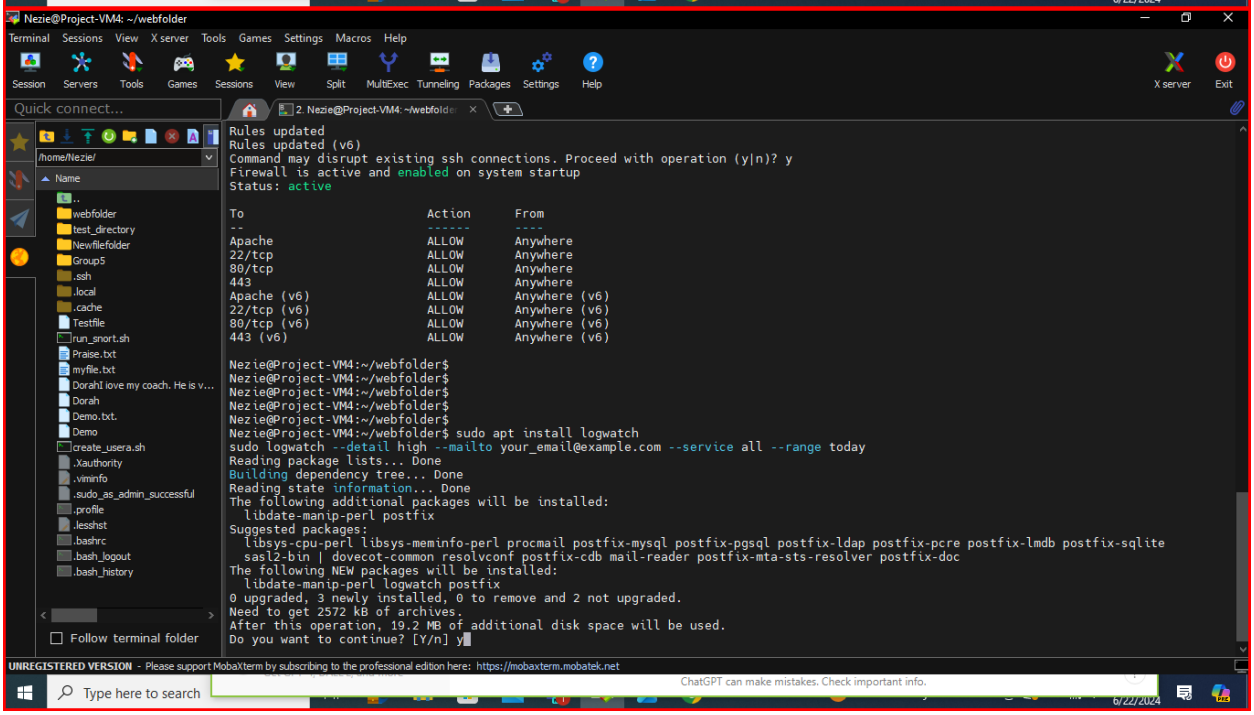
- **Syslog:** Centralized logging service.
- **Logwatch:** Log analyzer and reporter.
- **ELK Stack (Elasticsearch, Logstash, Kibana):** Powerful log management and analysis suite. Commands used: sudo apt install logwatch

- sudo logwatch --detail high --mailto your_email@example.com --service all --range today




Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
Dorah I love my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Reading state information... Done
The following additional packages will be installed:
libdate-manip-perl postfix
Suggested packages:
libsys-cpu-perl libsys-meminfo-perl procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre postfix-lmdb postfix-sqlite
sasl2-bin | dovecot-common resolvconf postfix-cdb mail-reader postfix-mta-sts-resolver postfix-doc
The following NEW packages will be installed:
libdate-manip-perl logwatch postfix
0 upgraded, 3 newly installed, 0 to remove and 2 not upgraded.
Need to get 2572 kB of archives.
After this operation, 19.2 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://azure.archive.ubuntu.com/ubuntu jammy-updates/main amd64 postfix amd64 3.6.4-1ubuntu1.3 [1248 kB]
Get:2 http://azure.archive.ubuntu.com/ubuntu jammy/main amd64 libdate-manip-perl all 6.86-1 [946 kB]
Get:3 http://azure.archive.ubuntu.com/ubuntu jammy/main amd64 logwatch all 7.5.6-1ubuntu1 [378 kB]
Fetched 2572 kB in 1s (2301 kB/s)
Preconfiguring packages ...
Selecting previously unselected package postfix.
(Reading database ... 101485 files and directories currently installed.)
Preparing to unpack .../postfix_3.6.4-1ubuntu1.3_amd64.deb ...
Unpacking postfix (3.6.4-1ubuntu1.3) ...
Selecting previously unselected package libdate-manip-perl.
Preparing to unpack .../libdate-manip-perl_6.86-1_all.deb ...
Unpacking libdate-manip-perl (6.86-1) ...
Selecting previously unselected package logwatch.
Preparing to unpack .../logwatch_7.5.6-1ubuntu1_all.deb ...
Unpacking logwatch (7.5.6-1ubuntu1) ...
Setting up postfix (3.6.4-1ubuntu1.3) ...
Adding group `postfix' (GID 125) ...
Done.
Adding system user `postfix' (UID 115) ...
Adding new user `postfix' (UID 115) with group `postfix' ...
Not creating home directory `/var/spool/postfix'.
Creating /etc/postfix/dynamicmaps.cf
Adding group `postdrop' (GID 126) ...
Done.
Progress: [54%] [##.....]
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
ChatGPT can make mistakes. Check important info.
6/22/2024
Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
Dorah I love my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Package configuration
Postfix Configuration
The 'mail name' is the domain name used to 'qualify' _ALL_ mail addresses without a domain name. This includes mail to and from
<root>: please do not make your machine send out mail from root@example.org unless root@example.org has told you to.
This name will also be used by other programs. It should be the single, fully qualified domain name (FQDN).
Thus, if a mail address on the local host is foo@example.org, the correct value for this option would be example.org.
System mail name:
Project-VM4.cybo32sqrf2e1a2frofif0rolb.cx.internal.cloudapp.net
<Ok>
<Cancel>
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
ChatGPT can make mistakes. Check important info.
6/22/2024





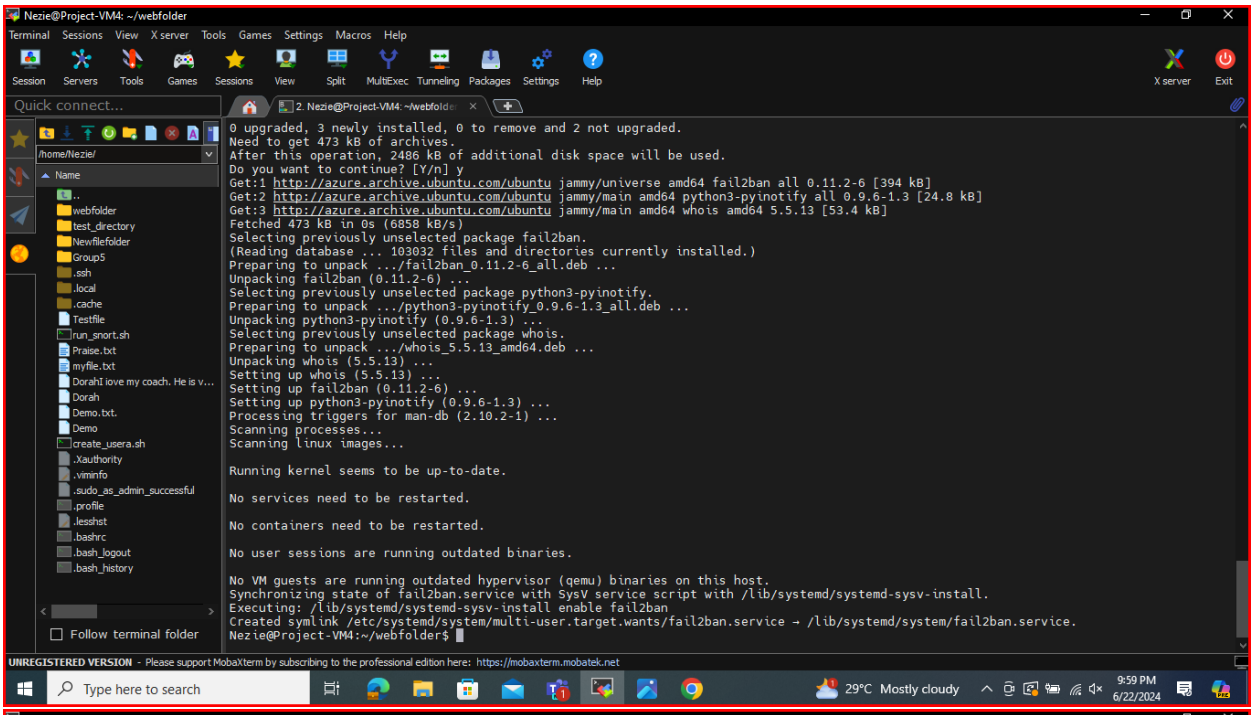
5. Install and Configure Fail2ban: Protect against brute-force attacks.

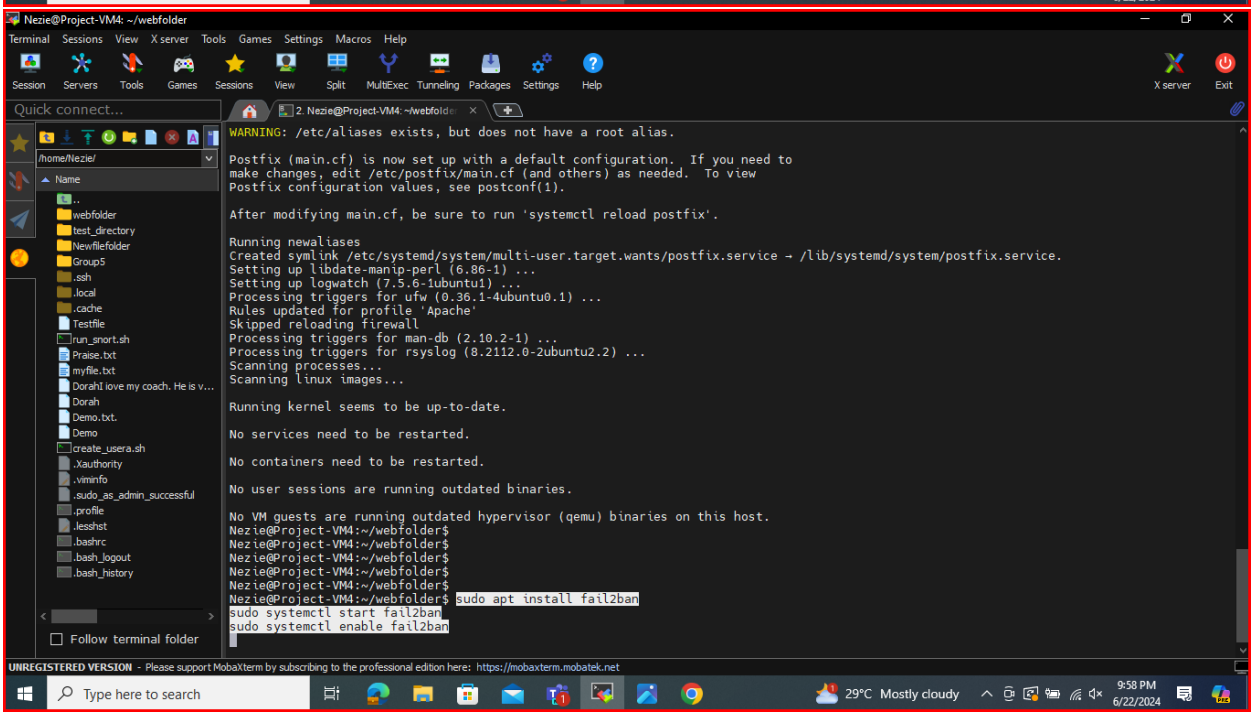
Commands used:

sudo apt install fail2ban

sudo systemctl start fail2ban

sudo systemctl enable fail2ban





6 Security Enhancements:

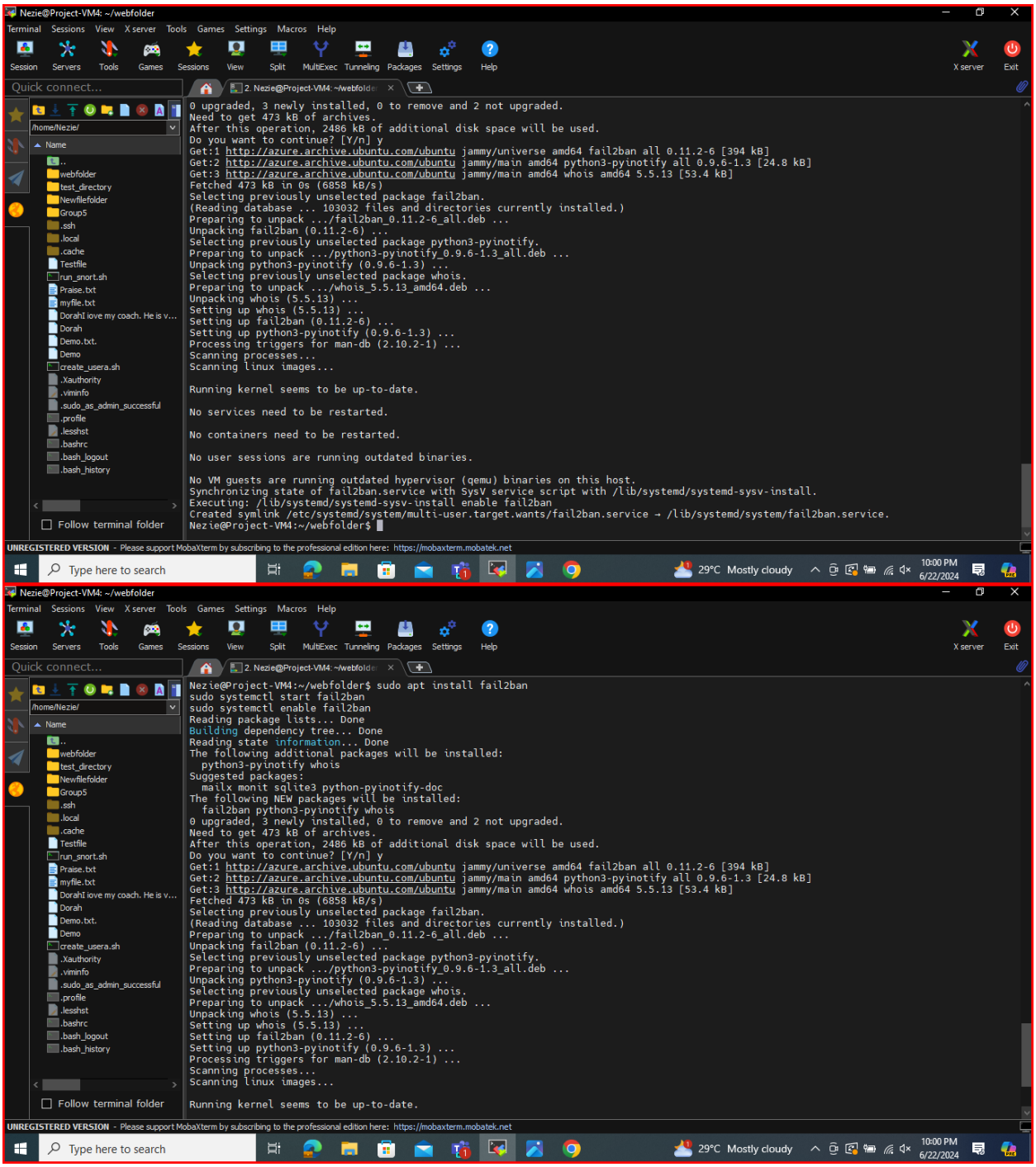
- **AppArmor/SELinux:** Mandatory access control frameworks.
- **ClamAV:** Antivirus for Linux.

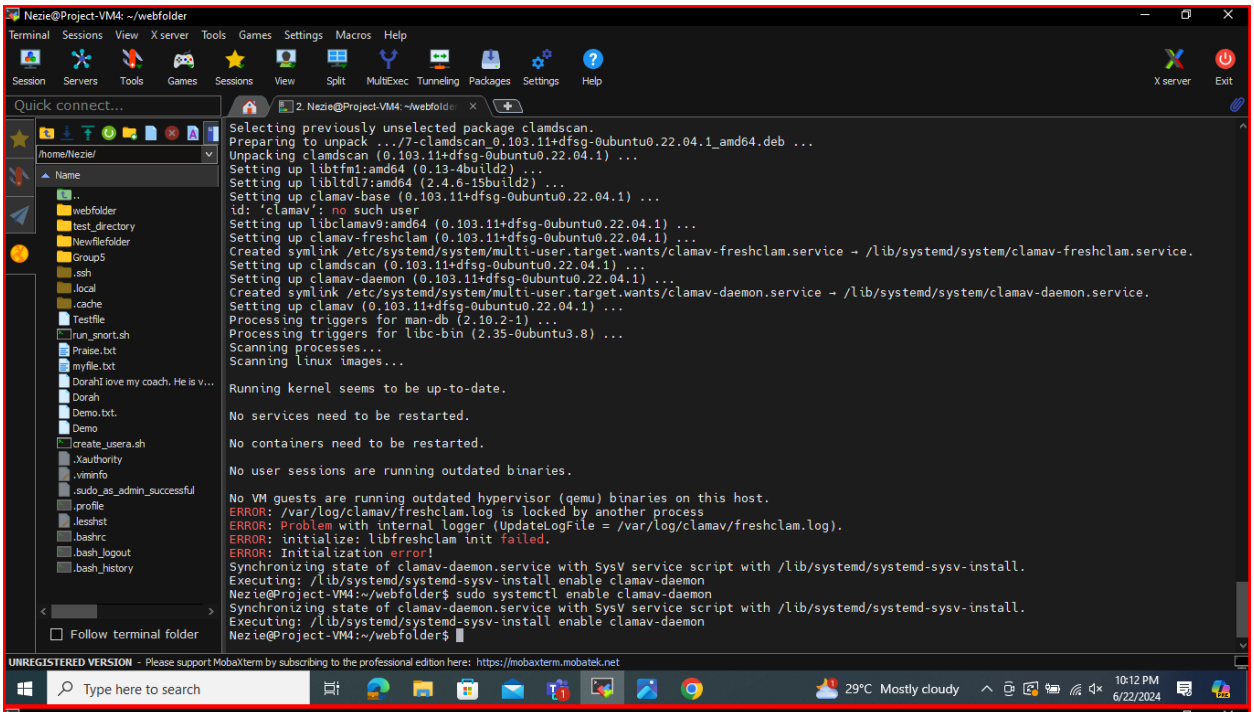
Commands: sudo apt install clamav clamav-daemon

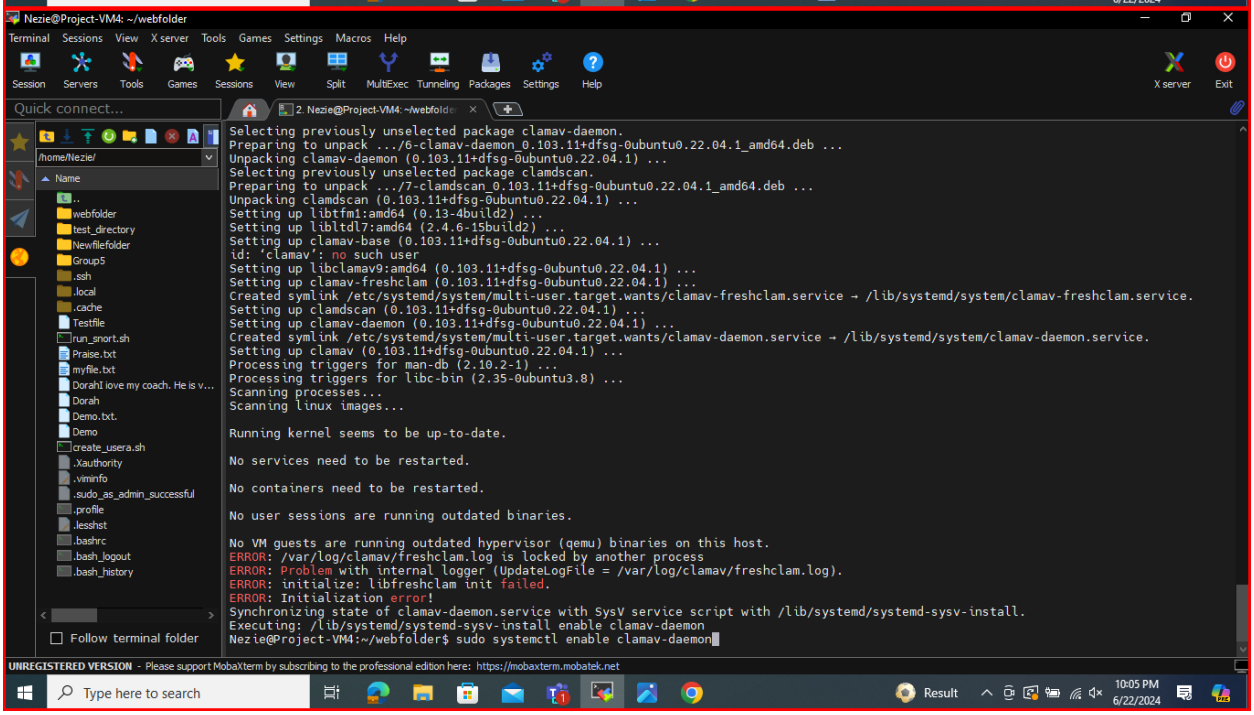
sudo freshclam

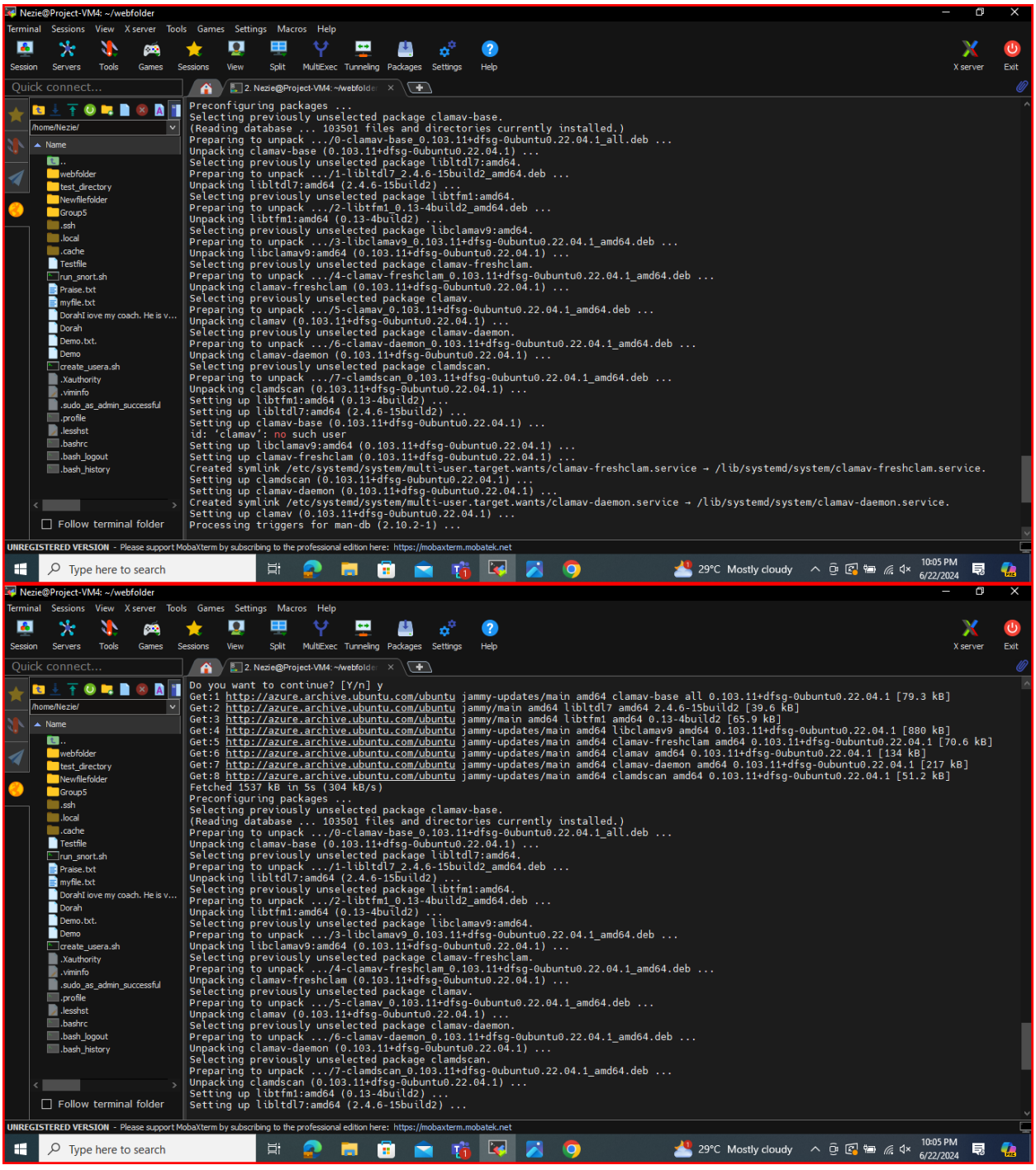
sudo systemctl start clamav-daemon

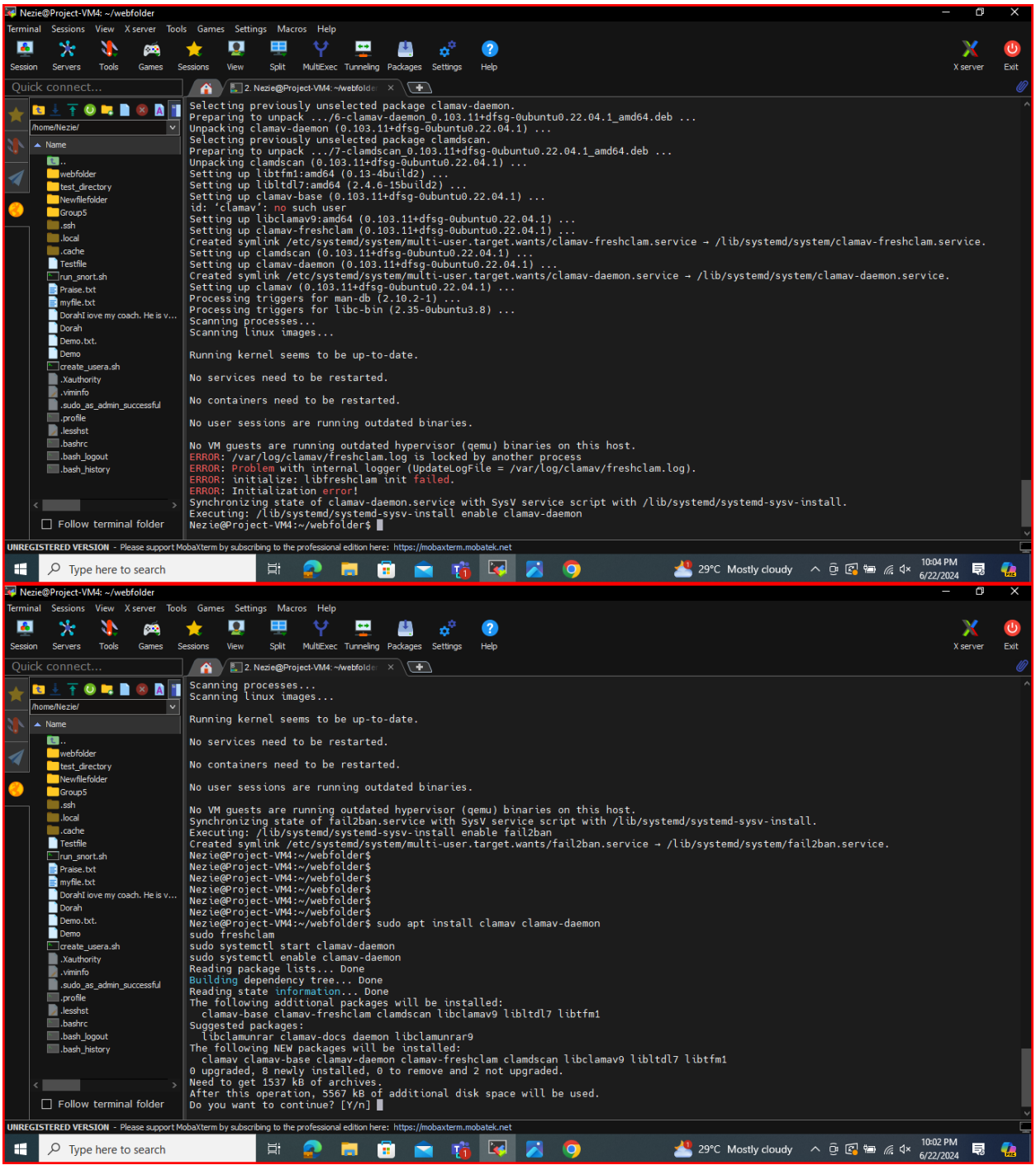
sudo systemctl enable clamav-daemon

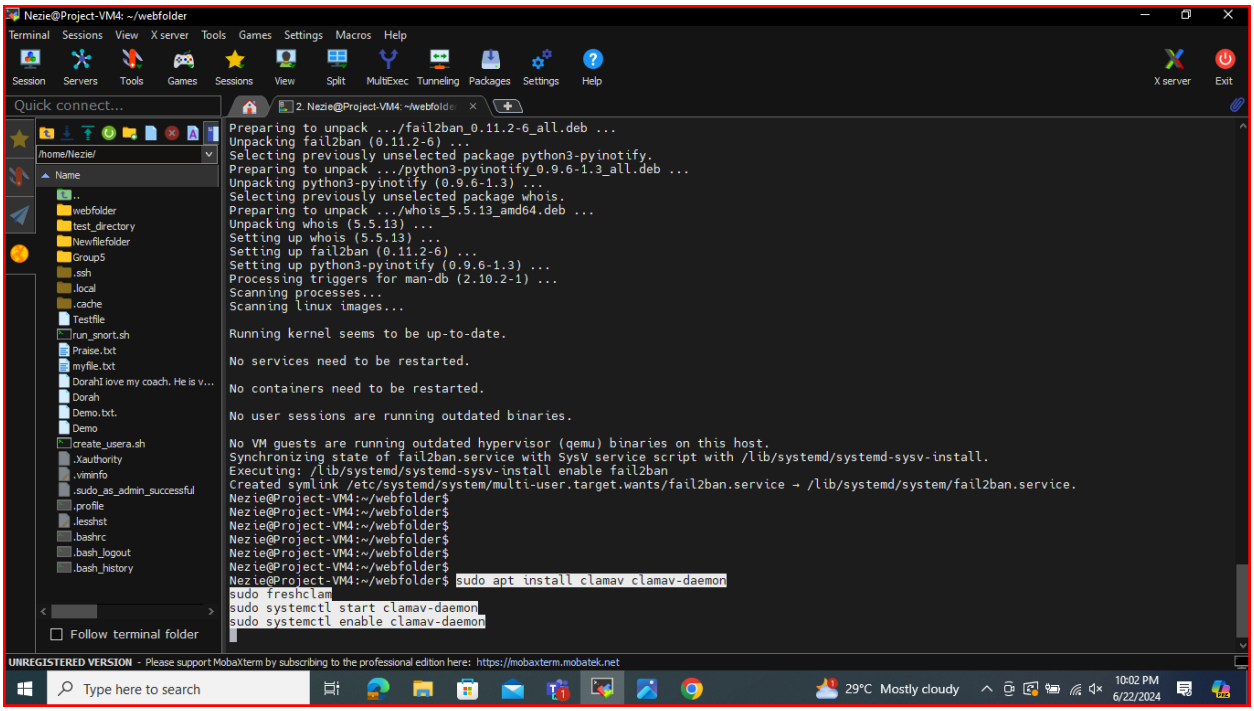



Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
Dorah I love my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Selecting previously unselected package clamdscan.
Preparing to unpack .../7-clamdscan_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamdscan (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Setting up libtfm1:amd64 (0.13-4build2) ...
Setting up libltdl7:amd64 (2.4.6-15build2) ...
Setting up clamav-base (0.103.11+dfsg-0ubuntu0.22.04.1) ...
id: 'clamav': no such user
Setting up libclamav9:amd64 (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Setting up clamav-freshclam (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/clamav-freshclam.service → /lib/systemd/system/clamav-freshclam.service.
Setting up clamdscan (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Setting up clamav-daemon (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/clamav-daemon.service → /lib/systemd/system/clamav-daemon.service.
Setting up clamav (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.8) ...
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.
ERROR: /var/log/clamav/freshclam.log is locked by another process
ERROR: Problem with internal logger (UpdateLogFile = /var/log/clamav/freshclam.log).
ERROR: initialize: libfreshclam init failed.
ERROR: Initialization error!
Synchronizing state of clamav-daemon.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable clamav-daemon
Nezie@Project-VM4:~/webfolder$ sudo systemctl enable clamav-daemon
Synchronizing state of clamav-daemon.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable clamav-daemon
Nezie@Project-VM4:~/webfolder$
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
29°C Mostly cloudy
10:12 PM
6/22/2024

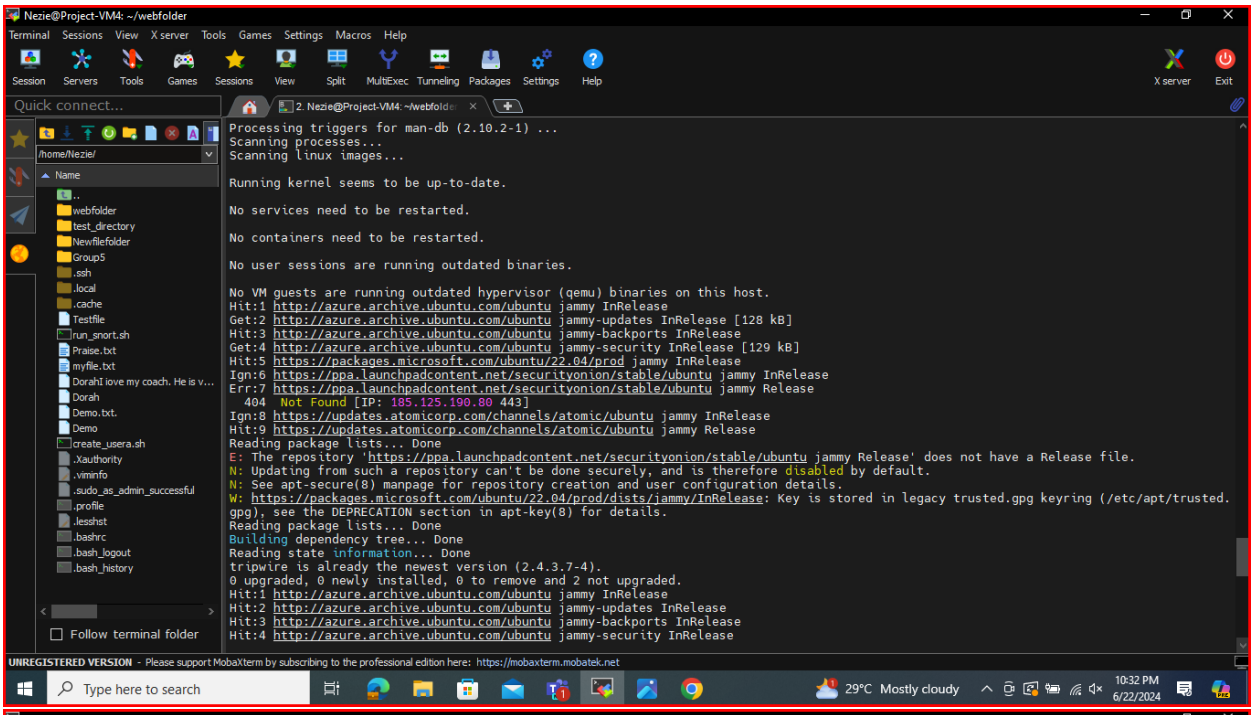

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
Dorah I love my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Selecting previously unselected package clamav-daemon.
Preparing to unpack .../6-clamav-daemon_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamav-daemon (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package clamdscan.
Preparing to unpack .../7-clamdscan_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamdscan (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Setting up libtfm1:amd64 (0.13-4build2) ...
Setting up libltdl7:amd64 (2.4.6-15build2) ...
Setting up clamav-base (0.103.11+dfsg-0ubuntu0.22.04.1) ...
id: 'clamav': no such user
Setting up libclamav9:amd64 (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Setting up clamav-freshclam (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/clamav-freshclam.service → /lib/systemd/system/clamav-freshclam.service.
Setting up clamdscan (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Setting up clamav-daemon (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/clamav-daemon.service → /lib/systemd/system/clamav-daemon.service.
Setting up clamav (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.8) ...
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.
ERROR: /var/log/clamav/freshclam.log is locked by another process
ERROR: Problem with internal logger (UpdateLogFile = /var/log/clamav/freshclam.log).
ERROR: initialize: libfreshclam init failed.
ERROR: Initialization error!
Synchronizing state of clamav-daemon.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable clamav-daemon
Nezie@Project-VM4:~/webfolder$ sudo systemctl enable clamav-daemon
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
Result
10:05 PM
6/22/2024

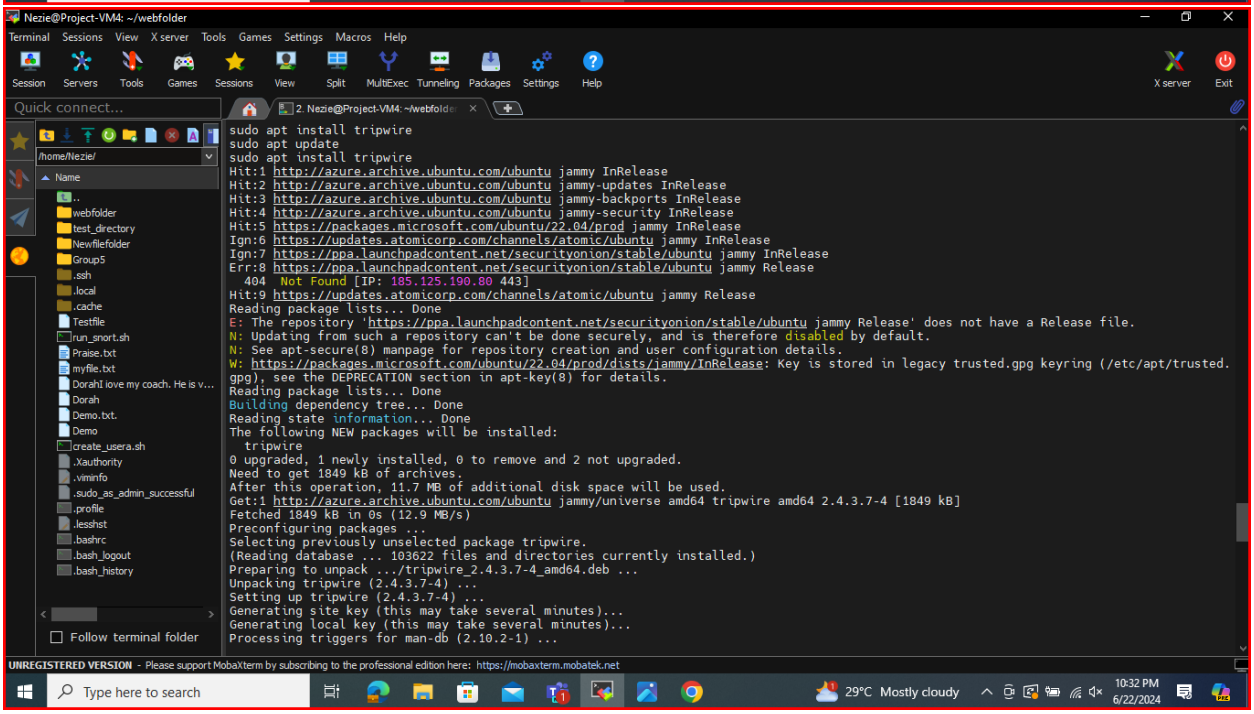

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
Dorah I love my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Preconfiguring packages ...
Selecting previously unselected package clamav-base.
(Reading database ... 103501 files and directories currently installed.)
Preparing to unpack .../0-clamav-base_0.103.11+dfsg-0ubuntu0.22.04.1_all.deb ...
Unpacking clamav-base (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package libltdl7:amd64.
Preparing to unpack .../1-libltdl7_2.4.6-15build2_amd64.deb ...
Unpacking libltdl7:amd64 (2.4.6-15build2) ...
Selecting previously unselected package libtfm1:amd64.
Preparing to unpack .../2-libtfm1_0.13-4build2_amd64.deb ...
Unpacking libtfm1:amd64 (0.13-4build2) ...
Selecting previously unselected package libclamav9:amd64.
Preparing to unpack .../3-libclamav9_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking libclamav9:amd64 (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package clamav-freshclam.
Preparing to unpack .../4-clamav-freshclam_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamav-freshclam (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package clamav.
Preparing to unpack .../5-clamav_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamav (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package clamav-daemon.
Preparing to unpack .../6-clamav-daemon_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamav-daemon (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package clamdscan.
Preparing to unpack .../7-clamdscan_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamdscan (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Setting up libtfm1:amd64 (0.13-4build2) ...
Setting up libltdl7:amd64 (2.4.6-15build2) ...
Setting up clamav-base (0.103.11+dfsg-0ubuntu0.22.04.1) ...
id: 'clamav': no such user
Setting up libclamav9:amd64 (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Setting up clamav-freshclam (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/clamav-freshclam.service → /lib/systemd/system/clamav-freshclam.service.
Setting up clamdscan (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Setting up clamav-daemon (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/clamav-daemon.service → /lib/systemd/system/clamav-daemon.service.
Setting up clamav (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Processing triggers for man-db (2.10.2-1) ...
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
29°C Mostly cloudy
10:05 PM
6/22/2024
Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
Dorah I love my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Do you want to continue? [Y/n] y
Get:1 http://azure.archive.ubuntu.com/ubuntu jammy-updates/main amd64 clamav-base all 0.103.11+dfsg-0ubuntu0.22.04.1 [79.3 kB]
Get:2 http://azure.archive.ubuntu.com/ubuntu jammy/main amd64 libltdl7 amd64 2.4.6-15build2 [39.6 kB]
Get:3 http://azure.archive.ubuntu.com/ubuntu jammy/main amd64 libtfm1 amd64 0.13-4build2 [65.9 kB]
Get:4 http://azure.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libclamav9 amd64 0.103.11+dfsg-0ubuntu0.22.04.1 [880 kB]
Get:5 http://azure.archive.ubuntu.com/ubuntu jammy-updates/main amd64 clamav-freshclam amd64 0.103.11+dfsg-0ubuntu0.22.04.1 [70.6 kB]
Get:6 http://azure.archive.ubuntu.com/ubuntu jammy-updates/main amd64 clamav amd64 0.103.11+dfsg-0ubuntu0.22.04.1 [134 kB]
Get:7 http://azure.archive.ubuntu.com/ubuntu jammy-updates/main amd64 clamav-daemon amd64 0.103.11+dfsg-0ubuntu0.22.04.1 [217 kB]
Get:8 http://azure.archive.ubuntu.com/ubuntu jammy-updates/main amd64 clamdscan amd64 0.103.11+dfsg-0ubuntu0.22.04.1 [51.2 kB]
Fetched 1537 kB in 5s (304 kB/s)
Preconfiguring packages ...
Selecting previously unselected package clamav-base.
(Reading database ... 103501 files and directories currently installed.)
Preparing to unpack .../0-clamav-base_0.103.11+dfsg-0ubuntu0.22.04.1_all.deb ...
Unpacking clamav-base (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package libltdl7:amd64.
Preparing to unpack .../1-libltdl7_2.4.6-15build2_amd64.deb ...
Unpacking libltdl7:amd64 (2.4.6-15build2) ...
Selecting previously unselected package libtfm1:amd64.
Preparing to unpack .../2-libtfm1_0.13-4build2_amd64.deb ...
Unpacking libtfm1:amd64 (0.13-4build2) ...
Selecting previously unselected package libclamav9:amd64.
Preparing to unpack .../3-libclamav9_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking libclamav9:amd64 (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package clamav-freshclam.
Preparing to unpack .../4-clamav-freshclam_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamav-freshclam (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package clamav.
Preparing to unpack .../5-clamav_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamav (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package clamav-daemon.
Preparing to unpack .../6-clamav-daemon_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamav-daemon (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package clamdscan.
Preparing to unpack .../7-clamdscan_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamdscan (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Setting up libtfm1:amd64 (0.13-4build2) ...
Setting up libltdl7:amd64 (2.4.6-15build2) ...
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
29°C Mostly cloudy
10:05 PM
6/22/2024

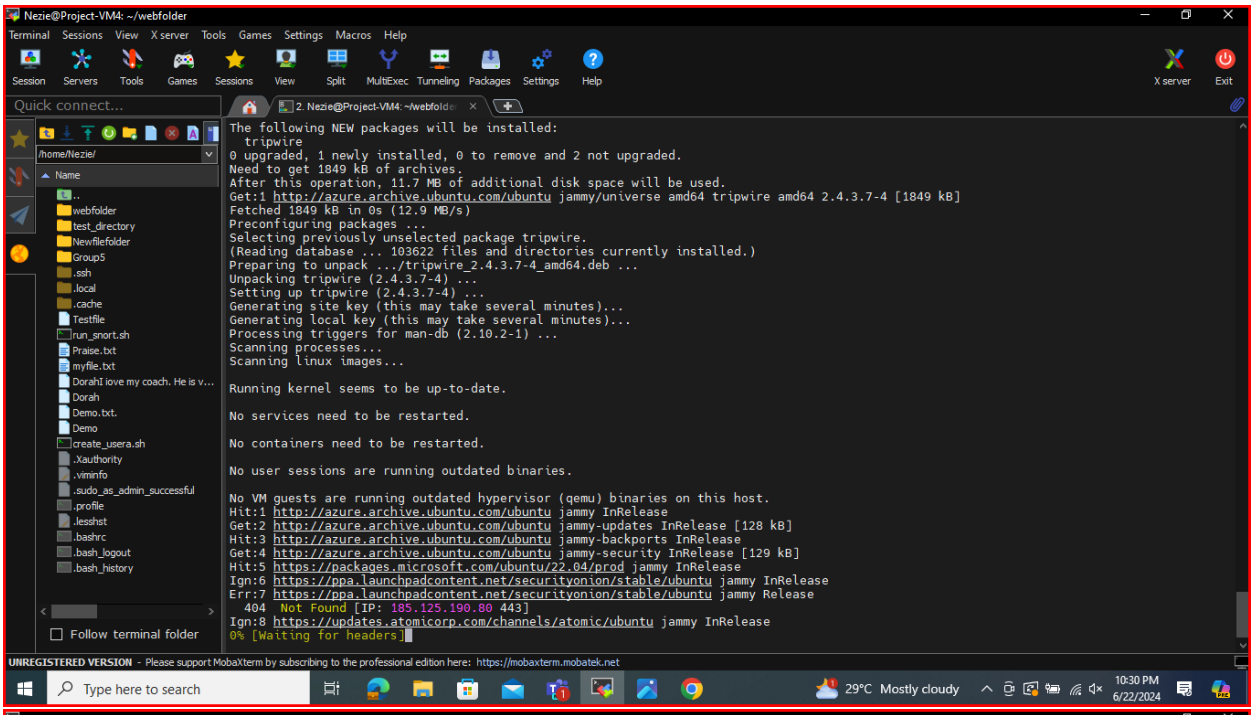

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
..
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
Dorah I love my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Selecting previously unselected package clamav-daemon.
Preparing to unpack .../6-clamav-daemon_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamav-daemon (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package clamdscan.
Preparing to unpack .../7-clamdscan_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamdscan (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Setting up libtfm1:amd64 (0.13-4build2) ...
Setting up libltdl7:amd64 (2.4.6-15build2) ...
Setting up clamav-base (0.103.11+dfsg-0ubuntu0.22.04.1) ...
id: 'clamav': no such user
Setting up libclamav9:amd64 (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Setting up clamav-freshclam (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/clamav-freshclam.service → /lib/systemd/system/clamav-freshclam.service.
Setting up clamdscan (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Setting up clamav-daemon (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/clamav-daemon.service → /lib/systemd/system/clamav-daemon.service.
Setting up clamav (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.8) ...
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.
ERROR: /var/log/clamav/freshclam.log is locked by another process
ERROR: Problem with internal logger (UpdateLogFile = /var/log/clamav/freshclam.log).
ERROR: initialize: libfreshclam init failed.
ERROR: Initialization error!
Synchronizing state of clamav-daemon.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable clamav-daemon
Nezie@Project-VM4:~/webfolder$
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
29°C Mostly cloudy
10:04 PM
6/22/2024
Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
..
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
Dorah I love my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
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.
Synchronizing state of fail2ban.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /lib/systemd/system/fail2ban.service.
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo apt install clamav clamav-daemon
sudo freshclam
sudo systemctl start clamav-daemon
sudo systemctl enable clamav-daemon
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
clamav-base clamav-freshclam clamdscan libclamav9 libltdl7 libtfm1
Suggested packages:
libclamunrar clamav-docs daemon libclamunrar9
The following NEW packages will be installed:
clamav clamav-base clamav-daemon clamav-freshclam clamdscan libclamav9 libltdl7 libtfm1
0 upgraded, 8 newly installed, 0 to remove and 2 not upgraded.
Need to get 1537 kB of archives.
After this operation, 5567 kB of additional disk space will be used.
Do you want to continue? [Y/n]
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
29°C Mostly cloudy
10:02 PM
6/22/2024

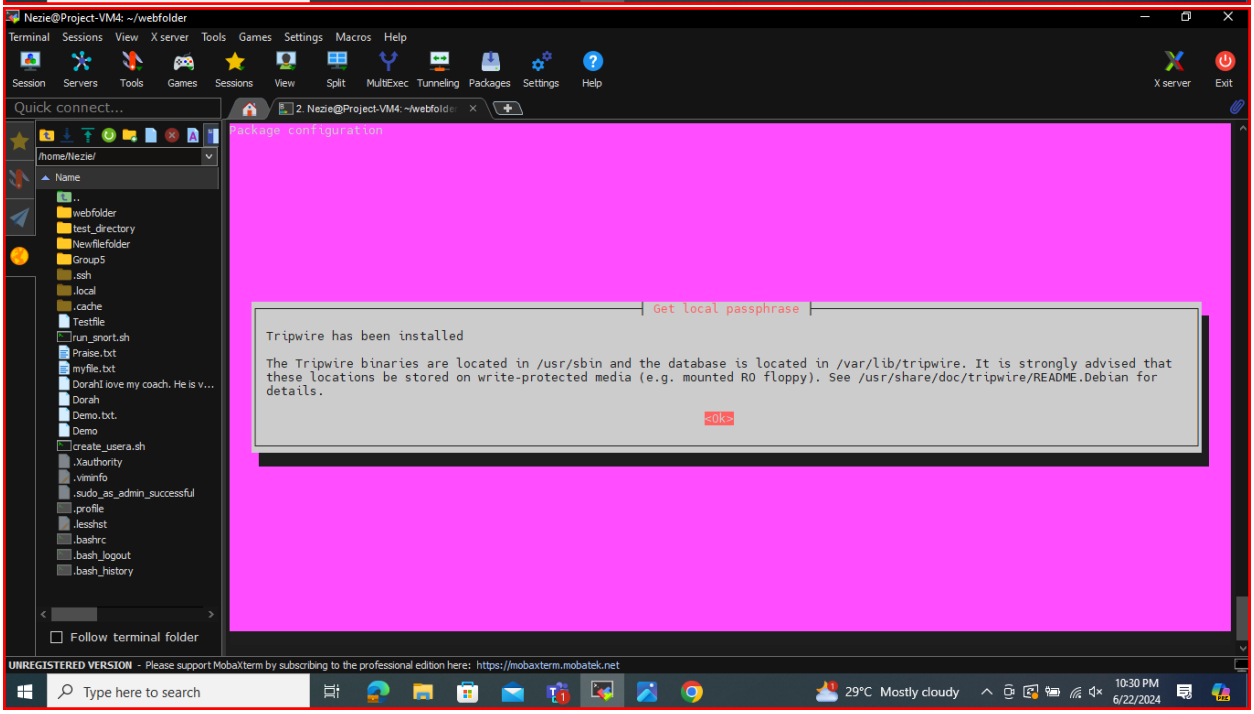


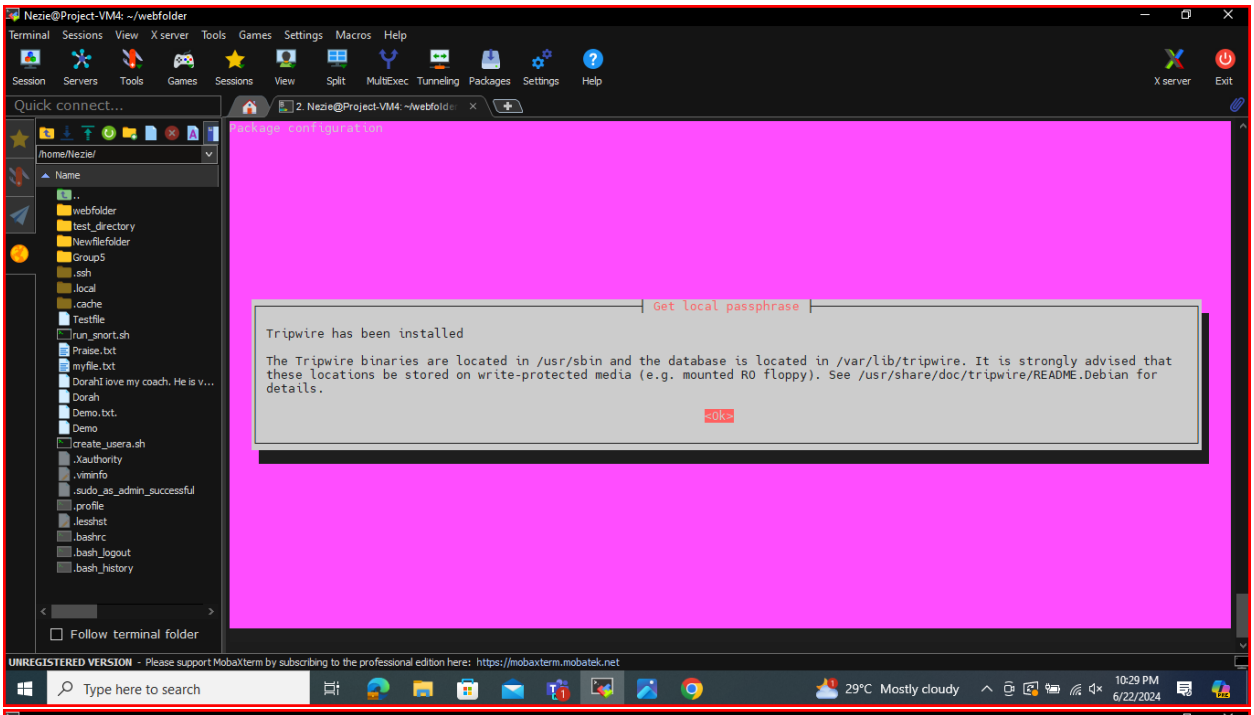
File Integrity Check
Using Tripwire
Commands used: sudo apt update
sudo apt install tripwire

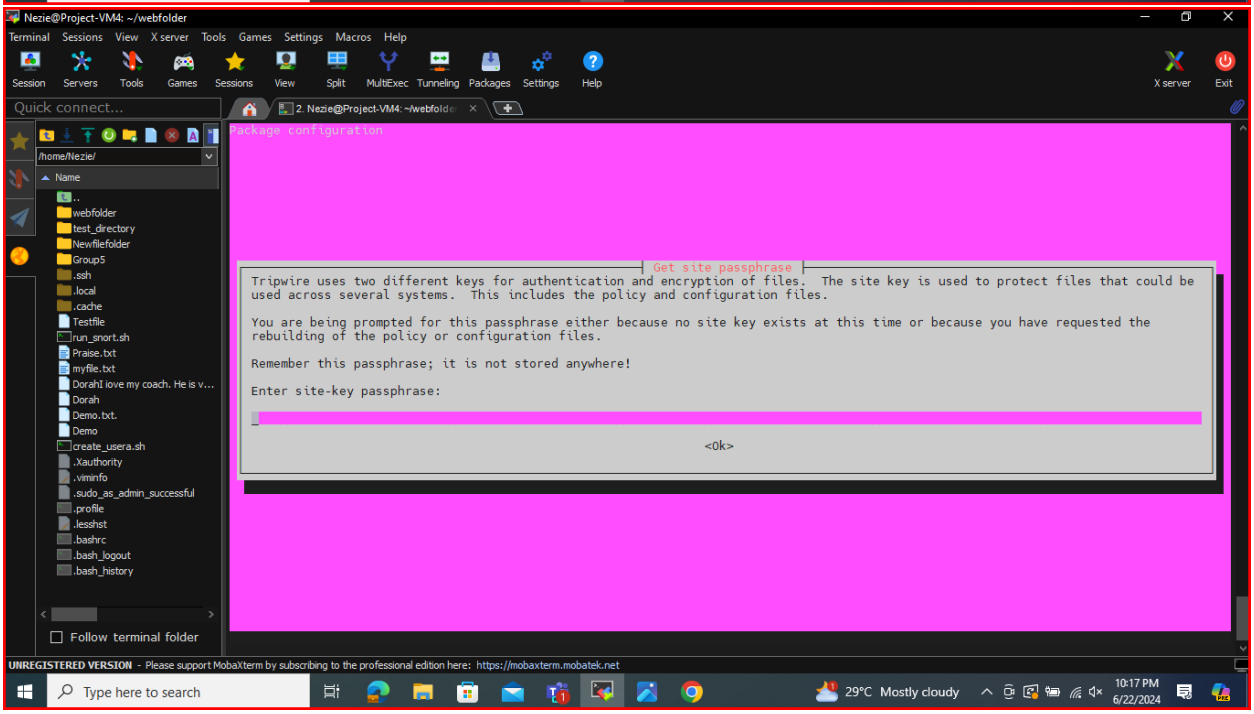

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Processing triggers for man-db (2.10.2-1) ...
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.
Hit:1 http://azure.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://azure.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Hit:3 http://azure.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:4 http://azure.archive.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Hit:5 https://packages.microsoft.com/ubuntu/22.04/prod jammy InRelease
Ign:6 https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy InRelease
Err:7 https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy Release
404 Not Found [IP: 185.125.190.80 443]
Ign:8 https://updates.atomicorp.com/channels/atomic/ubuntu jammy InRelease
Hit:9 https://updates.atomicorp.com/channels/atomic/ubuntu jammy Release
Reading package lists... Done
E: The repository 'https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy Release' does not have a Release file.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
W: https://packages.microsoft.com/ubuntu/22.04/prod/dists/jammy/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
tripwire is already the newest version (2.4.3.7-4).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
Hit:1 http://azure.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://azure.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://azure.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://azure.archive.ubuntu.com/ubuntu jammy-security InRelease
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
29°C Mostly cloudy
10:32 PM
6/22/2024

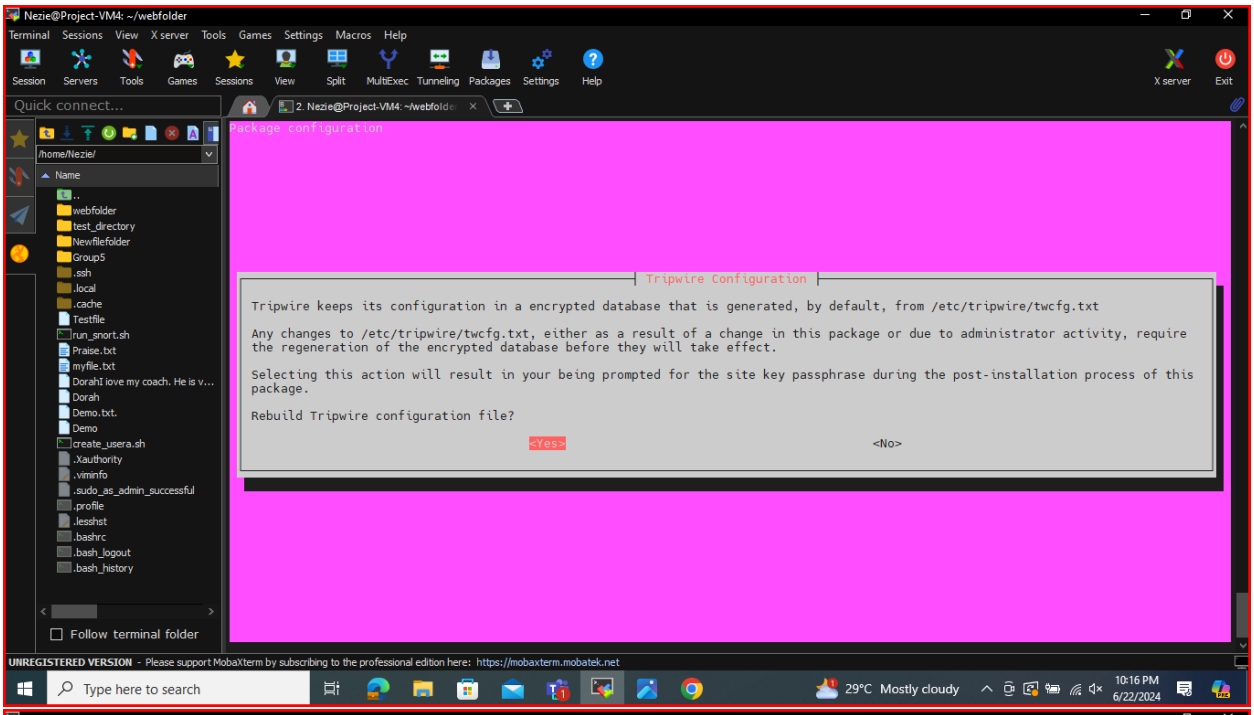

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
sudo apt install tripwire
sudo apt update
sudo apt install tripwire
Hit:1 http://azure.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://azure.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://azure.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://azure.archive.ubuntu.com/ubuntu jammy-security InRelease
Hit:5 https://packages.microsoft.com/ubuntu/22.04/prod jammy InRelease
Ign:6 https://updates.atomicorp.com/channels/atomic/ubuntu jammy InRelease
Ign:7 https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy InRelease
Err:8 https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy Release
404 Not Found [IP: 185.125.190.80 443]
Hit:9 https://updates.atomicorp.com/channels/atomic/ubuntu jammy Release
Reading package lists... Done
E: The repository 'https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy Release' does not have a Release file.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
W: https://packages.microsoft.com/ubuntu/22.04/prod/dists/jammy/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
tripwire
0 upgraded, 1 newly installed, 0 to remove and 2 not upgraded.
Need to get 1849 kB of archives.
After this operation, 11.7 MB of additional disk space will be used.
Get:1 http://azure.archive.ubuntu.com/ubuntu jammy/universe amd64 tripwire amd64 2.4.3.7-4 [1849 kB]
Fetched 1849 kB in 0s (12.9 MB/s)
Preconfiguring packages ...
Selecting previously unselected package tripwire.
(Reading database ... 103622 files and directories currently installed.)
Preparing to unpack .../tripwire_2.4.3.7-4_amd64.deb ...
Unpacking tripwire (2.4.3.7-4) ...
Setting up tripwire (2.4.3.7-4) ...
Generating site key (this may take several minutes)...
Generating local key (this may take several minutes)...
Processing triggers for man-db (2.10.2-1) ...
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
29°C Mostly cloudy
10:32 PM
6/22/2024

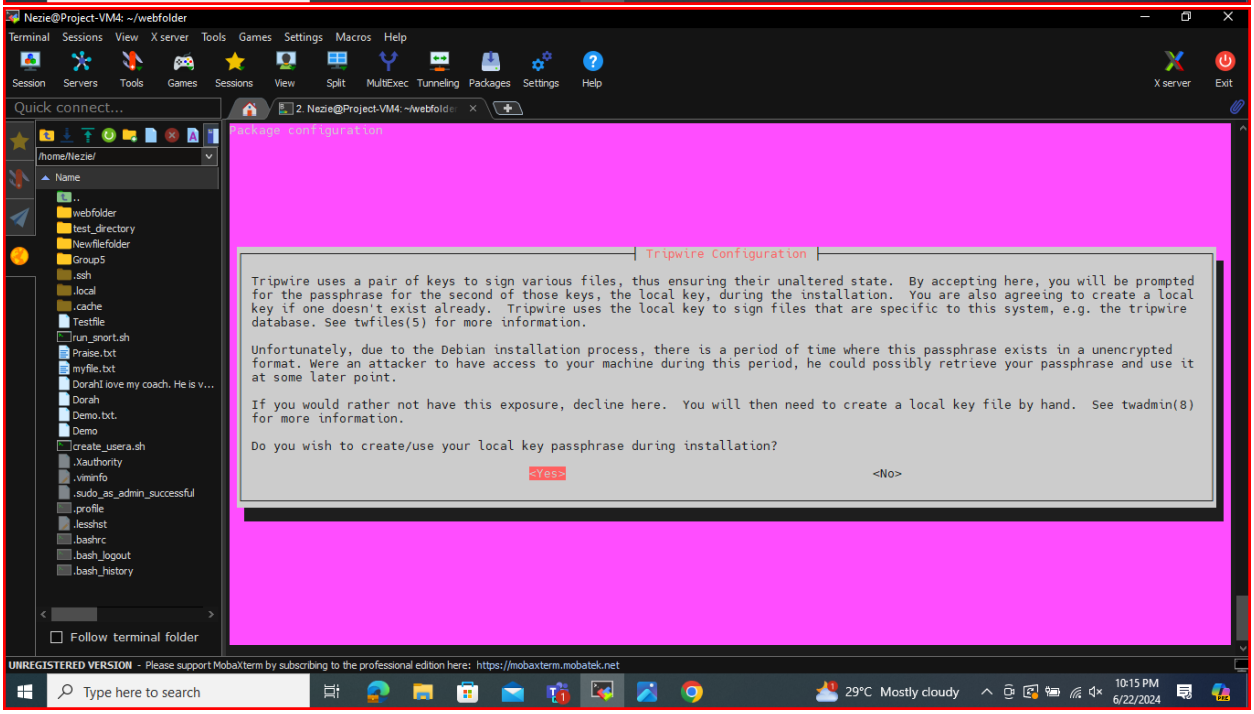

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
The following NEW packages will be installed:
tripwire
0 upgraded, 1 newly installed, 0 to remove and 2 not upgraded.
Need to get 1849 kB of archives.
After this operation, 11.7 MB of additional disk space will be used.
Get:1 http://azure.archive.ubuntu.com/ubuntu jammy/universe amd64 tripwire amd64 2.4.3.7-4 [1849 kB]
Fetched 1849 kB in 0s (12.9 MB/s)
Preconfiguring packages ...
Selecting previously unselected package tripwire.
(Reading database ... 103622 files and directories currently installed.)
Preparing to unpack .../tripwire_2.4.3.7-4_amd64.deb ...
Unpacking tripwire (2.4.3.7-4) ...
Setting up tripwire (2.4.3.7-4) ...
Generating site key (this may take several minutes)...
Generating local key (this may take several minutes)...
Processing triggers for man-db (2.10.2-1) ...
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.
Hit:1 http://azure.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://azure.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Hit:3 http://azure.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:4 http://azure.archive.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Hit:5 https://packages.microsoft.com/ubuntu/22.04/prod jammy InRelease
Ign:6 https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy InRelease
Err:7 https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy Release
404 Not Found [IP: 185.125.190.80 443]
Ign:8 https://updates.atomicorp.com/channels/atomic/ubuntu jammy InRelease
0% [Waiting for headers]
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
29°C Mostly cloudy
10:30 PM
6/22/2024

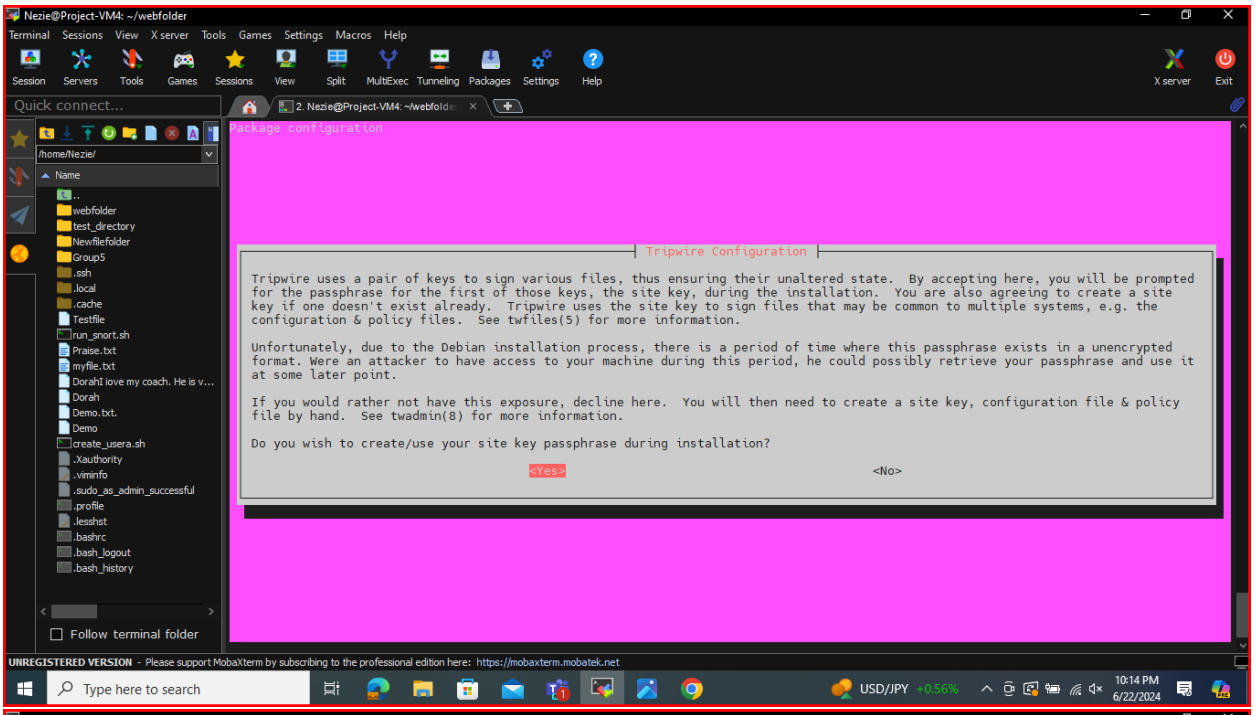

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Package configuration
Get local passphrase
Tripwire has been installed
The Tripwire binaries are located in /usr/sbin and the database is located in /var/lib/tripwire. It is strongly advised that these locations be stored on write-protected media (e.g. mounted RO floppy). See /usr/share/doc/tripwire/README.Debian for details.
<Ok>
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
29°C Mostly cloudy
10:30 PM
6/22/2024

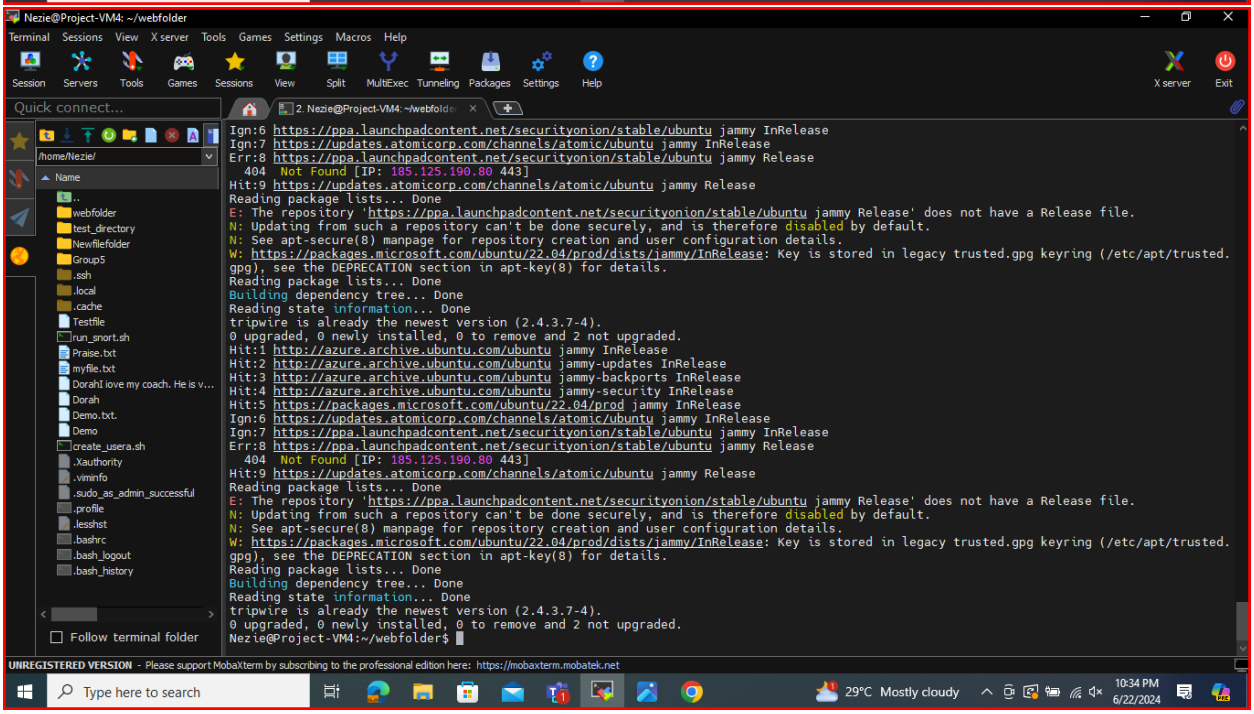

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
Package configuration
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Get local passphrase
Tripwire has been installed
The Tripwire binaries are located in /usr/sbin and the database is located in /var/lib/tripwire. It is strongly advised that these locations be stored on write-protected media (e.g. mounted RO floppy). See /usr/share/doc/tripwire/README.Debian for details.
<Ok>
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
29°C Mostly cloudy
10:29 PM
6/22/2024

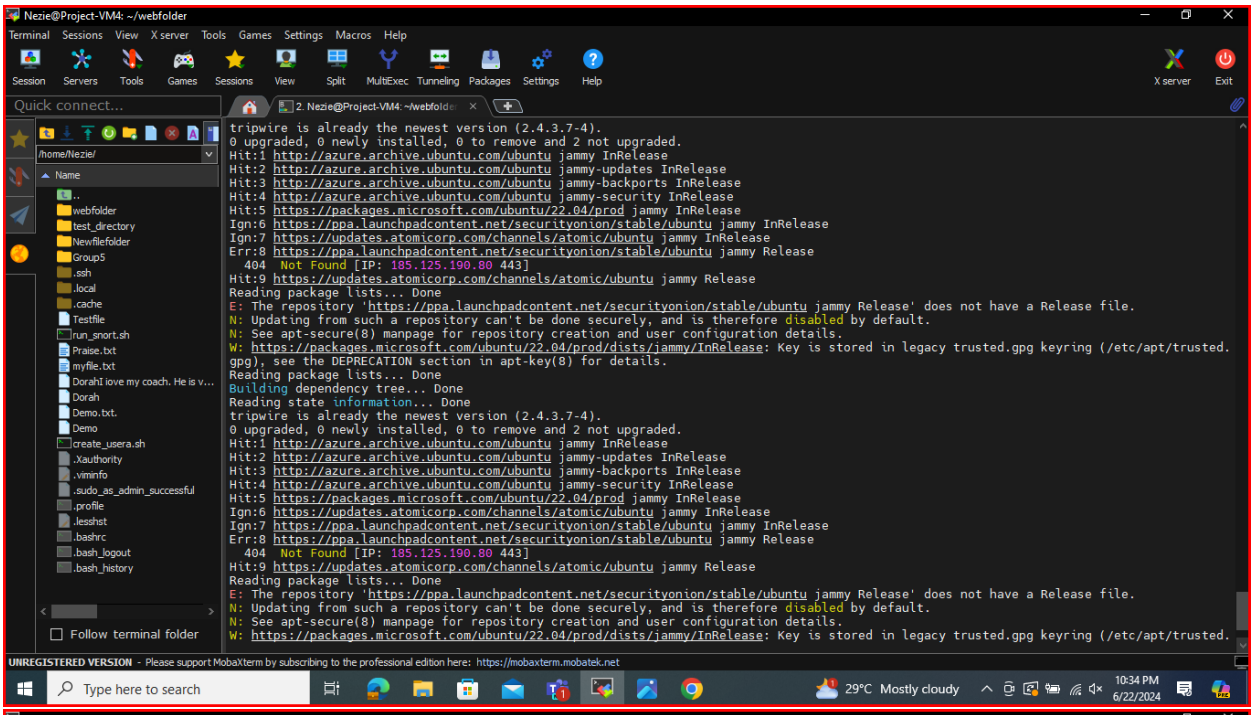

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
Package configuration
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Get site passphrase
Tripwire uses two different keys for authentication and encryption of files. The site key is used to protect files that could be used across several systems. This includes the policy and configuration files.
You are being prompted for this passphrase either because no site key exists at this time or because you have requested the rebuilding of the policy or configuration files.
Remember this passphrase; it is not stored anywhere!
Enter site-key passphrase:
<Ok>
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
29°C Mostly cloudy
10:17 PM
6/22/2024

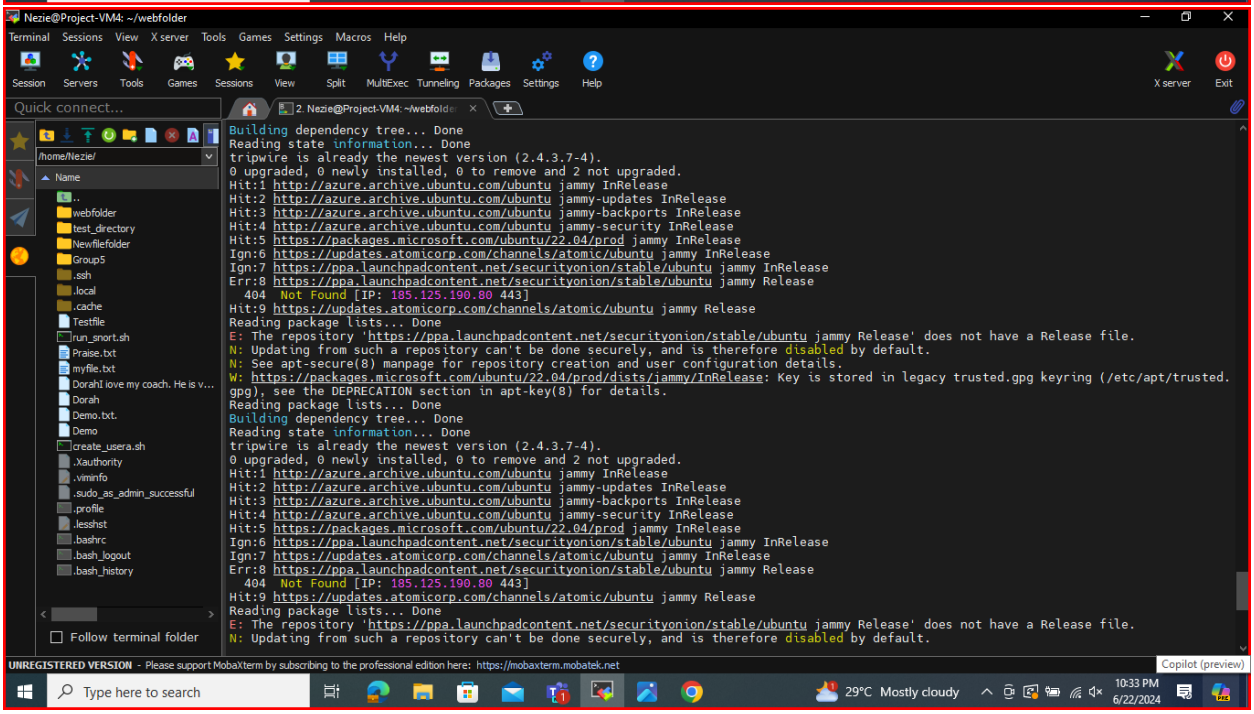

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Package configuration
Tripwire Configuration
Tripwire keeps its configuration in a encrypted database that is generated, by default, from /etc/tripwire/twcfg.txt
Any changes to /etc/tripwire/twcfg.txt, either as a result of a change in this package or due to administrator activity, require the regeneration of the encrypted database before they will take effect.
Selecting this action will result in your being prompted for the site key passphrase during the post-installation process of this package.
Rebuild Tripwire configuration file?
<Yes>
<No>
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
29°C Mostly cloudy
10:16 PM
6/22/2024

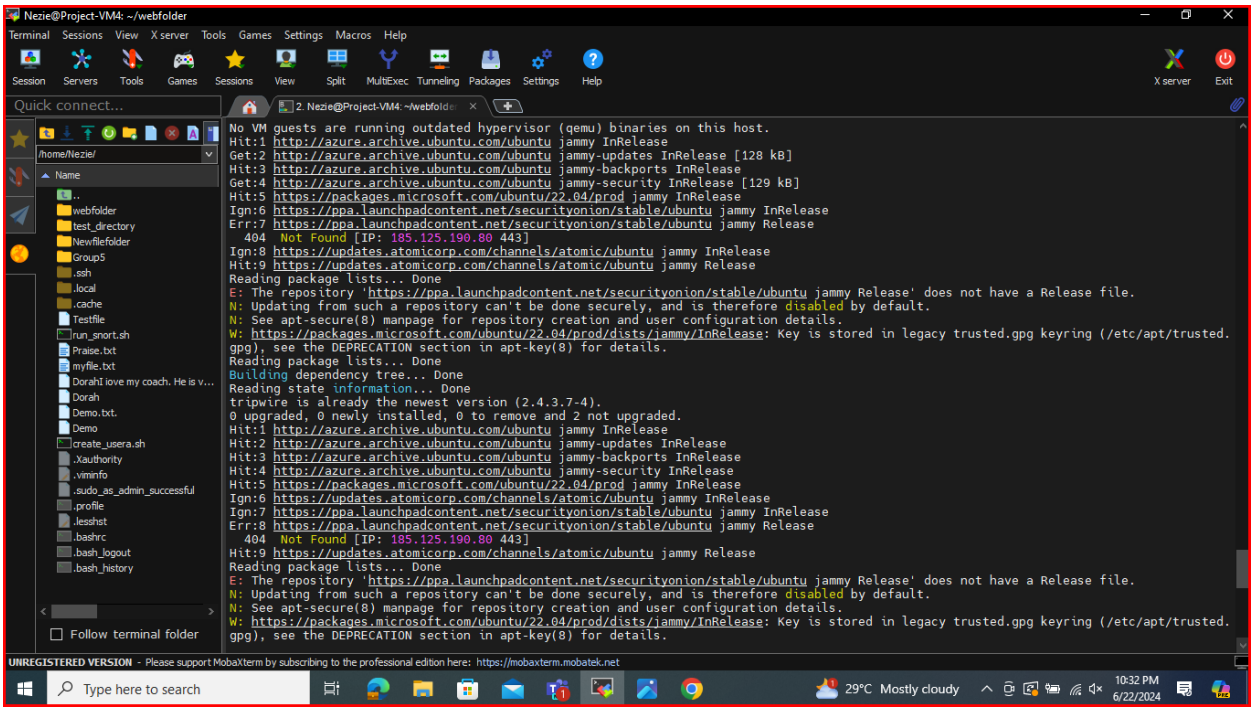

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Package configuration
Tripwire Configuration
Tripwire uses a pair of keys to sign various files, thus ensuring their unaltered state. By accepting here, you will be prompted for the passphrase for the second of those keys, the local key, during the installation. You are also agreeing to create a local key if one doesn't exist already. Tripwire uses the local key to sign files that are specific to this system, e.g. the tripwire database. See twfiles(5) for more information.
Unfortunately, due to the Debian installation process, there is a period of time where this passphrase exists in a unencrypted format. Were an attacker to have access to your machine during this period, he could possibly retrieve your passphrase and use it at some later point.
If you would rather not have this exposure, decline here. You will then need to create a local key file by hand. See twadmin(8) for more information.
Do you wish to create/use your local key passphrase during installation?
<Yes>
<No>
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
29°C Mostly cloudy
10:15 PM
6/22/2024


Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Package configuration
Tripwire Configuration
Tripwire uses a pair of keys to sign various files, thus ensuring their unaltered state. By accepting here, you will be prompted for the passphrase for the first of those keys, the site key, during the installation. You are also agreeing to create a site key if one doesn't exist already. Tripwire uses the site key to sign files that may be common to multiple systems, e.g. the configuration & policy files. See twfiles(5) for more information.
Unfortunately, due to the Debian installation process, there is a period of time where this passphrase exists in a unencrypted format. Were an attacker to have access to your machine during this period, he could possibly retrieve your passphrase and use it at some later point.
If you would rather not have this exposure, decline here. You will then need to create a site key, configuration file & policy file by hand. See twadmin(8) for more information.
Do you wish to create/use your site key passphrase during installation?
<Yes>
<No>
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
USD/JPY +0.56%
10:14 PM
6/22/2024


Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Ign:6 https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy InRelease
Ign:7 https://updates.atomicorp.com/channels/atomic/ubuntu jammy InRelease
Err:8 https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy Release
404 Not Found [IP: 185.125.190.80 443]
Hit:9 https://updates.atomicorp.com/channels/atomic/ubuntu jammy Release
Reading package lists... Done
E: The repository 'https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy Release' does not have a Release file.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
W: https://packages.microsoft.com/ubuntu/22.04/prod/dists/jammy/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
tripwire is already the newest version (2.4.3.7-4).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
Hit:1 http://azure.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://azure.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://azure.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://azure.archive.ubuntu.com/ubuntu jammy-security InRelease
Hit:5 https://packages.microsoft.com/ubuntu/22.04/prod jammy InRelease
Ign:6 https://updates.atomicorp.com/channels/atomic/ubuntu jammy InRelease
Ign:7 https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy InRelease
Err:8 https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy Release
404 Not Found [IP: 185.125.190.80 443]
Hit:9 https://updates.atomicorp.com/channels/atomic/ubuntu jammy Release
Reading package lists... Done
E: The repository 'https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy Release' does not have a Release file.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
W: https://packages.microsoft.com/ubuntu/22.04/prod/dists/jammy/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
tripwire is already the newest version (2.4.3.7-4).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
Nezie@Project-VM4:~/webfolder$
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
29°C Mostly cloudy
10:34 PM
6/22/2024

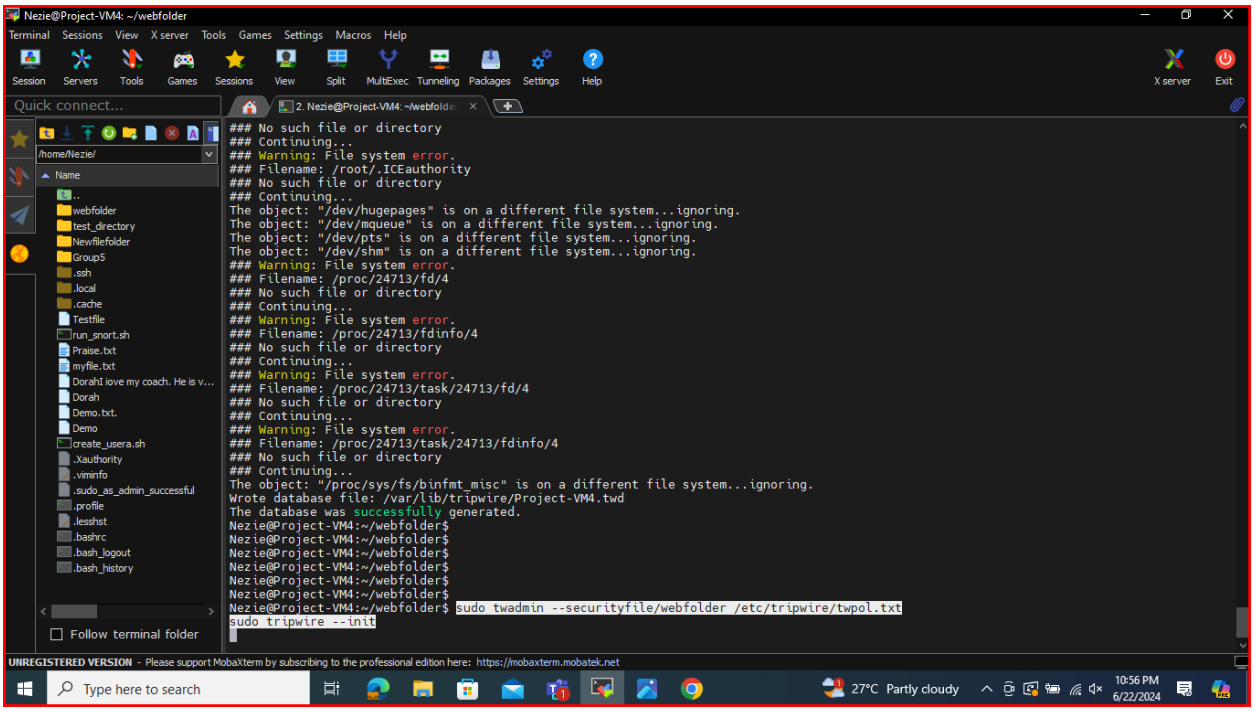

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
tripwire is already the newest version (2.4.3.7-4).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
Hit:1 http://azure.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://azure.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://azure.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://azure.archive.ubuntu.com/ubuntu jammy-security InRelease
Hit:5 https://packages.microsoft.com/ubuntu/22.04/prod jammy InRelease
Ign:6 https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy InRelease
Ign:7 https://updates.atomicorp.com/channels/atomic/ubuntu jammy InRelease
Err:8 https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy Release
404 Not Found [IP: 185.125.190.80 443]
Hit:9 https://updates.atomicorp.com/channels/atomic/ubuntu jammy Release
Reading package lists... Done
E: The repository 'https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy Release' does not have a Release file.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
W: https://packages.microsoft.com/ubuntu/22.04/prod/dists/jammy/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
tripwire is already the newest version (2.4.3.7-4).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
Hit:1 http://azure.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://azure.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://azure.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://azure.archive.ubuntu.com/ubuntu jammy-security InRelease
Hit:5 https://packages.microsoft.com/ubuntu/22.04/prod jammy InRelease
Ign:6 https://updates.atomicorp.com/channels/atomic/ubuntu jammy InRelease
Ign:7 https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy InRelease
Err:8 https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy Release
404 Not Found [IP: 185.125.190.80 443]
Hit:9 https://updates.atomicorp.com/channels/atomic/ubuntu jammy Release
Reading package lists... Done
E: The repository 'https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy Release' does not have a Release file.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
W: https://packages.microsoft.com/ubuntu/22.04/prod/dists/jammy/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
29°C Mostly cloudy
10:34 PM
6/22/2024

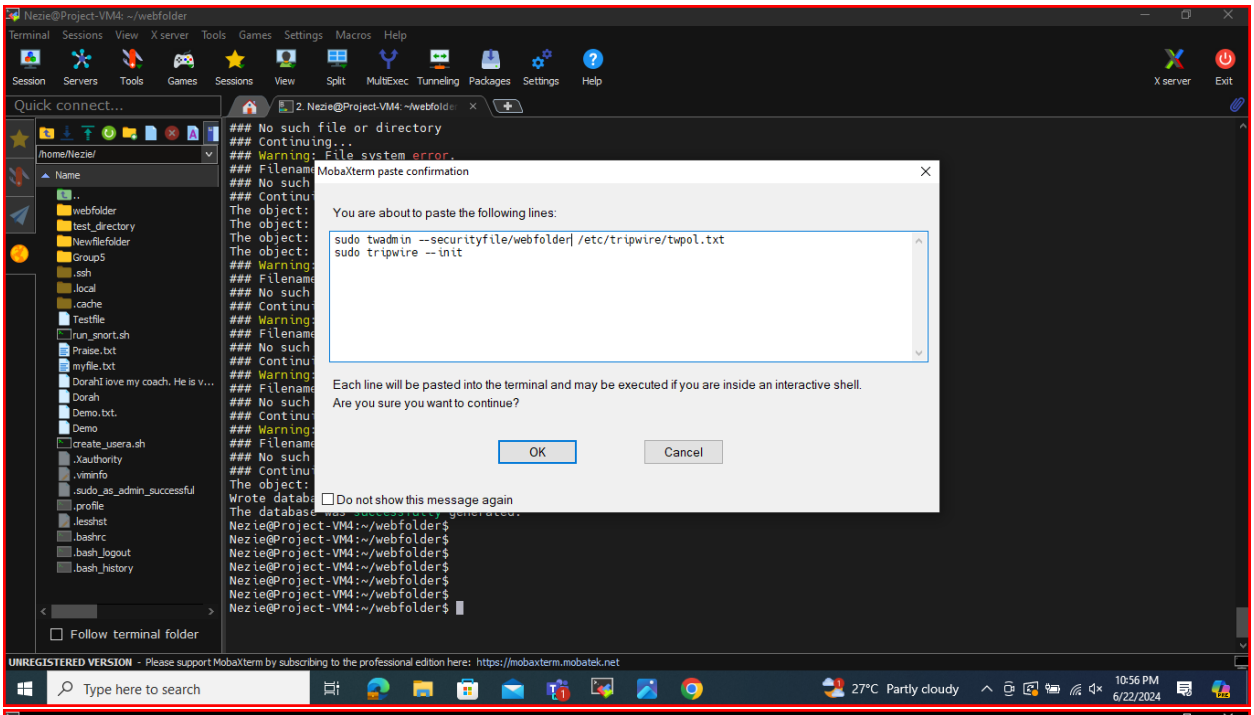

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Building dependency tree... Done
Reading state information... Done
tripwire is already the newest version (2.4.3.7-4).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
Hit:1 http://azure.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://azure.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://azure.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://azure.archive.ubuntu.com/ubuntu jammy-security InRelease
Hit:5 https://packages.microsoft.com/ubuntu/22.04/prod jammy InRelease
Ign:6 https://updates.atomicorp.com/channels/atomic/ubuntu jammy InRelease
Ign:7 https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy InRelease
Err:8 https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy Release
404 Not Found [IP: 185.125.190.80 443]
Hit:9 https://updates.atomicorp.com/channels/atomic/ubuntu jammy Release
Reading package lists... Done
E: The repository 'https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy Release' does not have a Release file.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
W: https://packages.microsoft.com/ubuntu/22.04/prod/dists/jammy/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
tripwire is already the newest version (2.4.3.7-4).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
Hit:1 http://azure.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://azure.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://azure.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://azure.archive.ubuntu.com/ubuntu jammy-security InRelease
Hit:5 https://packages.microsoft.com/ubuntu/22.04/prod jammy InRelease
Ign:6 https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy InRelease
Ign:7 https://updates.atomicorp.com/channels/atomic/ubuntu jammy InRelease
Err:8 https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy Release
404 Not Found [IP: 185.125.190.80 443]
Hit:9 https://updates.atomicorp.com/channels/atomic/ubuntu jammy Release
Reading package lists... Done
E: The repository 'https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy Release' does not have a Release file.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Copilot (preview)
Type here to search
29°C Mostly cloudy
10:33 PM
6/22/2024

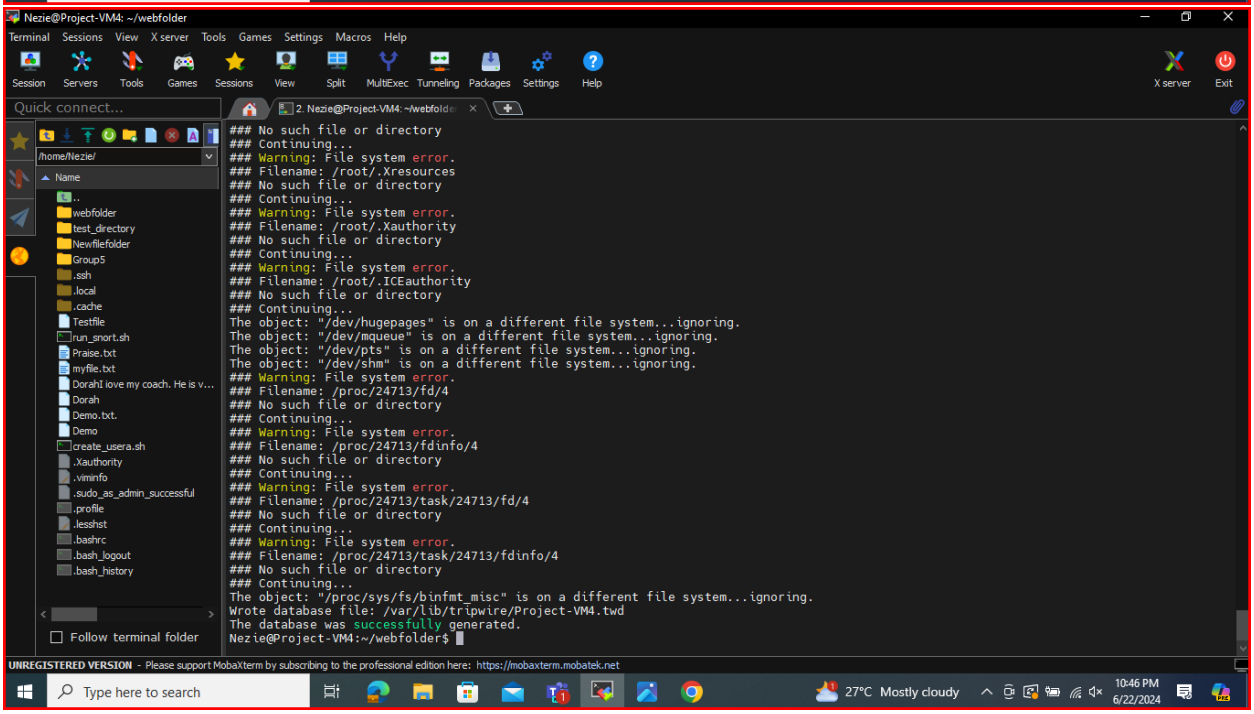


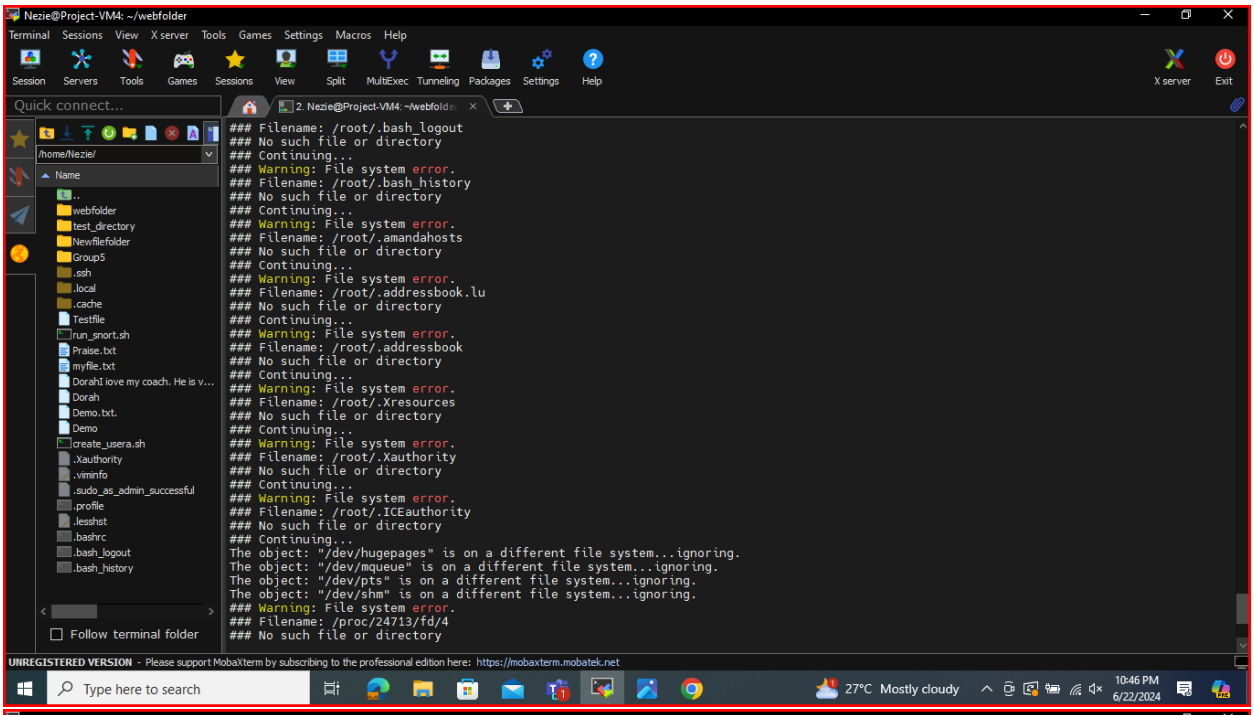
2. Initialize Tripwire

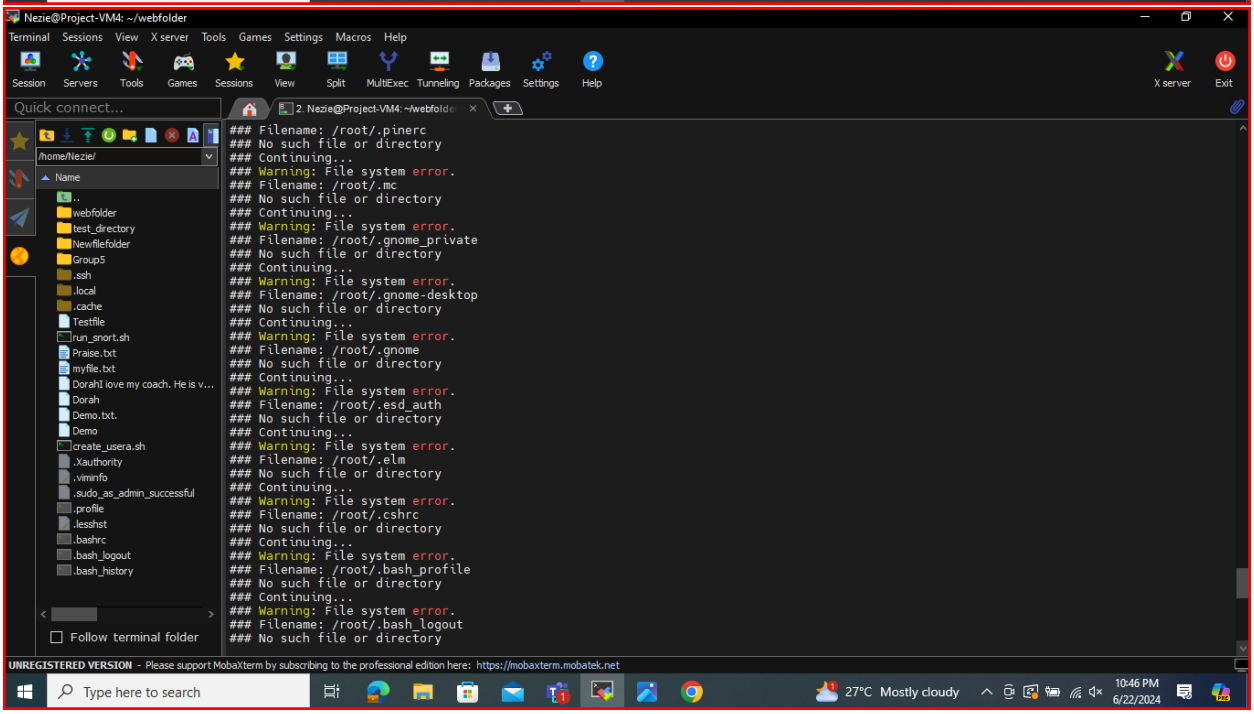
Command used: sudo tripwire –init

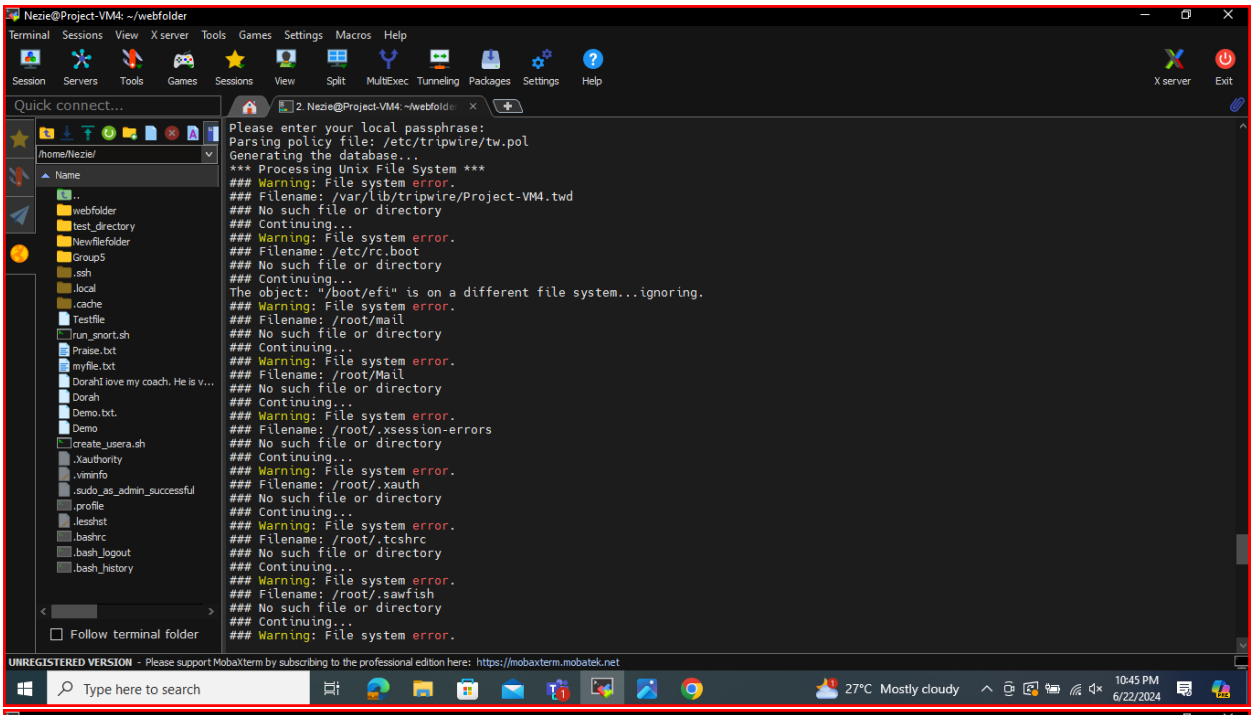


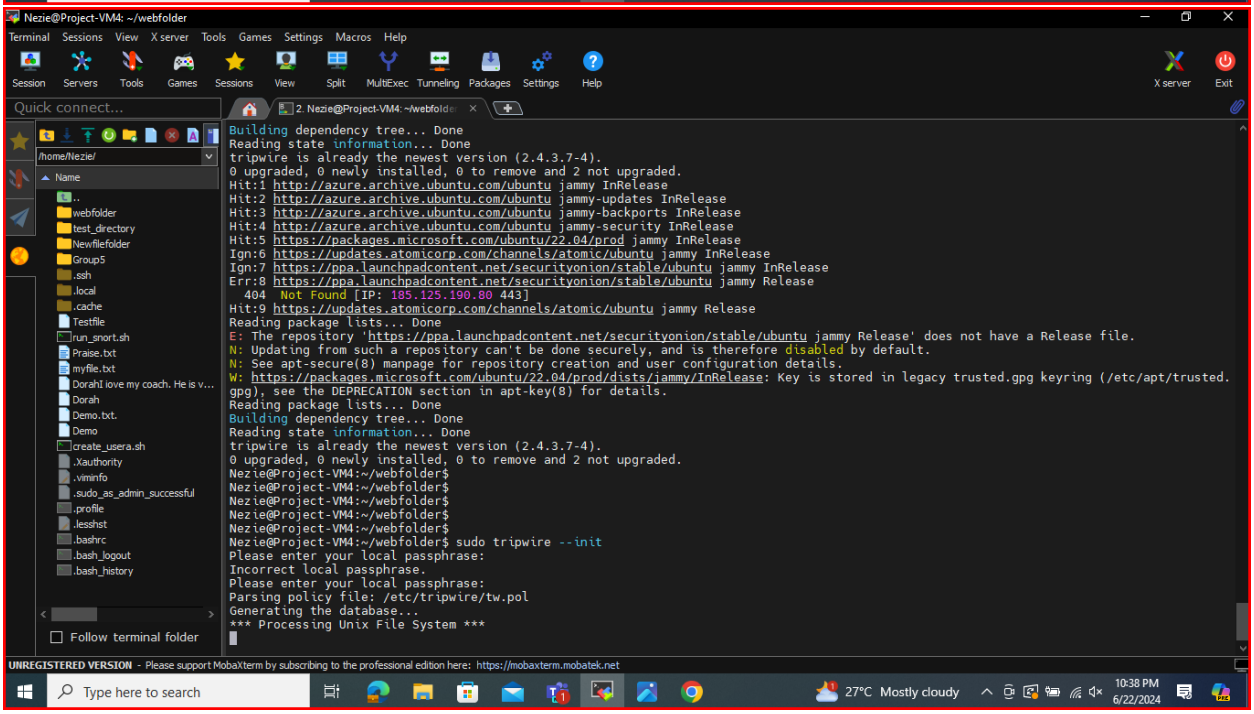

Nezie@Project-VM4: ~/webfolder
MobaXterm paste confirmation
You are about to paste the following lines:
sudo twadmin --securityfile/webfolder /etc/tripwire/twpol.txt
sudo tripwire --init
Each line will be pasted into the terminal and may be executed if you are inside an interactive shell.
Are you sure you want to continue?
OK
Cancel
Do not show this message again
Nezie@Project-VM4:~/webfolder$
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
27°C Partly cloudy
10:56 PM
6/22/2024


Nezie@Project-VM4: ~/webfolder
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.Xresources
Filename: /root/.Xauthority
Filename: /root/.ICEauthority
The object: "/dev/hugepages" is on a different file system...ignoring.
The object: "/dev/mqueue" is on a different file system...ignoring.
The object: "/dev/pts" is on a different file system...ignoring.
The object: "/dev/shm" is on a different file system...ignoring.
Filename: /proc/24713/fd/4
Filename: /proc/24713/fdinfo/4
Filename: /proc/24713/task/24713/fd/4
Filename: /proc/24713/task/24713/fdinfo/4
The object: "/proc/sys/fs/binfmt_misc" is on a different file system...ignoring.
Wrote database file: /var/lib/tripwire/Project-VM4.twd
The database was successfully generated.
Nezie@Project-VM4:~/webfolder$
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
27°C Mostly cloudy
10:46 PM
6/22/2024


Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Filename: /root/.bash_logout
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.bash_history
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.amandahosts
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.addressbook.lu
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.addressbook
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.Xresources
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.Xauthority
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.ICEauthority
No such file or directory
Continuing...
The object: "/dev/hugepages" is on a different file system...ignoring.
The object: "/dev/mqueue" is on a different file system...ignoring.
The object: "/dev/pts" is on a different file system...ignoring.
The object: "/dev/shm" is on a different file system...ignoring.
Warning: File system error.
Filename: /proc/24713/fd/4
No such file or directory
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
27°C Mostly cloudy
10:46 PM
6/22/2024


Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Filename: /root/.pinerc
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.mc
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.gnome_private
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.gnome-desktop
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.gnome
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.esd_auth
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.elm
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.cshrc
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.bash_profile
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.bash_logout
No such file or directory
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
27°C Mostly cloudy
10:46 PM
6/22/2024

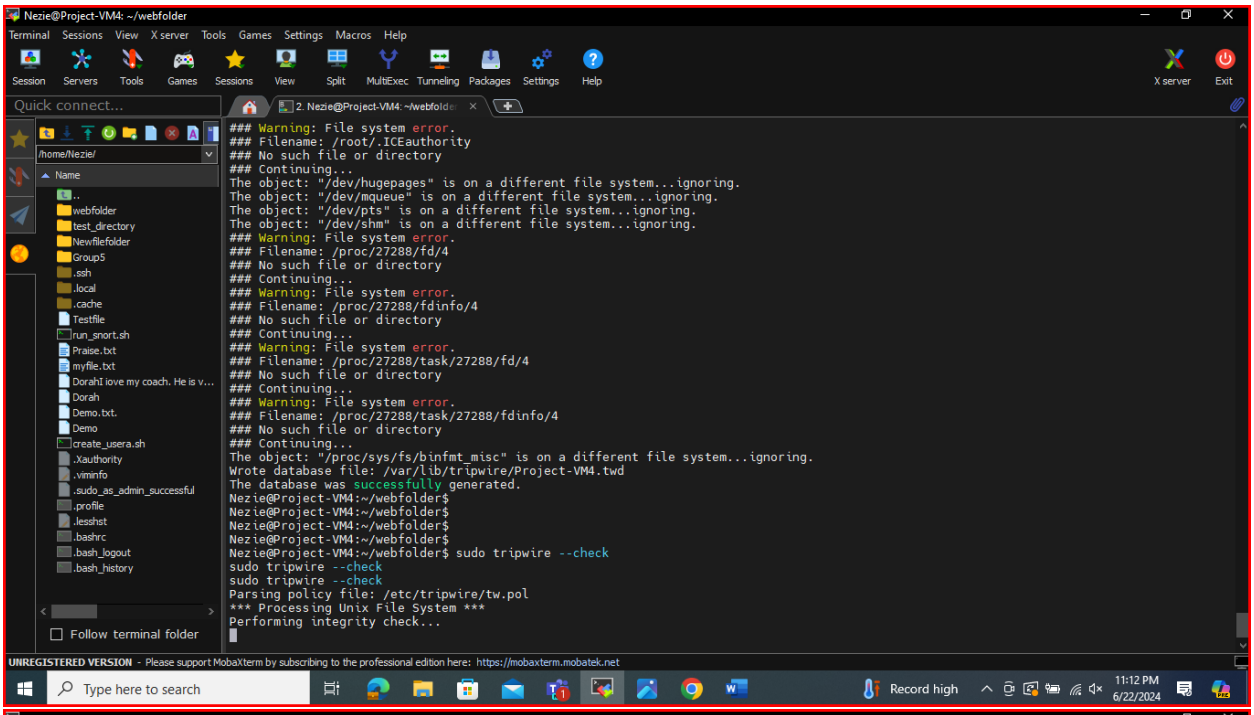


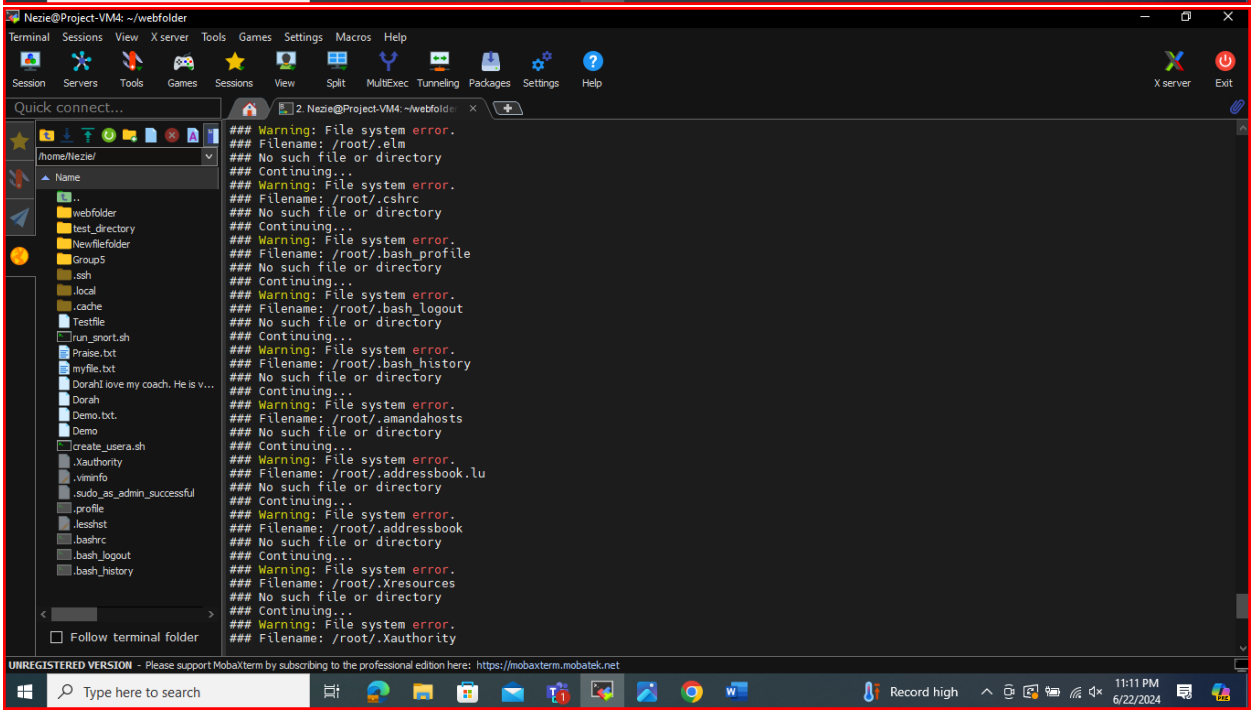


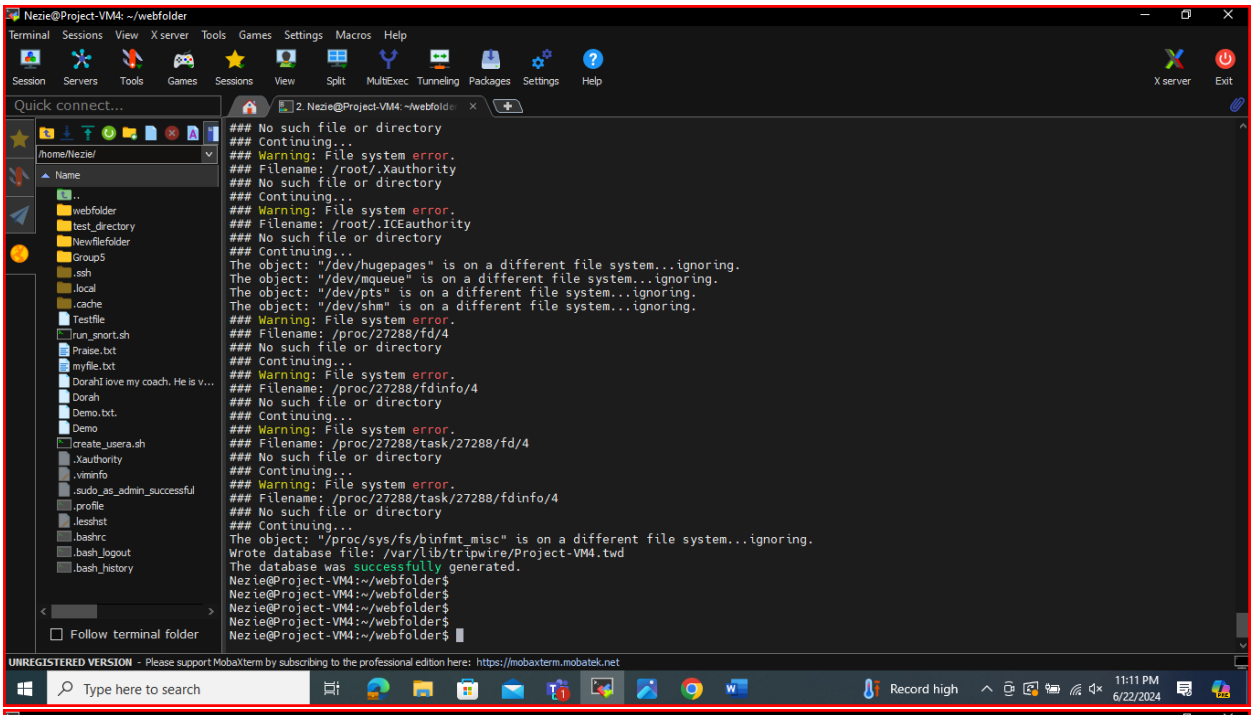
3. Configure Tripwire Policies

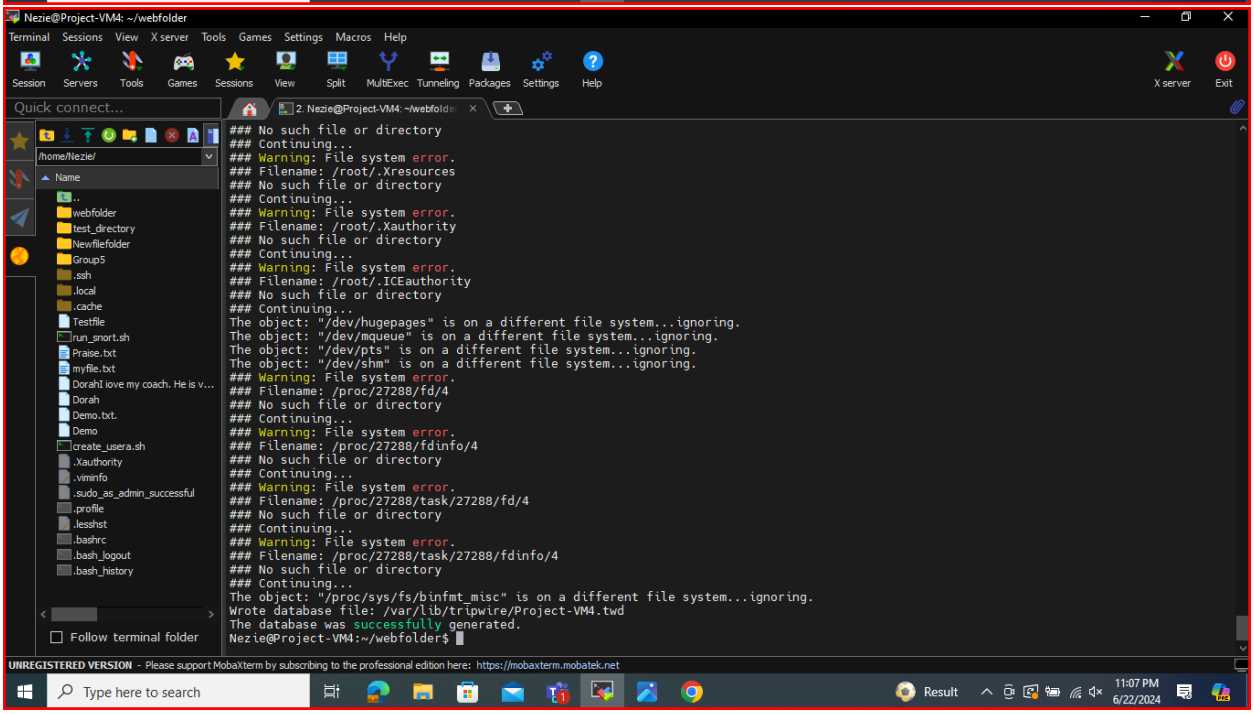
sudo twadmin --create-polfile /etc/tripwire/twpol.txt

sudo tripwire --init


Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Warning: File system error.
Filename: /root/.ICEauthority
No such file or directory
Continuing...
The object: "/dev/hugepages" is on a different file system...ignoring.
The object: "/dev/mqueue" is on a different file system...ignoring.
The object: "/dev/pts" is on a different file system...ignoring.
The object: "/dev/shm" is on a different file system...ignoring.
Warning: File system error.
Filename: /proc/27288/fd/4
No such file or directory
Continuing...
Warning: File system error.
Filename: /proc/27288/fdinfo/4
No such file or directory
Continuing...
Warning: File system error.
Filename: /proc/27288/task/27288/fd/4
No such file or directory
Continuing...
Warning: File system error.
Filename: /proc/27288/task/27288/fdinfo/4
No such file or directory
Continuing...
The object: "/proc/sys/fs/binfmt_misc" is on a different file system...ignoring.
Wrote database file: /var/lib/tripwire/Project-VM4.twd
The database was successfully generated.
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo tripwire --check
sudo tripwire --check
sudo tripwire --check
Parsing policy file: /etc/tripwire/tw.pol
*** Processing Unix File System ***
Performing integrity check...
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
Record high
11:12 PM
6/22/2024

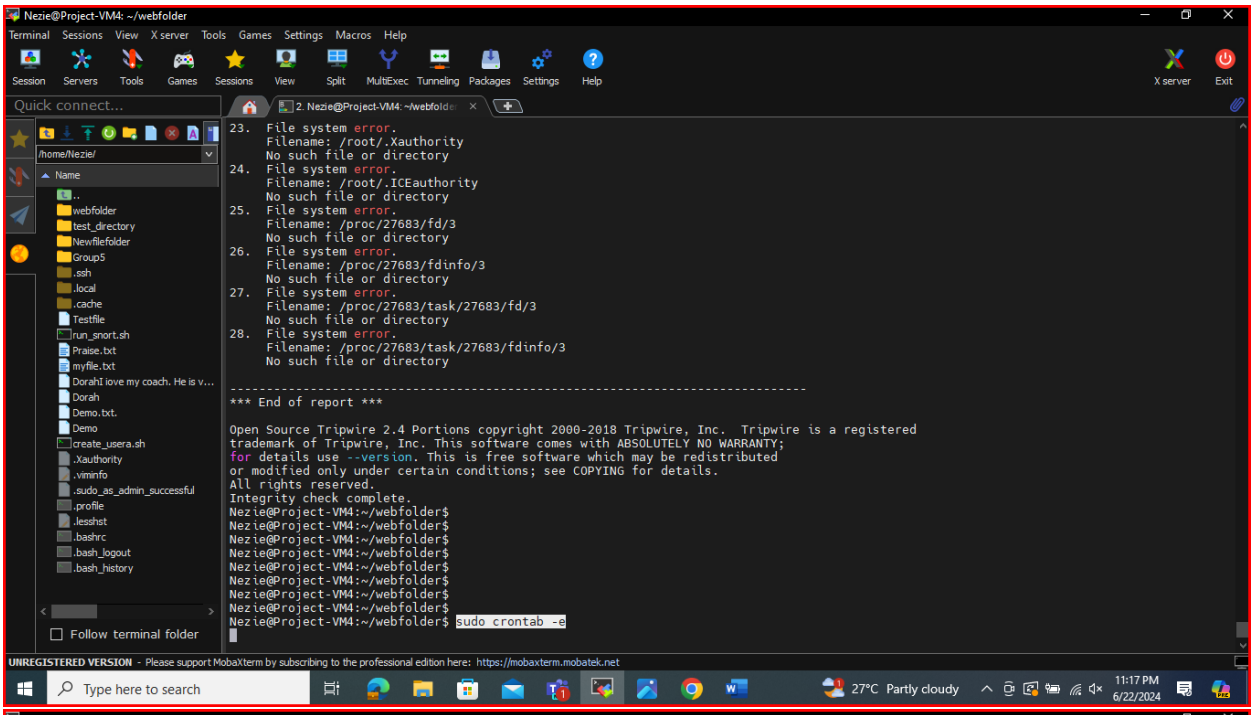

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Warning: File system error.
Filename: /root/.elm
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.cshrc
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.bash_profile
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.bash_logout
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.bash_history
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.amandahosts
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.addressbook.lu
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.addressbook
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.Xresources
No such file or directory
Continuing...
Warning: File system error.
Filename: /root/.Xauthority
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
Record high
11:11 PM
6/22/2024

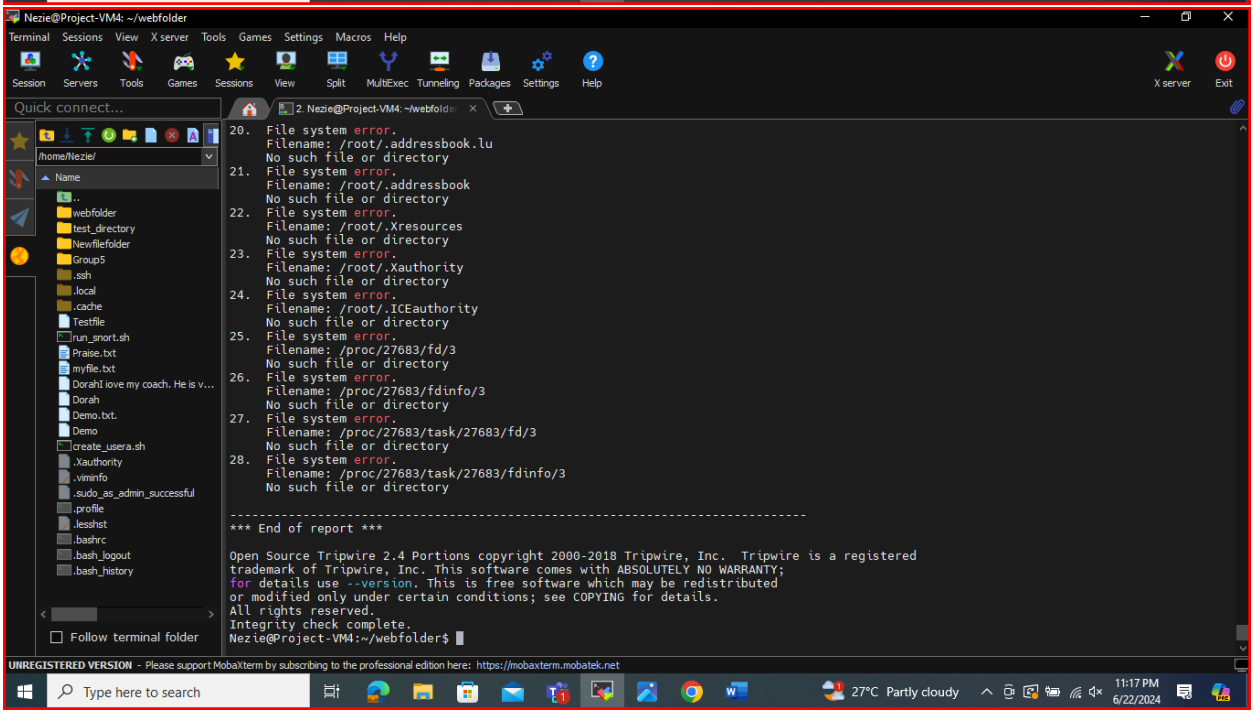




4. Integrity Checks

To check the integrity of our files, the following command was used: sudo tripwire --check





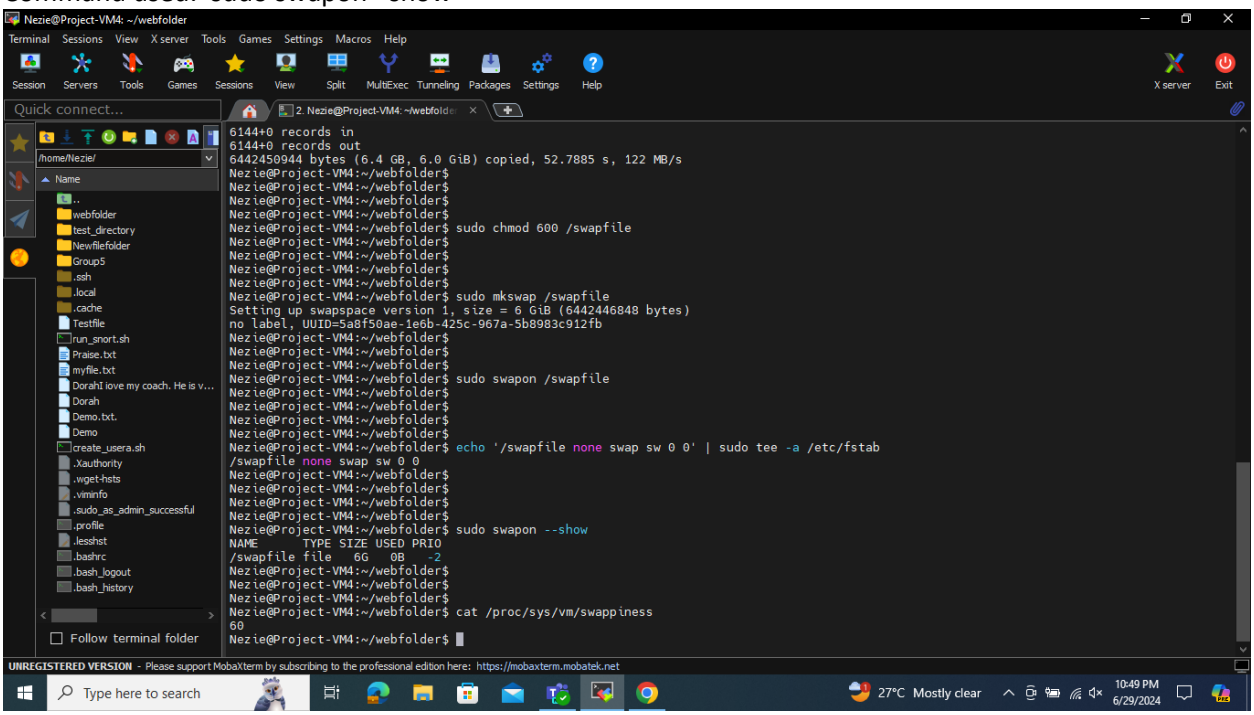
TASK 3: **Swap File Configuration**

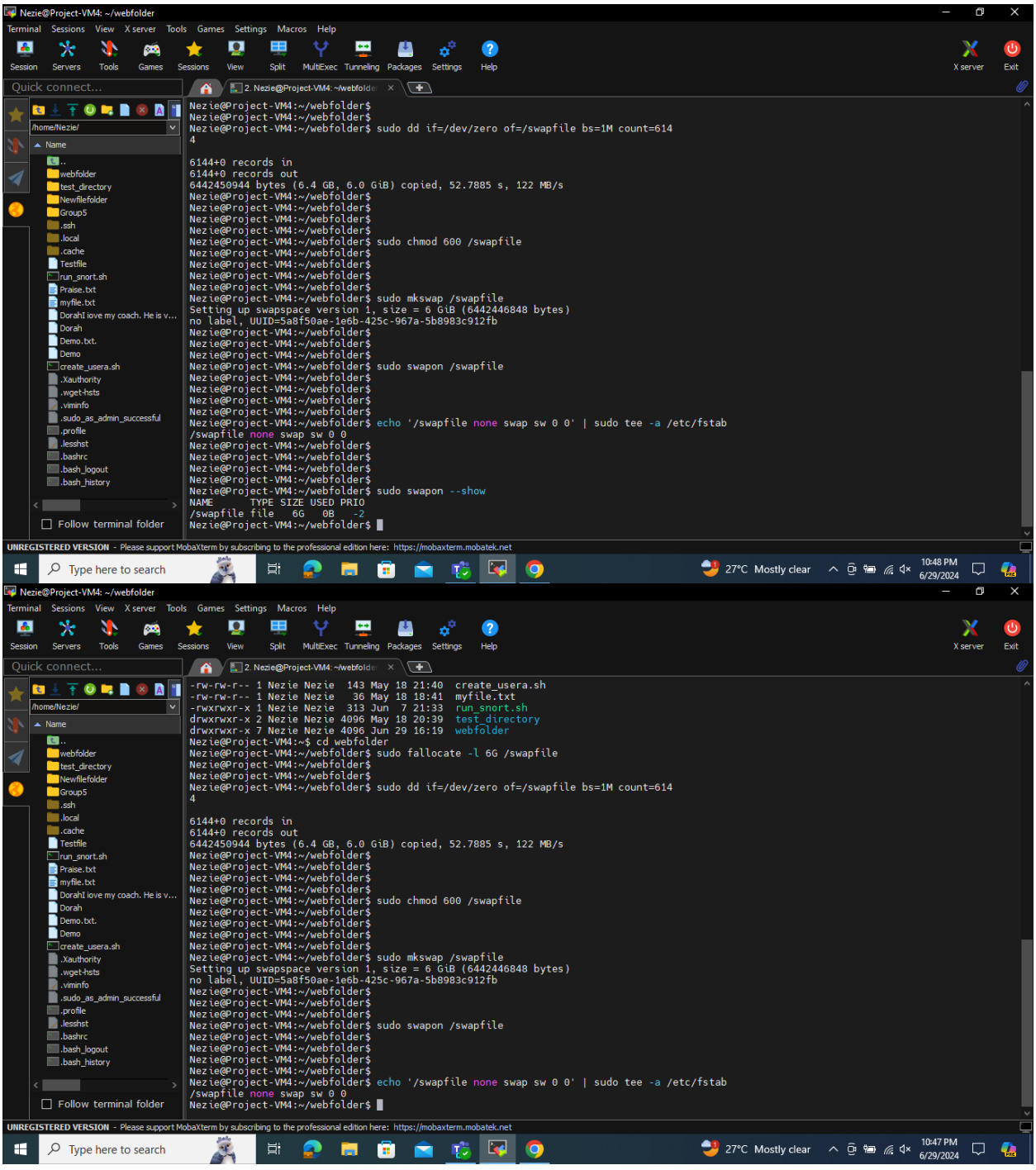
Create a Swap File

1. **Create a swap file of 6GB size.**

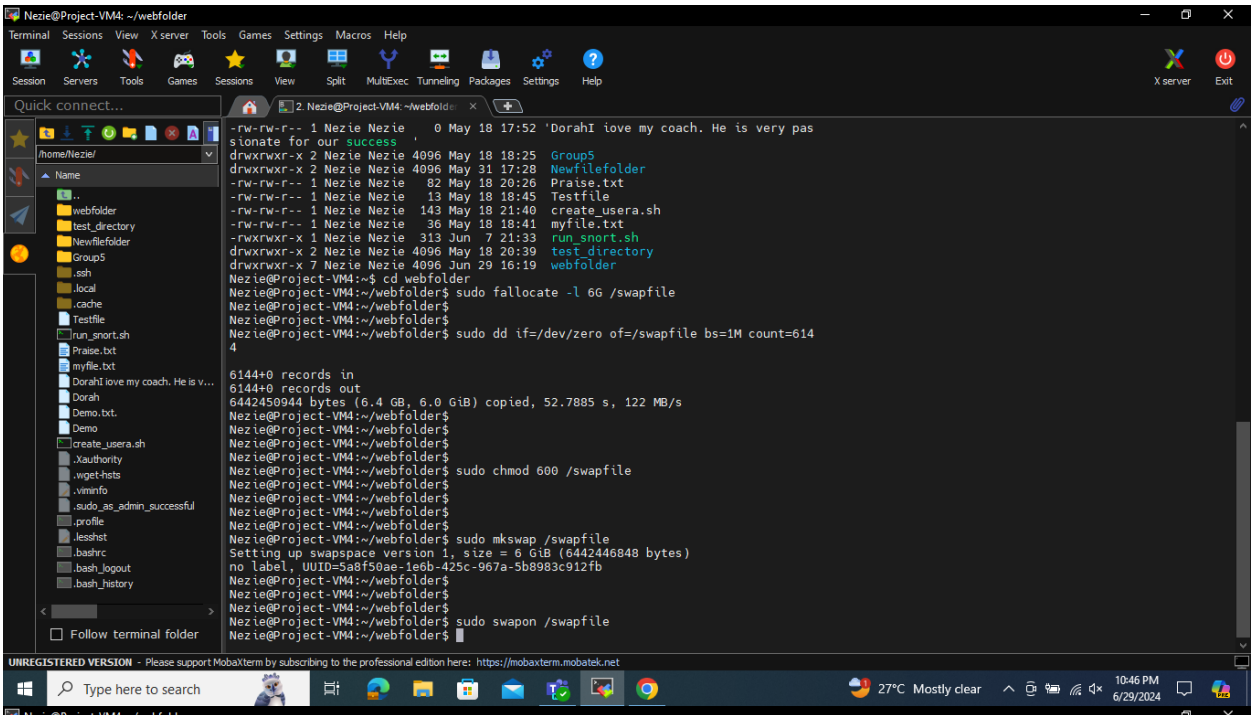
   Command used: sudo dd if=/dev/zero of=/swapfile bs=1M count=6144

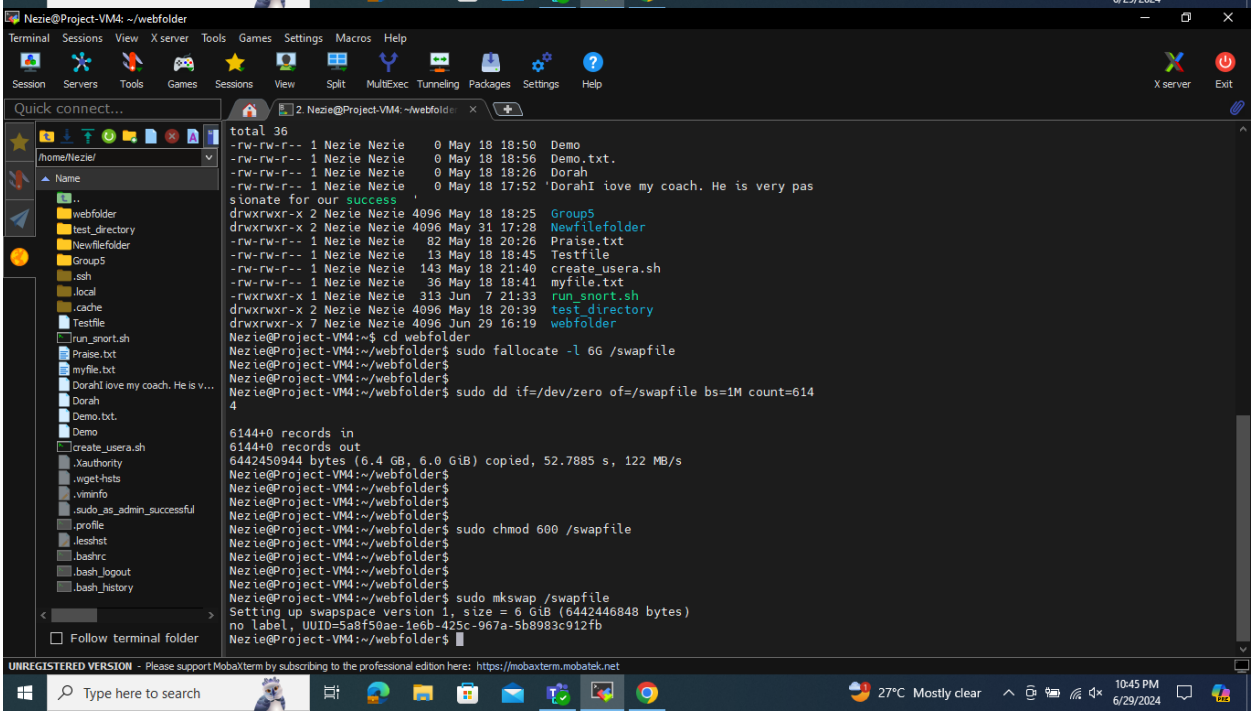
2. Setting of correct permissions for the swap file:
   Command used: sudo chmod 600 /swapfile
3. The file was marked as swap space:
   Command used: sudo mkswap /swapfile
4. Enabling the swap file:
   Command used: **sudo swapon /swapfile**
5. Make the swap file permanent by adding it to `/etc/fstab`:
   Command used: echo '/swapfile none swap sw 0 0' | sudo tee -a /etc/fstab
6. Verify that the swap file is active:
   Command used: sudo swapon –show

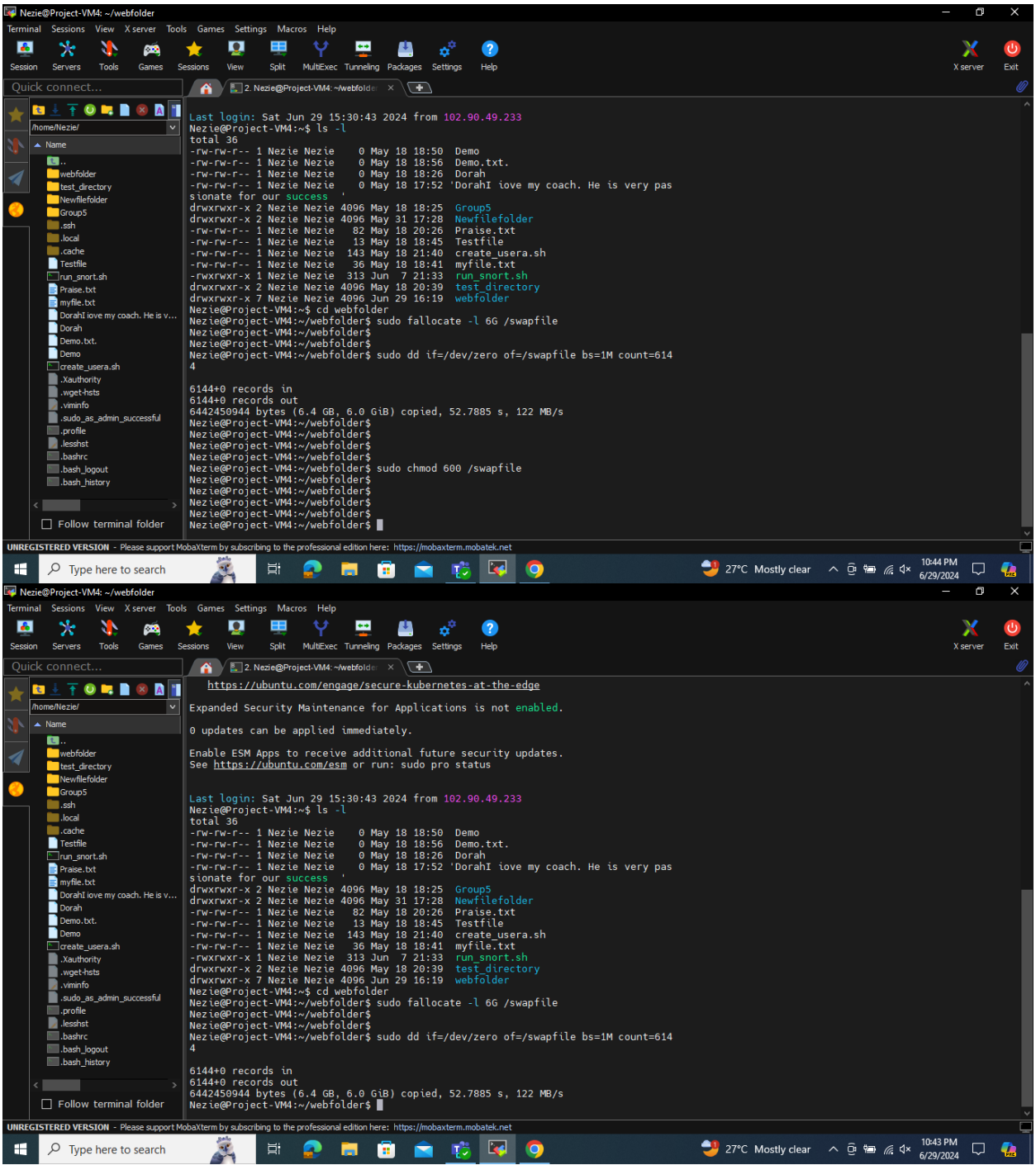



Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
..
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
Dorah I love my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.wget-hsts
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo dd if=/dev/zero of=/swapfile bs=1M count=614
4
6144+0 records in
6144+0 records out
6442450944 bytes (6.4 GB, 6.0 GiB) copied, 52.7885 s, 122 MB/s
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo chmod 600 /swapfile
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo mkswap /swapfile
Setting up swapspace version 1, size = 6 GiB (6442446848 bytes)
no label, UUID=5a8f50ae-1e6b-425c-967a-5b8983c912fb
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo swapon /swapfile
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ echo '/swapfile none swap sw 0 0' | sudo tee -a /etc/fstab
/swapfile none swap sw 0 0
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo swapon --show
NAME TYPE SIZE USED PRIO
/swapfile file 6G 0B -2
Nezie@Project-VM4:~/webfolder$
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
27°C Mostly clear
10:48 PM
6/29/2024

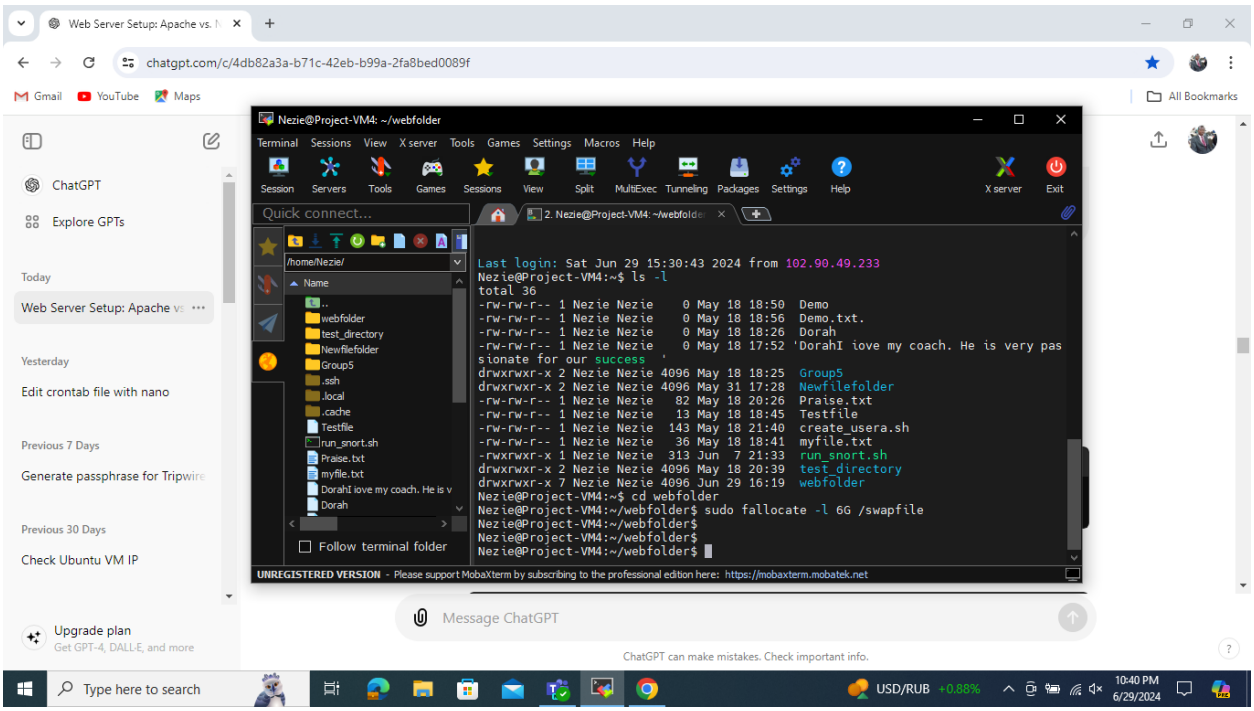
Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
..
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
Dorah I love my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.wget-hsts
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
-rw-rw-r-- 1 Nezie Nezie 143 May 18 21:40 create_usera.sh
-rw-rw-r-- 1 Nezie Nezie 36 May 18 18:41 myfile.txt
-rwxrwxr-x 1 Nezie Nezie 313 Jun 7 21:33 run_snort.sh
drwxrwxr-x 2 Nezie Nezie 4096 May 18 20:39 test_directory
drwxrwxr-x 7 Nezie Nezie 4096 Jun 29 16:19 webfolder
Nezie@Project-VM4:~$ cd webfolder
Nezie@Project-VM4:~/webfolder$ sudo fallocate -l 6G /swapfile
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo dd if=/dev/zero of=/swapfile bs=1M count=614
4
6144+0 records in
6144+0 records out
6442450944 bytes (6.4 GB, 6.0 GiB) copied, 52.7885 s, 122 MB/s
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo chmod 600 /swapfile
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo mkswap /swapfile
Setting up swapspace version 1, size = 6 GiB (6442446848 bytes)
no label, UUID=5a8f50ae-1e6b-425c-967a-5b8983c912fb
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo swapon /swapfile
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ echo '/swapfile none swap sw 0 0' | sudo tee -a /etc/fstab
/swapfile none swap sw 0 0
Nezie@Project-VM4:~/webfolder$
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
27°C Mostly clear
10:47 PM
6/29/2024


Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.wget-hsts
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
-rw-rw-r-- 1 Nezie Nezie 0 May 18 17:52 'DorahI iove my coach. He is very pas
sionate for our success '
drwxrwxr-x 2 Nezie Nezie 4096 May 18 18:25 Group5
drwxrwxr-x 2 Nezie Nezie 4096 May 31 17:28 Newfilefolder
-rw-rw-r-- 1 Nezie Nezie 82 May 18 20:26 Praise.txt
-rw-rw-r-- 1 Nezie Nezie 13 May 18 18:45 Testfile
-rw-rw-r-- 1 Nezie Nezie 143 May 18 21:40 create_usera.sh
-rw-rw-r-- 1 Nezie Nezie 36 May 18 18:41 myfile.txt
-rwxrwxr-x 1 Nezie Nezie 313 Jun 7 21:33 run_snort.sh
drwxrwxr-x 2 Nezie Nezie 4096 May 18 20:39 test_directory
drwxrwxr-x 7 Nezie Nezie 4096 Jun 29 16:19 webfolder
Nezie@Project-VM4:~$ cd webfolder
Nezie@Project-VM4:~/webfolder$ sudo fallocate -l 6G /swapfile
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo dd if=/dev/zero of=/swapfile bs=1M count=614
4
6144+0 records in
6144+0 records out
6442450944 bytes (6.4 GB, 6.0 GiB) copied, 52.7885 s, 122 MB/s
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo chmod 600 /swapfile
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo mkswap /swapfile
Setting up swapspace version 1, size = 6 GiB (6442446848 bytes)
no label, UUID=5a8f50ae-1e6b-425c-967a-5b8983c912fb
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo swapon /swapfile
Nezie@Project-VM4:~/webfolder$
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
27°C Mostly clear
10:46 PM
6/29/2024


Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.wget-hsts
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
total 36
-rw-rw-r-- 1 Nezie Nezie 0 May 18 18:50 Demo
-rw-rw-r-- 1 Nezie Nezie 0 May 18 18:56 Demo.txt.
-rw-rw-r-- 1 Nezie Nezie 0 May 18 18:26 Dorah
-rw-rw-r-- 1 Nezie Nezie 0 May 18 17:52 'DorahI iove my coach. He is very pas
sionate for our success '
drwxrwxr-x 2 Nezie Nezie 4096 May 18 18:25 Group5
drwxrwxr-x 2 Nezie Nezie 4096 May 31 17:28 Newfilefolder
-rw-rw-r-- 1 Nezie Nezie 82 May 18 20:26 Praise.txt
-rw-rw-r-- 1 Nezie Nezie 13 May 18 18:45 Testfile
-rw-rw-r-- 1 Nezie Nezie 143 May 18 21:40 create_usera.sh
-rw-rw-r-- 1 Nezie Nezie 36 May 18 18:41 myfile.txt
-rwxrwxr-x 1 Nezie Nezie 313 Jun 7 21:33 run_snort.sh
drwxrwxr-x 2 Nezie Nezie 4096 May 18 20:39 test_directory
drwxrwxr-x 7 Nezie Nezie 4096 Jun 29 16:19 webfolder
Nezie@Project-VM4:~$ cd webfolder
Nezie@Project-VM4:~/webfolder$ sudo fallocate -l 6G /swapfile
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo dd if=/dev/zero of=/swapfile bs=1M count=614
4
6144+0 records in
6144+0 records out
6442450944 bytes (6.4 GB, 6.0 GiB) copied, 52.7885 s, 122 MB/s
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo chmod 600 /swapfile
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo mkswap /swapfile
Setting up swapspace version 1, size = 6 GiB (6442446848 bytes)
no label, UUID=5a8f50ae-1e6b-425c-967a-5b8983c912fb
Nezie@Project-VM4:~/webfolder$
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
27°C Mostly clear
10:45 PM
6/29/2024


Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.wget-hsts
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Last login: Sat Jun 29 15:30:43 2024 from 102.90.49.233
Nezie@Project-VM4:~$ ls -l
total 36
-rw-rw-r-- 1 Nezie Nezie 0 May 18 18:50 Demo
-rw-rw-r-- 1 Nezie Nezie 0 May 18 18:56 Demo.txt.
-rw-rw-r-- 1 Nezie Nezie 0 May 18 18:26 Dorah
-rw-rw-r-- 1 Nezie Nezie 0 May 18 17:52 'DorahI iove my coach. He is very pas
sionate for our success '
drwxrwxr-x 2 Nezie Nezie 4096 May 18 18:25 Group5
drwxrwxr-x 2 Nezie Nezie 4096 May 31 17:28 Newfilefolder
-rw-rw-r-- 1 Nezie Nezie 82 May 18 20:26 Praise.txt
-rw-rw-r-- 1 Nezie Nezie 13 May 18 18:45 Testfile
-rw-rw-r-- 1 Nezie Nezie 143 May 18 21:40 create_usera.sh
-rw-rw-r-- 1 Nezie Nezie 36 May 18 18:41 myfile.txt
-rwxrwxr-x 1 Nezie Nezie 313 Jun 7 21:33 run_snort.sh
drwxrwxr-x 2 Nezie Nezie 4096 May 18 20:39 test_directory
drwxrwxr-x 7 Nezie Nezie 4096 Jun 29 16:19 webfolder
Nezie@Project-VM4:~$ cd webfolder
Nezie@Project-VM4:~/webfolder$ sudo fallocate -l 6G /swapfile
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo dd if=/dev/zero of=/swapfile bs=1M count=614
4
6144+0 records in
6144+0 records out
6442450944 bytes (6.4 GB, 6.0 GiB) copied, 52.7885 s, 122 MB/s
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo chmod 600 /swapfile
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
27°C Mostly clear
10:44 PM
6/29/2024

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolde
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
DorahI iove my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.wget-hsts
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
https://ubuntu.com/engage/secure-kubernetes-at-the-edge
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
Last login: Sat Jun 29 15:30:43 2024 from 102.90.49.233
Nezie@Project-VM4:~$ ls -l
total 36
-rw-rw-r-- 1 Nezie Nezie 0 May 18 18:50 Demo
-rw-rw-r-- 1 Nezie Nezie 0 May 18 18:56 Demo.txt.
-rw-rw-r-- 1 Nezie Nezie 0 May 18 18:26 Dorah
-rw-rw-r-- 1 Nezie Nezie 0 May 18 17:52 'DorahI iove my coach. He is very pas
sionate for our success '
drwxrwxr-x 2 Nezie Nezie 4096 May 18 18:25 Group5
drwxrwxr-x 2 Nezie Nezie 4096 May 31 17:28 Newfilefolder
-rw-rw-r-- 1 Nezie Nezie 82 May 18 20:26 Praise.txt
-rw-rw-r-- 1 Nezie Nezie 13 May 18 18:45 Testfile
-rw-rw-r-- 1 Nezie Nezie 143 May 18 21:40 create_usera.sh
-rw-rw-r-- 1 Nezie Nezie 36 May 18 18:41 myfile.txt
-rwxrwxr-x 1 Nezie Nezie 313 Jun 7 21:33 run_snort.sh
drwxrwxr-x 2 Nezie Nezie 4096 May 18 20:39 test_directory
drwxrwxr-x 7 Nezie Nezie 4096 Jun 29 16:19 webfolder
Nezie@Project-VM4:~$ cd webfolder
Nezie@Project-VM4:~/webfolder$ sudo fallocate -l 6G /swapfile
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo dd if=/dev/zero of=/swapfile bs=1M count=614
4
6144+0 records in
6144+0 records out
6442450944 bytes (6.4 GB, 6.0 GiB) copied, 52.7885 s, 122 MB/s
Nezie@Project-VM4:~/webfolder$
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
27°C Mostly clear
10:43 PM
6/29/2024



Step 2

Optimize Swap Settings:

1. Adjust Swappiness

   Command used to check the current swappiness value

   cat /proc/sys/vm/swappiness

   To temporarily set swappiness to a new value (e.g., 10):

   sudo sysctl vm.swappiness=10

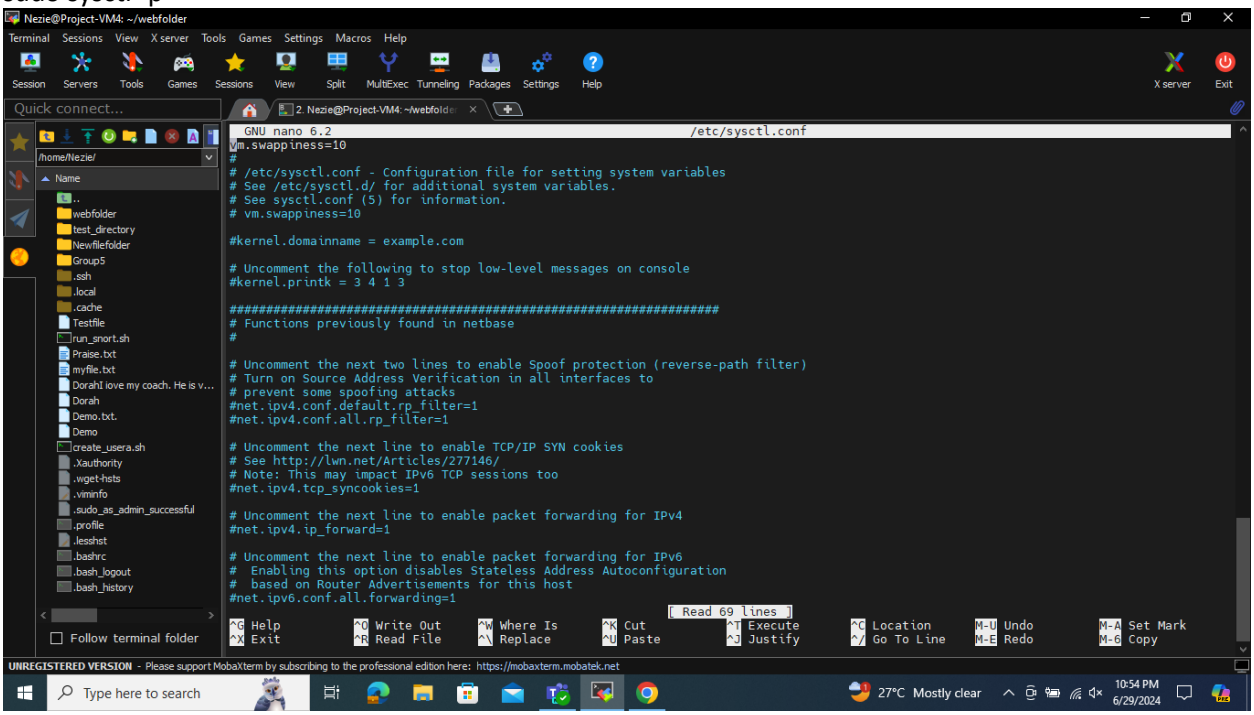
   To make this change permanent: sudo nano /etc/sysctl.conf

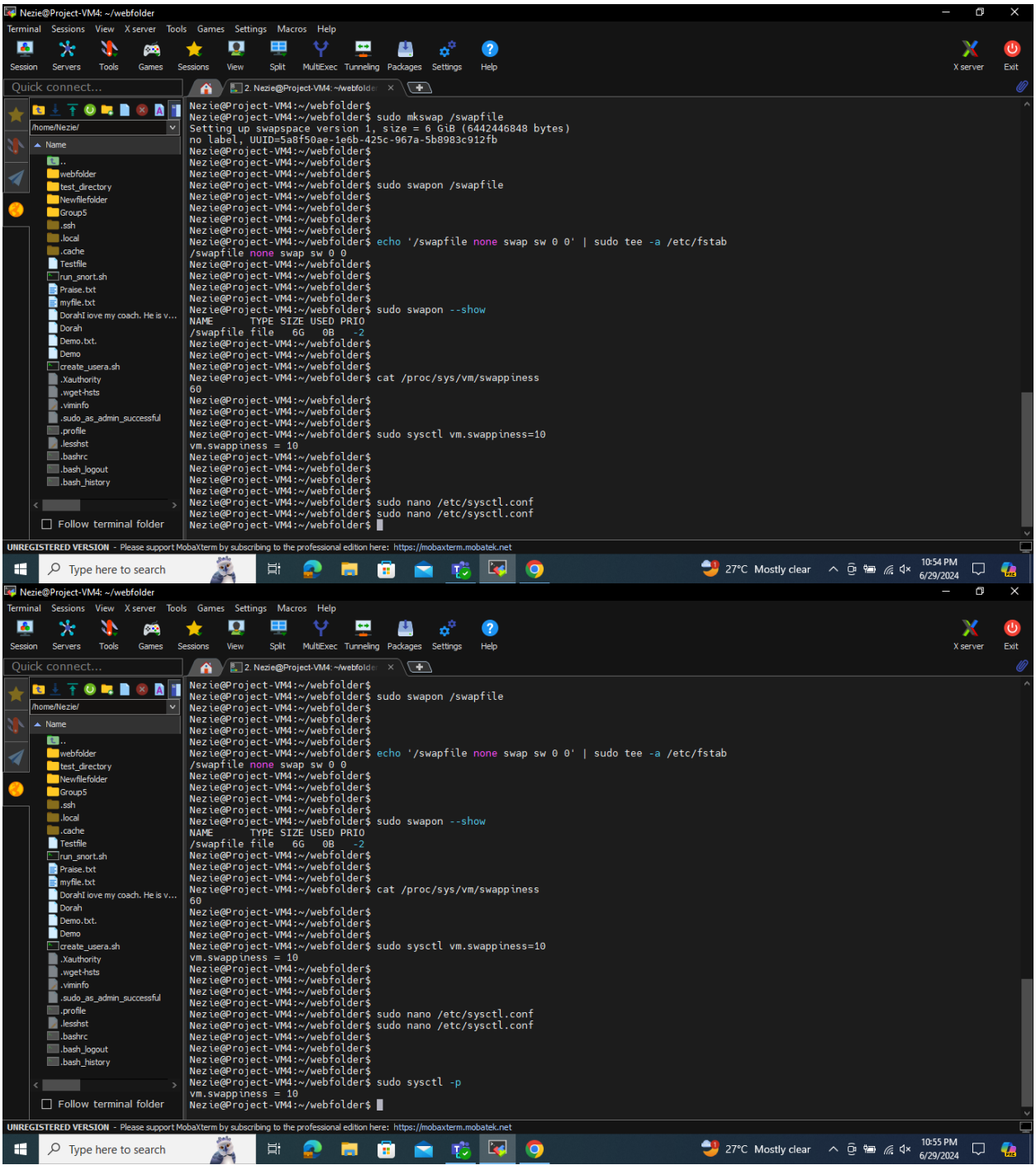
   It was modified by adding the following line

   vm.swappiness=10

   The file was saved and closed. The changes were then applied by using this command

sudo sysctl -p

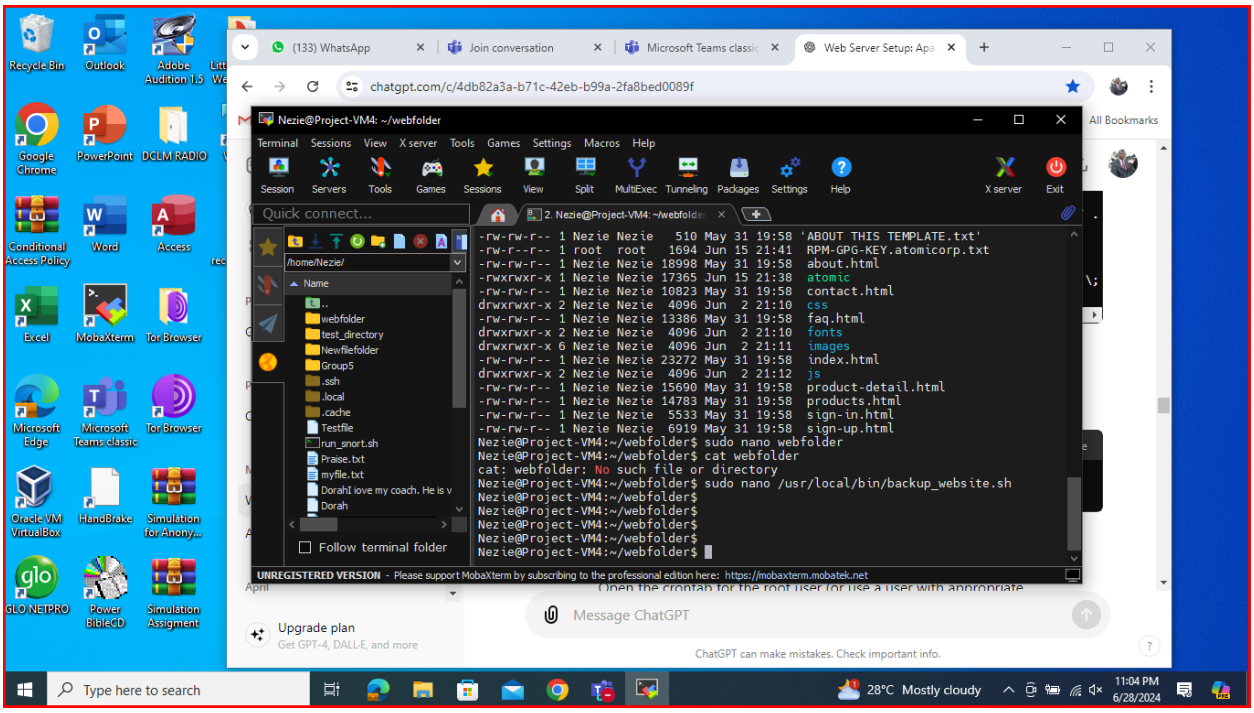


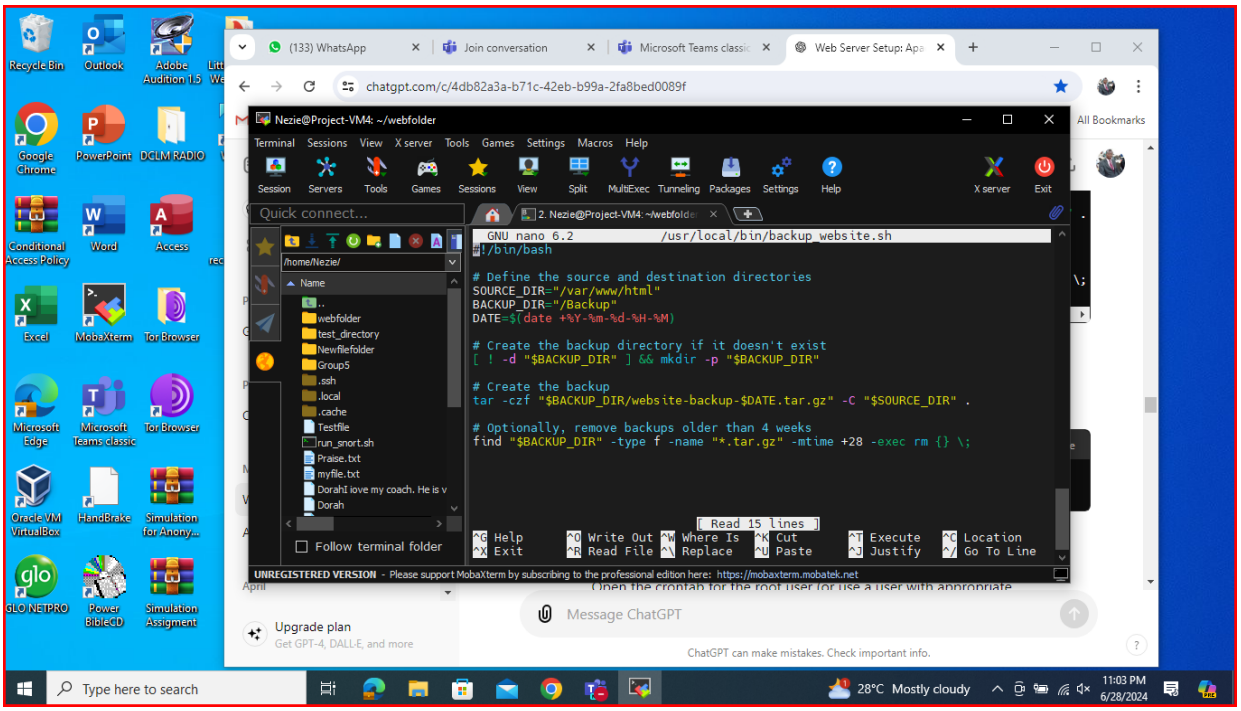

Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolder
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
Dorah I love my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.wget-hsts
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo mkswap /swapfile
Setting up swapspace version 1, size = 6 GiB (6442446848 bytes)
no label, UUID=5a8f50ae-1e6b-425c-967a-5b8983c912fb
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo swapon /swapfile
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ echo '/swapfile none swap sw 0 0' | sudo tee -a /etc/fstab
/swapfile none swap sw 0 0
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo swapon --show
NAME TYPE SIZE USED PRIO
/swapfile file 6G 0B -2
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ cat /proc/sys/vm/swappiness
60
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo sysctl vm.swappiness=10
vm.swappiness = 10
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo nano /etc/sysctl.conf
Nezie@Project-VM4:~/webfolder$ sudo nano /etc/sysctl.conf
Nezie@Project-VM4:~/webfolder$
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
27°C Mostly clear
10:54 PM
6/29/2024
Nezie@Project-VM4: ~/webfolder
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. Nezie@Project-VM4: ~/webfolder
/home/Nezie/
Name
webfolder
test_directory
Newfilefolder
Group5
.ssh
.local
.cache
Testfile
run_snort.sh
Praise.txt
myfile.txt
Dorah I love my coach. He is v...
Dorah
Demo.txt.
Demo
create_usera.sh
.Xauthority
.wget-hsts
.viminfo
.sudo_as_admin_successful
.profile
.lesshst
.bashrc
.bash_logout
.bash_history
Follow terminal folder
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo swapon /swapfile
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ echo '/swapfile none swap sw 0 0' | sudo tee -a /etc/fstab
/swapfile none swap sw 0 0
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo swapon --show
NAME TYPE SIZE USED PRIO
/swapfile file 6G 0B -2
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ cat /proc/sys/vm/swappiness
60
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo sysctl vm.swappiness=10
vm.swappiness = 10
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo nano /etc/sysctl.conf
Nezie@Project-VM4:~/webfolder$ sudo nano /etc/sysctl.conf
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo sysctl -p
vm.swappiness = 10
Nezie@Project-VM4:~/webfolder$
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
27°C Mostly clear
10:55 PM
6/29/2024

TASK 4: Automated Backup and Updates

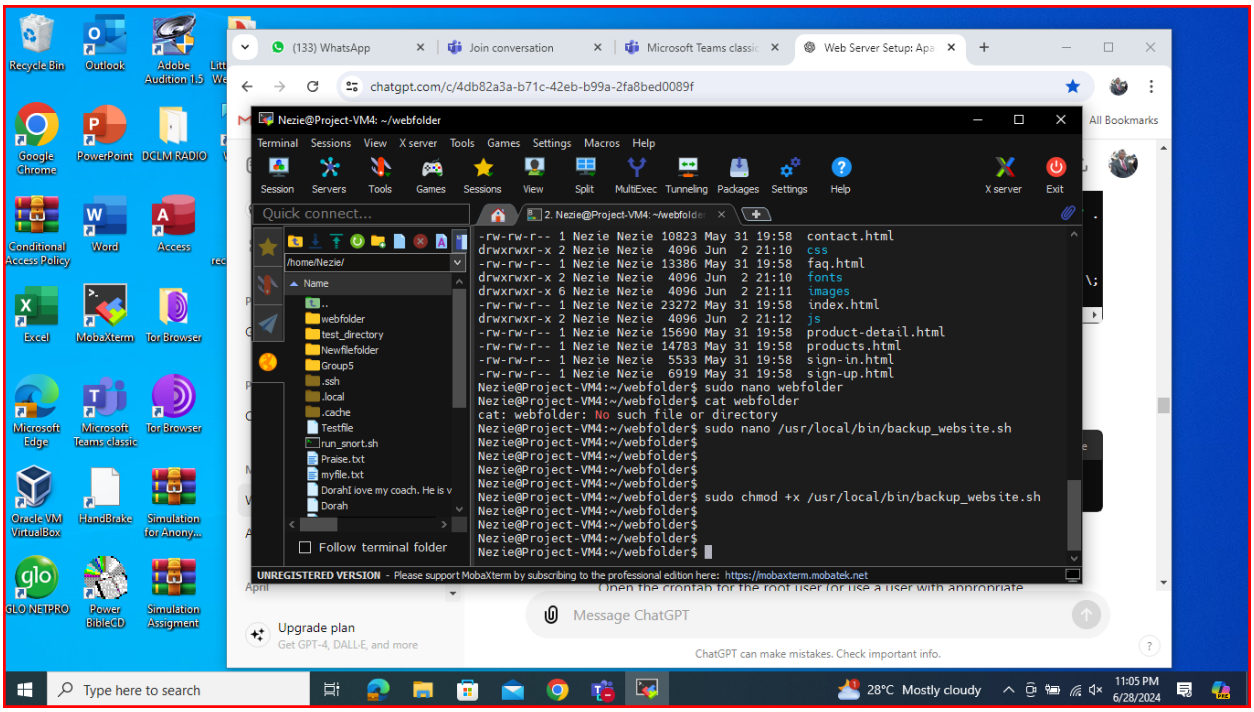
The following steps were followed to set up a cron job to create regular backups of the website directory and save them to the `/Backup` directory:

1. **Creating the Backup Script with this command: sudo nano /usr/local/bin/backup_website.sh**

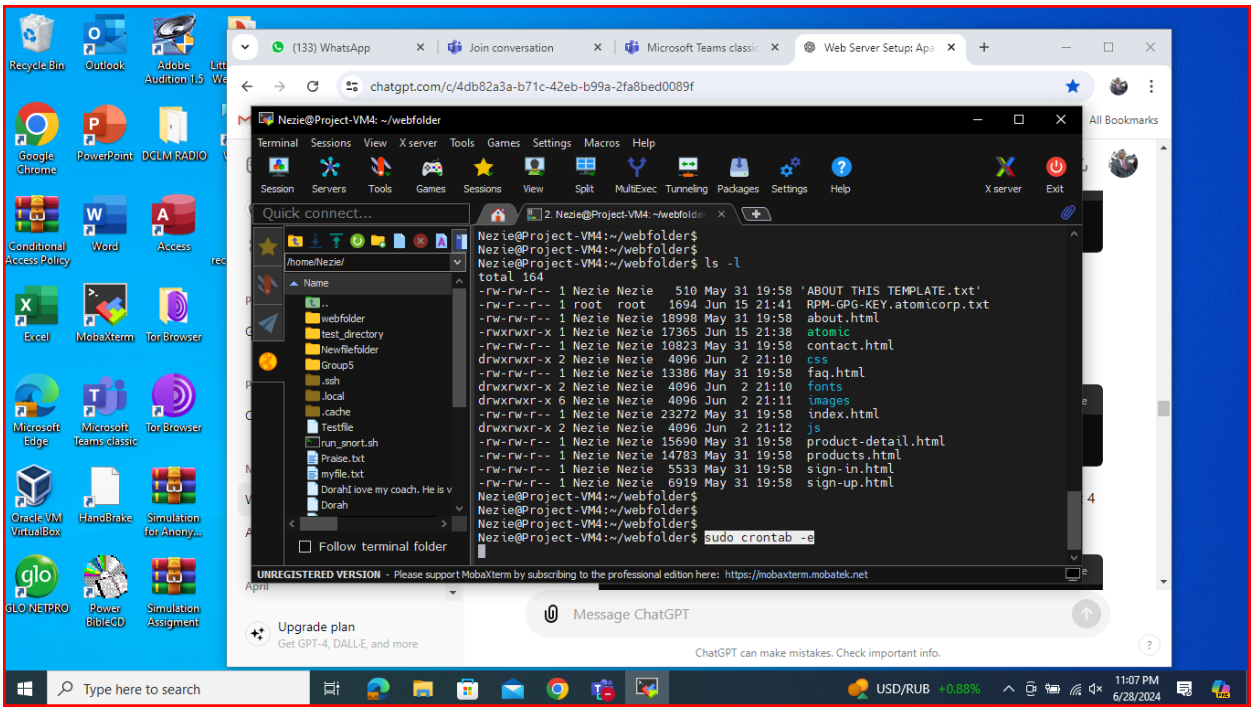




2. The Script was made Executable with this command: sudo chmod +x /usr/local/bin/backup_website.sh

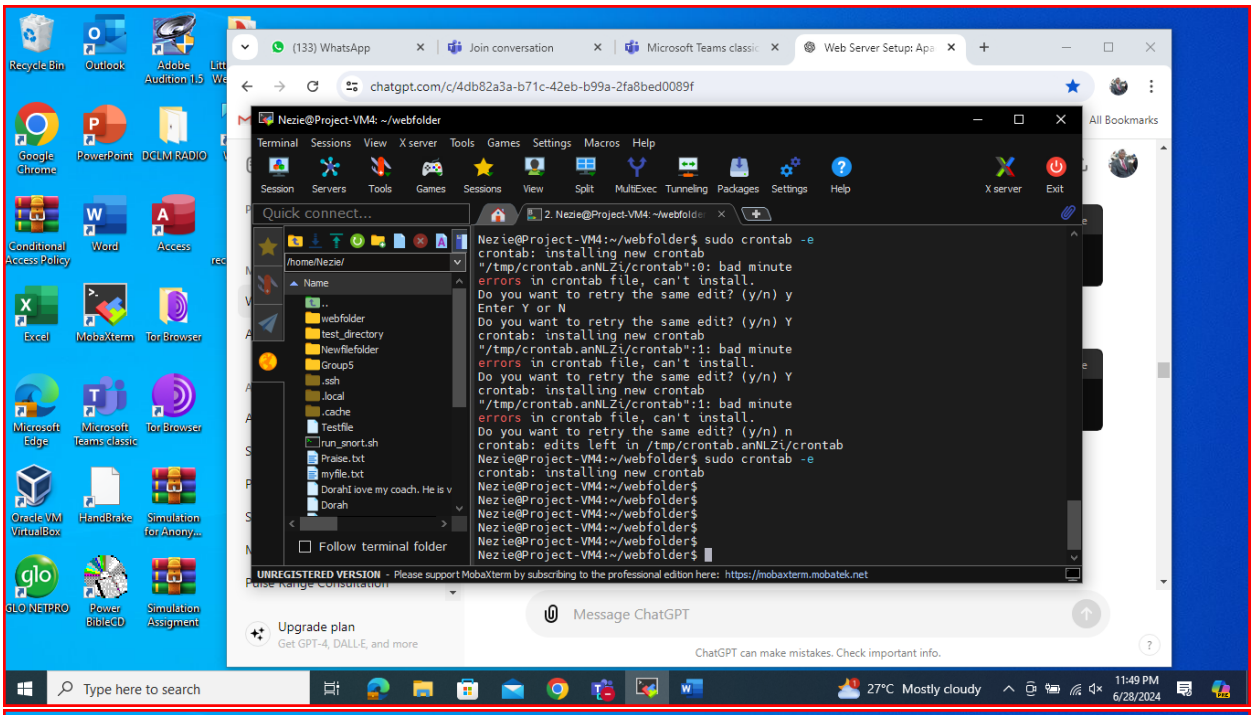


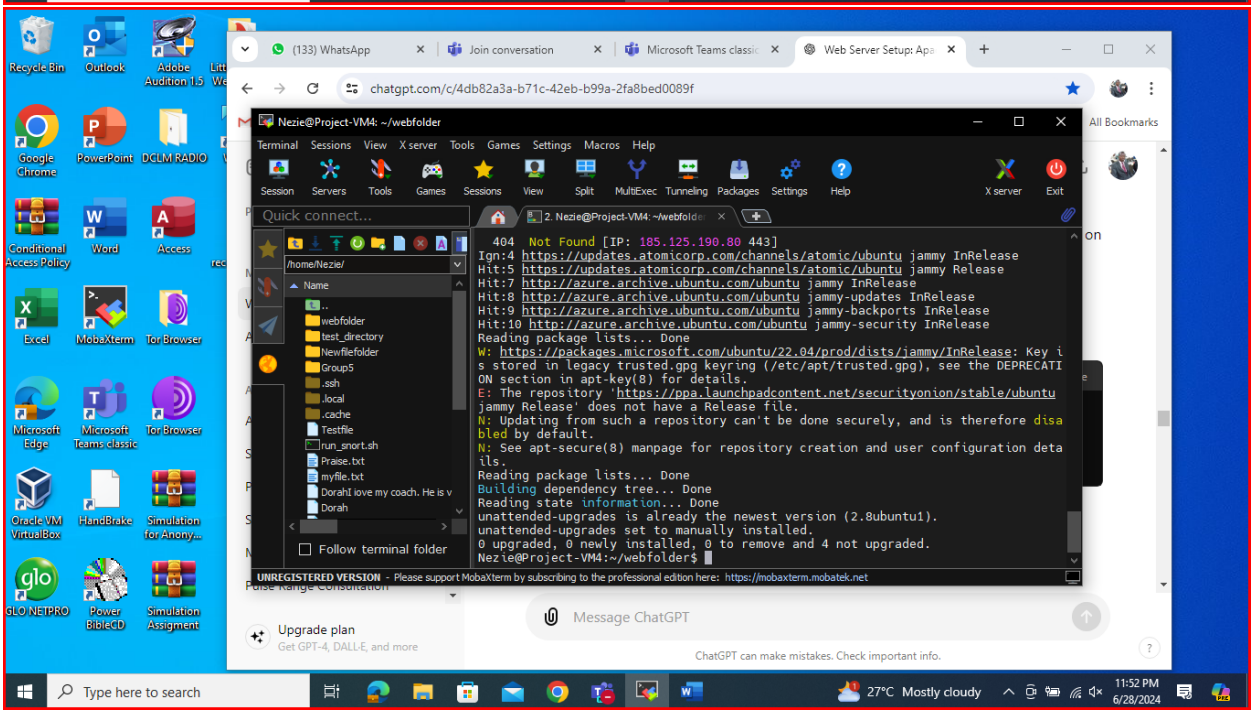
3. Creating a Cron Job for Regular Backups: sudo crontab -e



The following line was added to schedule the backup script to run every Sunday at 4 p.m.:

0 16 * * 0 /usr/local/bin/backup_website.sh

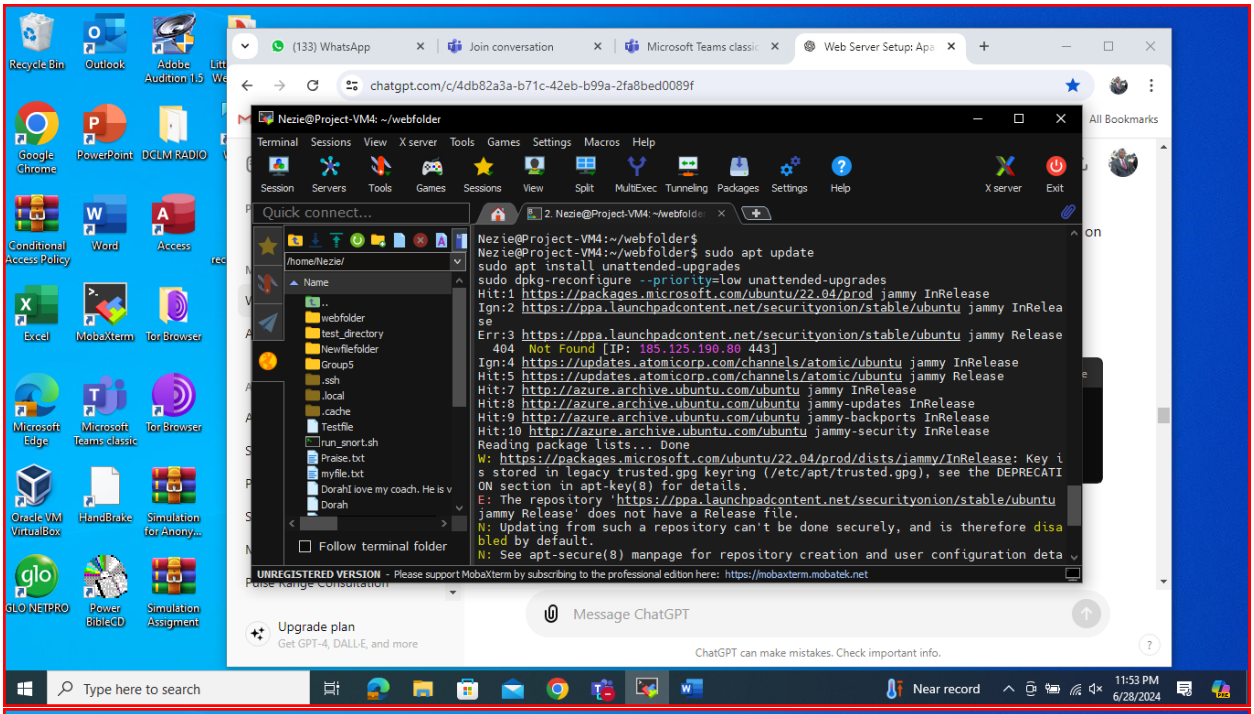


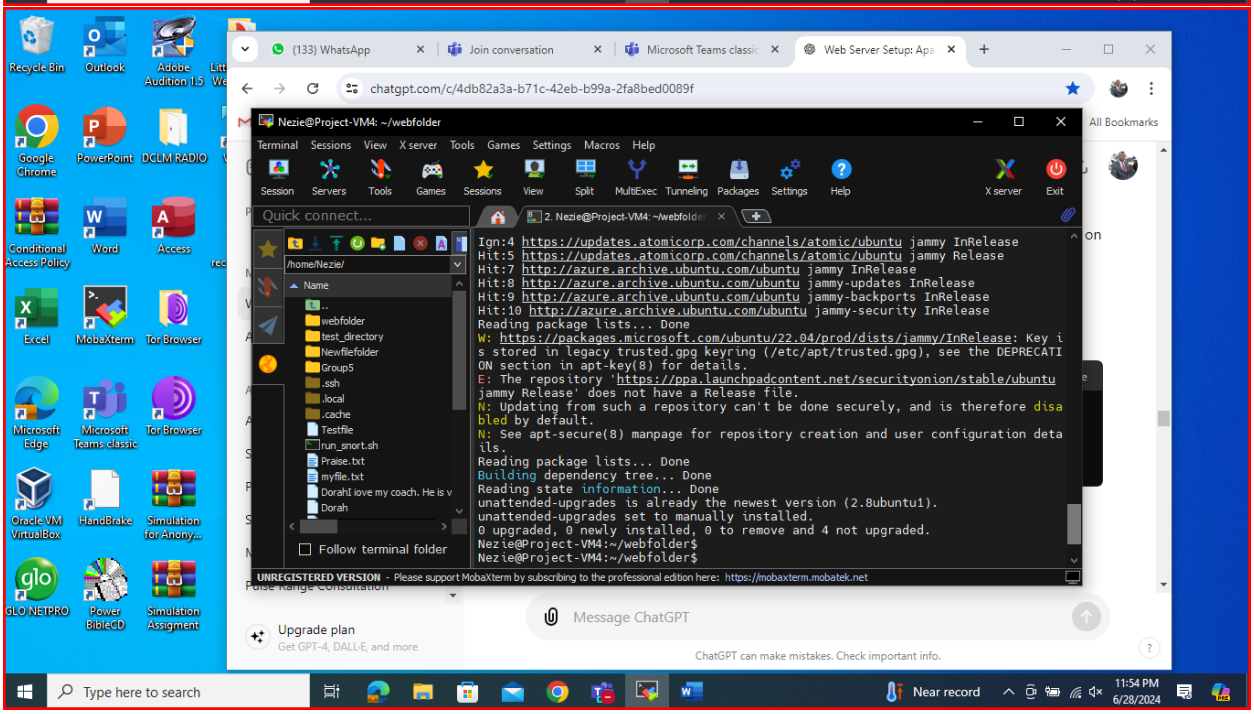


Configuring Automatic System Updates

For automatic system updates, the `unattended-upgrades` package on Debian/Ubuntu-based systems was used. Here's how it was set it up to run every Sunday at 3 p.m.

1. Unattended Upgrades were installed:
   sudo apt update
   sudo apt install unattended-upgrades
   sudo dpkg-reconfigure --priority=low unattended-upgrades





2. **Configure the Updates Schedule:**

Creating the following script: sudo nano /etc/apt/apt.conf.d/20auto-upgrades

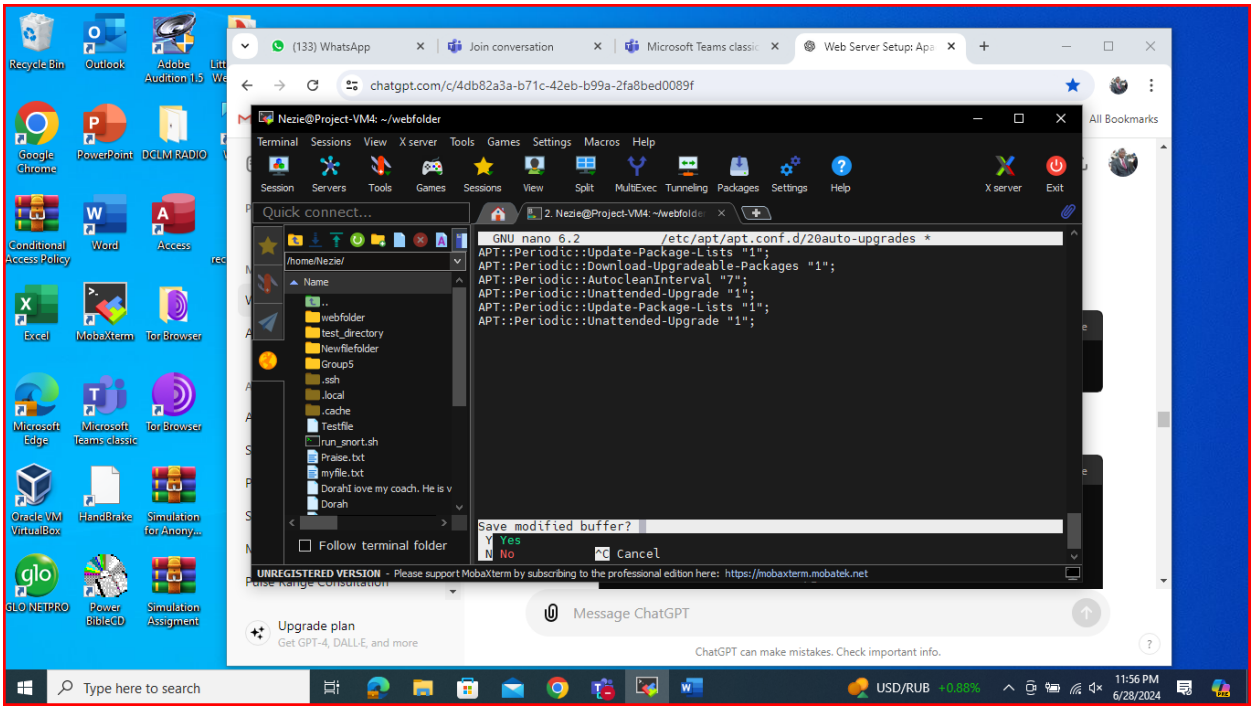
And the following lines were added

APT::Periodic::Update-Package-Lists "1";

APT::Periodic::Download-Upgradeable-Packages "1";

APT::Periodic::AutocleanInterval "7";

APT::Periodic::Unattended-Upgrade "1";



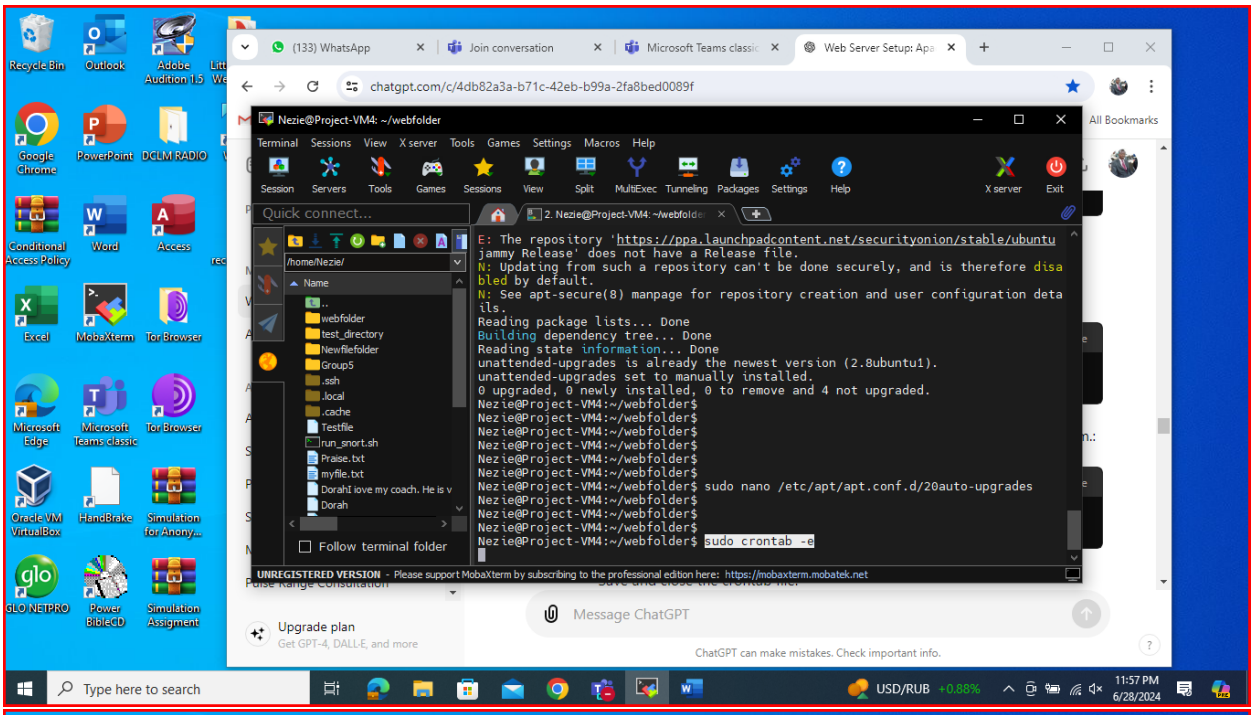
Create a Cron Job for Automatic Updates:

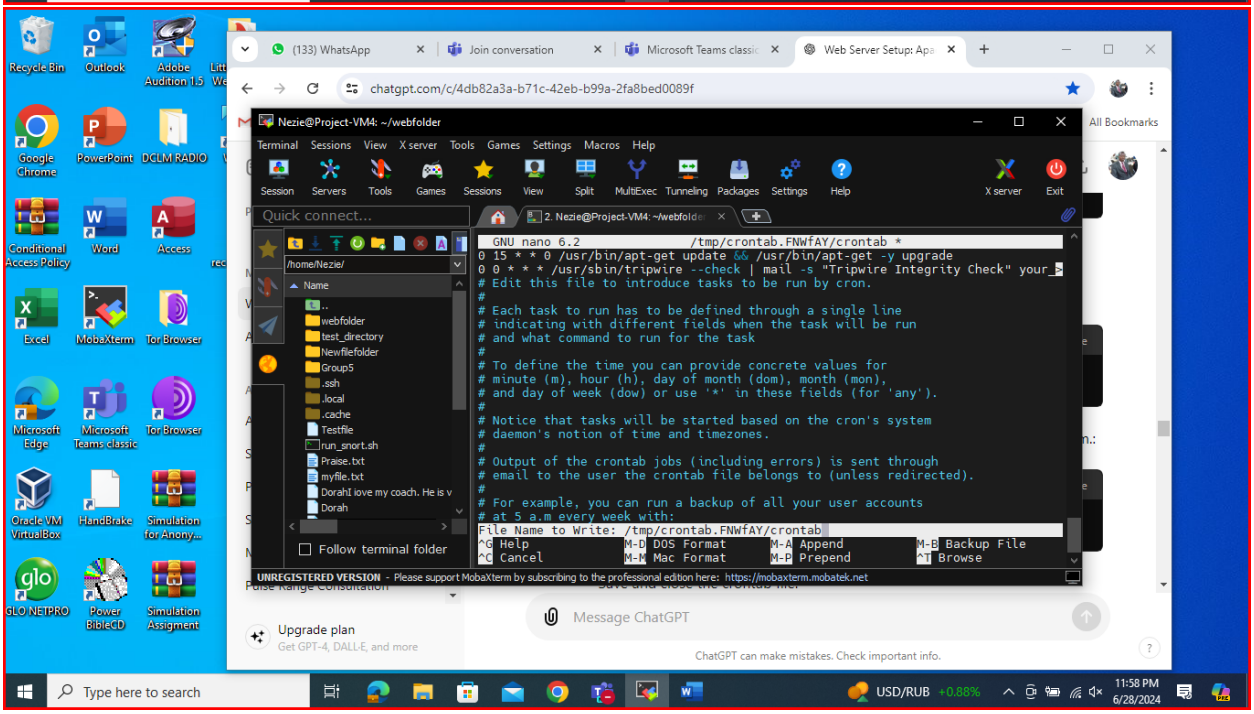
The root user's crontab was opened:

sudo crontab -e

The following line was added to schedule the updates to run every Sunday at 3 p.m.:

0 15 * * 0 /usr/bin/apt-get update && /usr/bin/apt-get -y upgrade


Nezie@Project-VM4: ~/webfolder
E: The repository 'https://ppa.launchpadcontent.net/securityonion/stable/ubuntu jammy Release' does not have a Release file.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
unattended-upgrades is already the newest version (2.8ubuntu1).
unattended-upgrades set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
Nezie@Project-VM4:~/webfolder$
Nezie@Project-VM4:~/webfolder$ sudo nano /etc/apt/apt.conf.d/20auto-upgrades
Nezie@Project-VM4:~/webfolder$ sudo crontab -e
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Upgrade plan
Get GPT-4, DALL·E, and more
Message ChatGPT
ChatGPT can make mistakes. Check important info.
Type here to search
USD/RUB +0.88%
11:57 PM
6/28/2024


GNU nano 6.2 /tmp/crontab.FNWfAY/crontab *
0 15 * * 0 /usr/bin/apt-get update && /usr/bin/apt-get -y upgrade
0 0 * * * /usr/sbin/tripwire --check | mail -s "Tripwire Integrity Check" your
Edit this file to introduce tasks to be run by cron.
Each task to run has to be defined through a single line
indicating with different fields when the task will be run
and what command to run for the task
To define the time you can provide concrete values for
minute (m), hour (h), day of month (dom), month (mon),
and day of week (dow) or use '*' in these fields (for 'any').
Notice that tasks will be started based on the cron's system
daemon's notion of time and timezones.
Output of the crontab jobs (including errors) is sent through
email to the user the crontab file belongs to (unless redirected).
For example, you can run a backup of all your user accounts
at 5 a.m every week with:
File Name to Write: /tmp/crontab.FNWfAY/crontab
^G Help M-D DOS Format M-A Append M-B Backup File
^C Cancel M-M Mac Format M-P Prepend ^T Browse
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Upgrade plan
Get GPT-4, DALL·E, and more
Message ChatGPT
ChatGPT can make mistakes. Check important info.
Type here to search
USD/RUB +0.88%
11:58 PM
6/28/2024

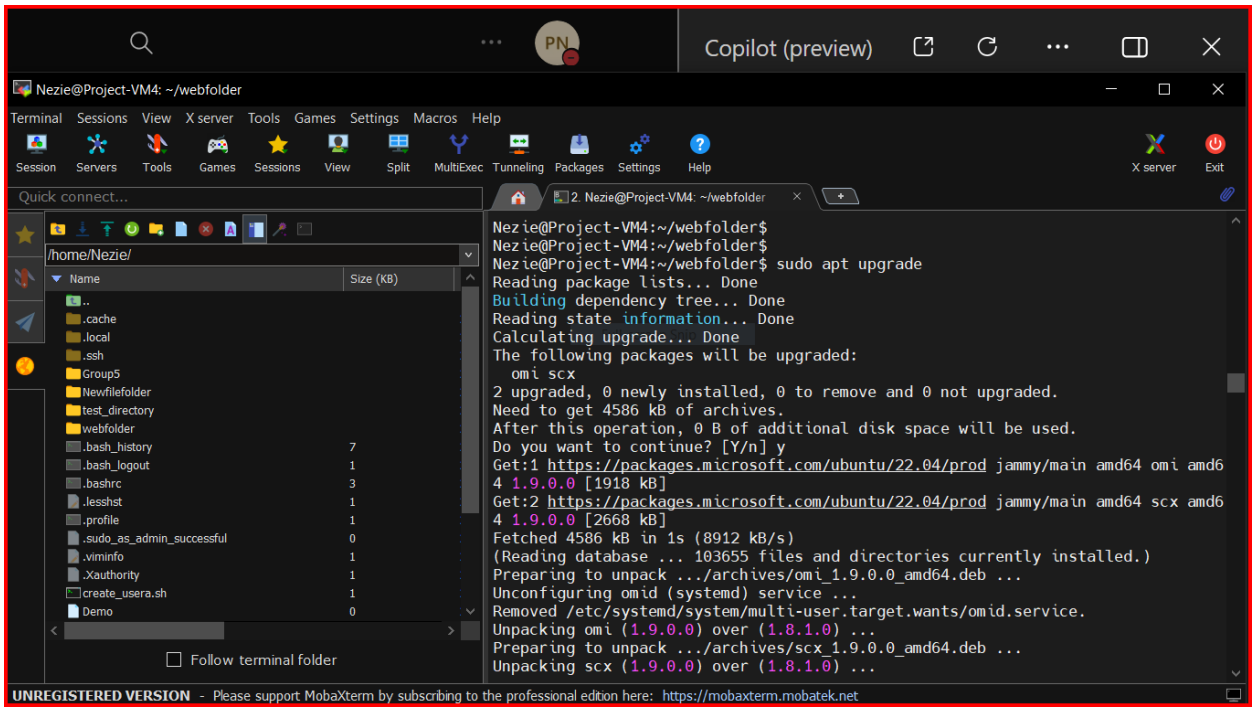
TASK 5: Monitoring Linux Web Server with Nagios

The following steps were taken:

1. Install and Configure Nagios:

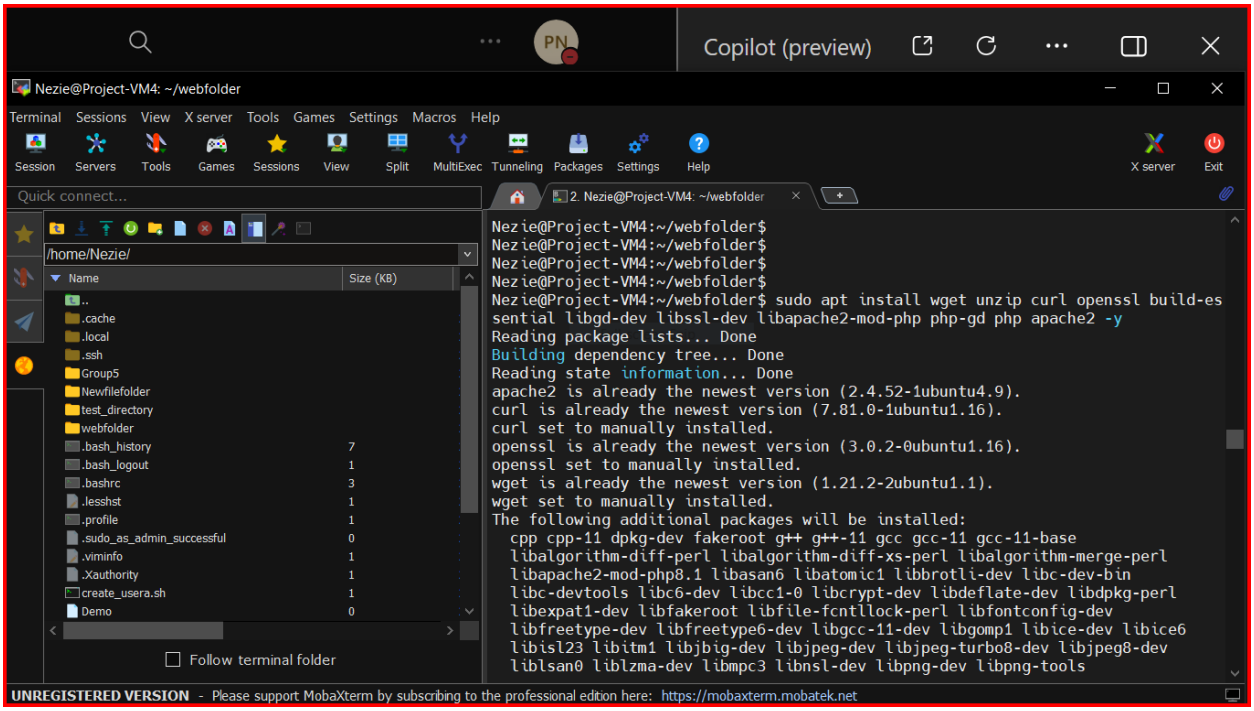
1. **Install Required Packages:**

Updating the system: `sudo apt update`



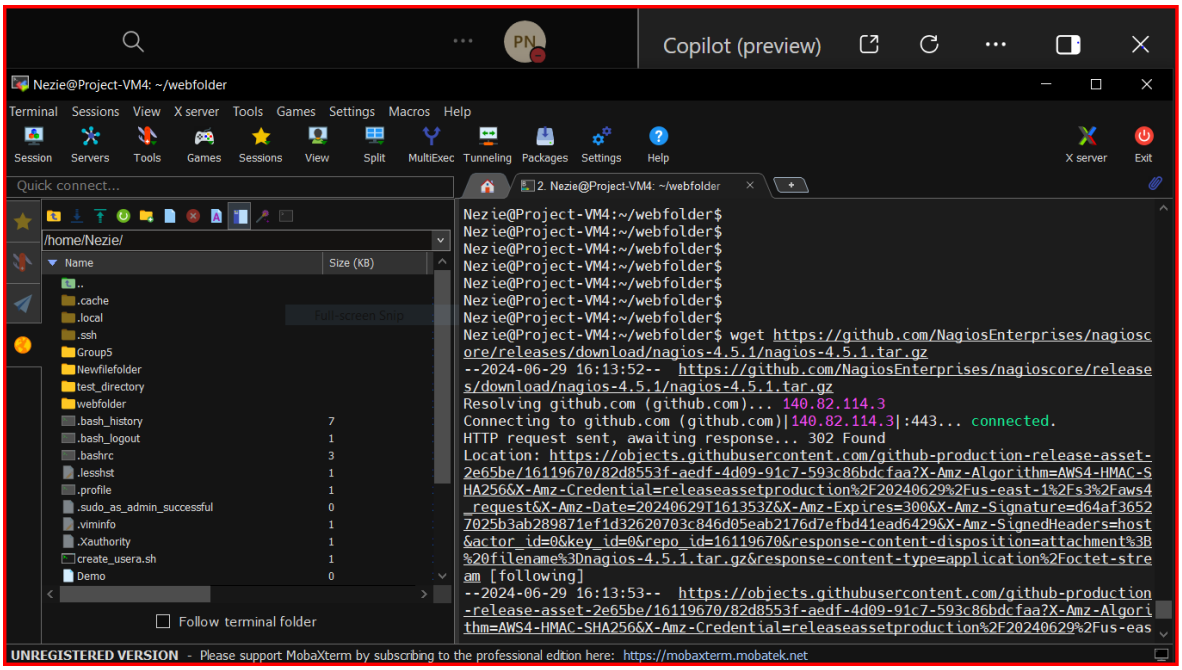
Installing necessary packages:

```
sudo apt install wget unzip curl openssl build-essential libgd-dev libssl-dev
libapache2-mod-php php-gd php apache2 -y
```



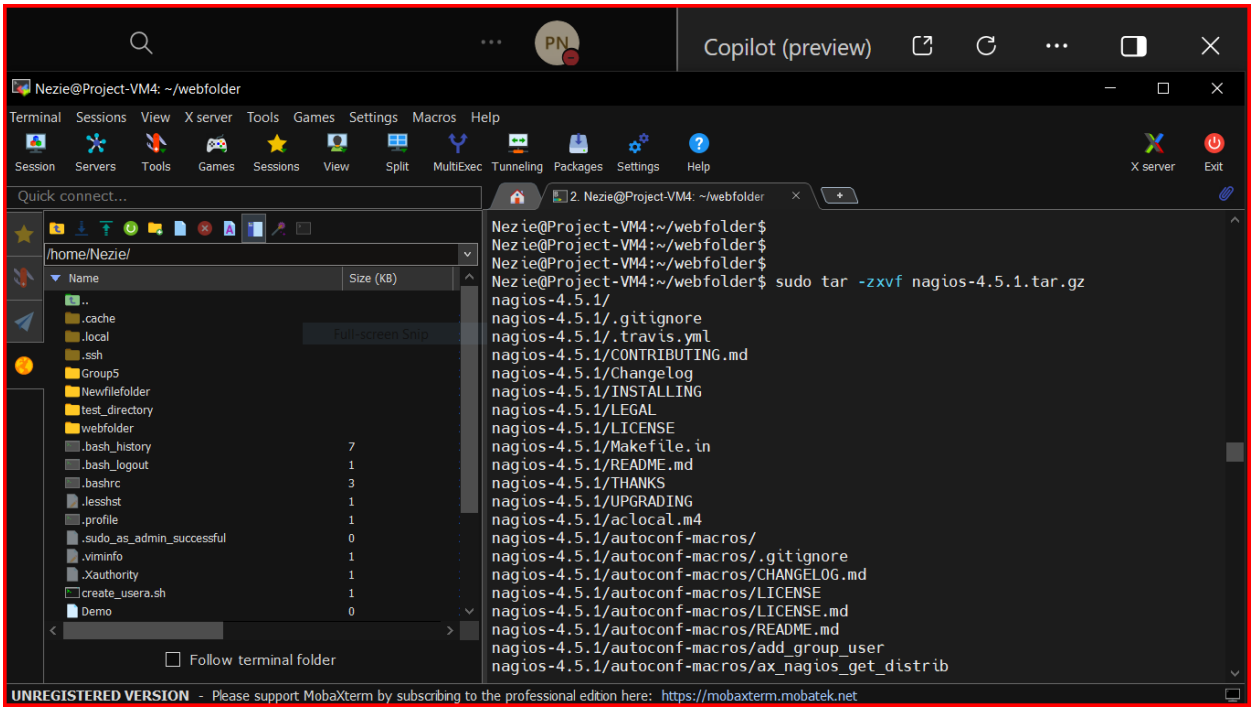
2. **Downloading Nagios Core**
   Download the latest Nagios Core setup files:

```
wget
https://github.com/NagiosEnterprises/nagioscore/releases/download/nagios-4.5.1/nagios-4.5.1.tar.gz
```



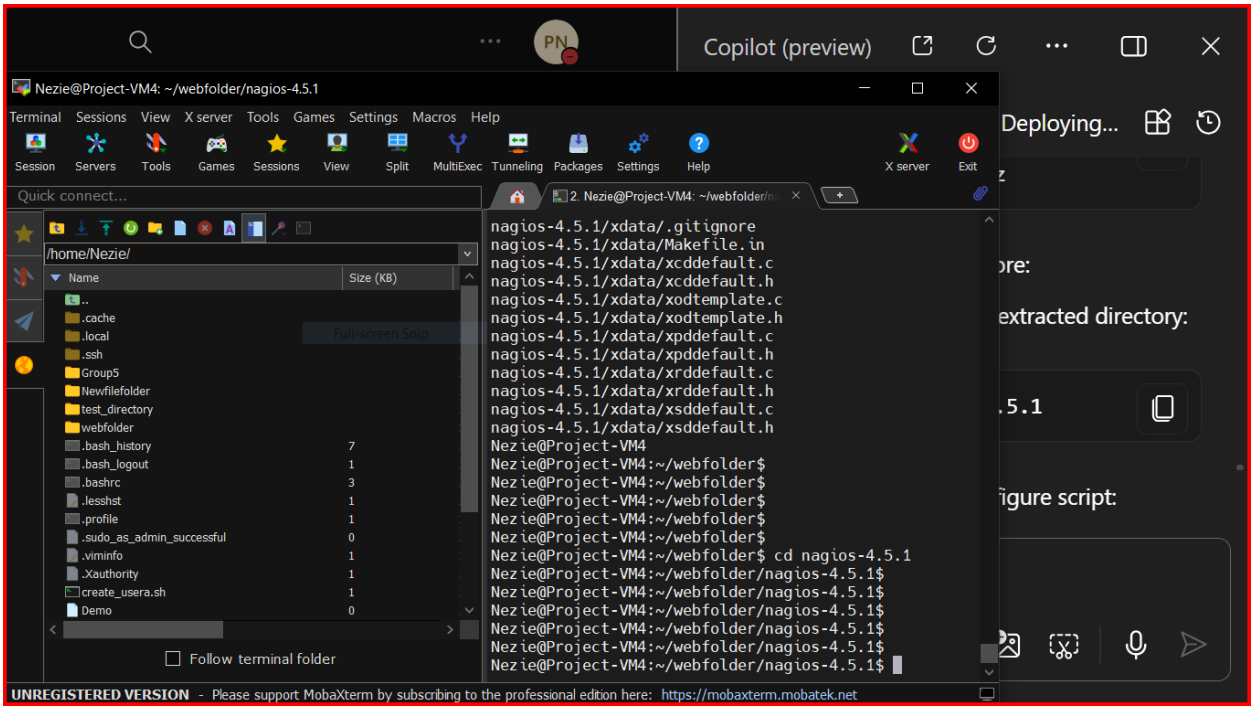
Extracting the downloaded files:

```
sudo tar -zxvf nagios-4.5.1.tar.gz
```

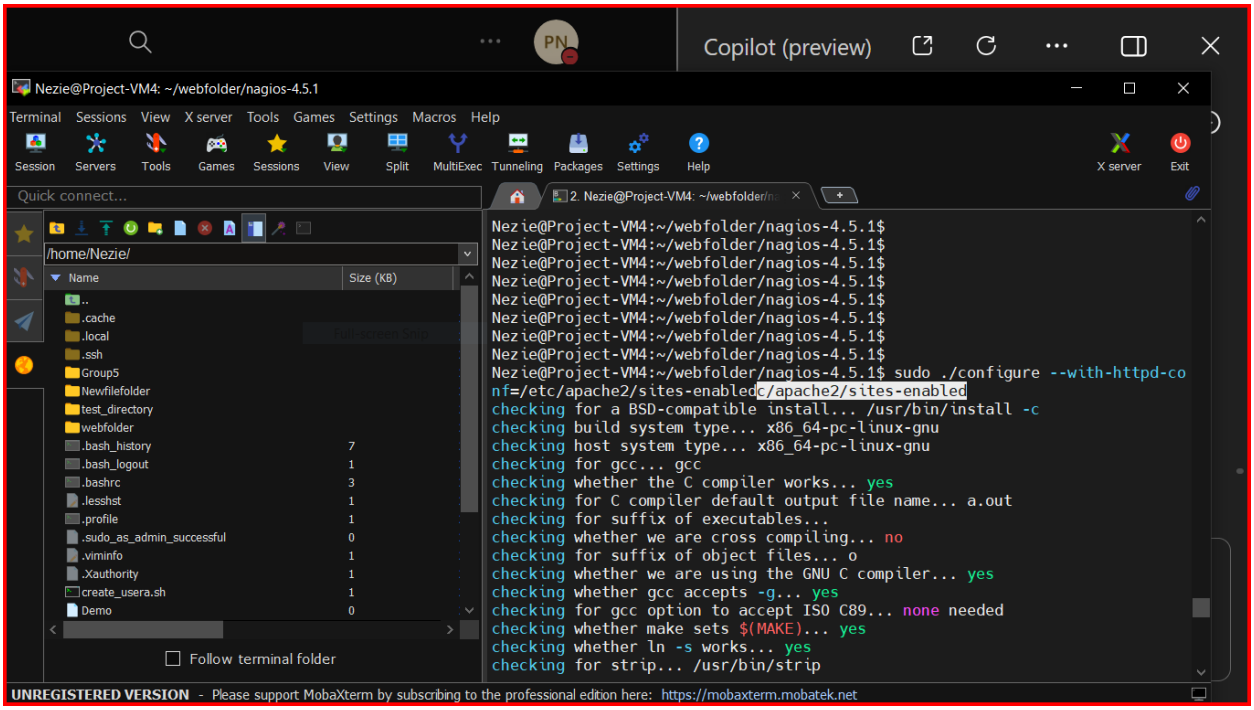


3. **Configure Nagios Core:**
   Navigate to the extracted directory:

```
cd nagios-4.5.1
```

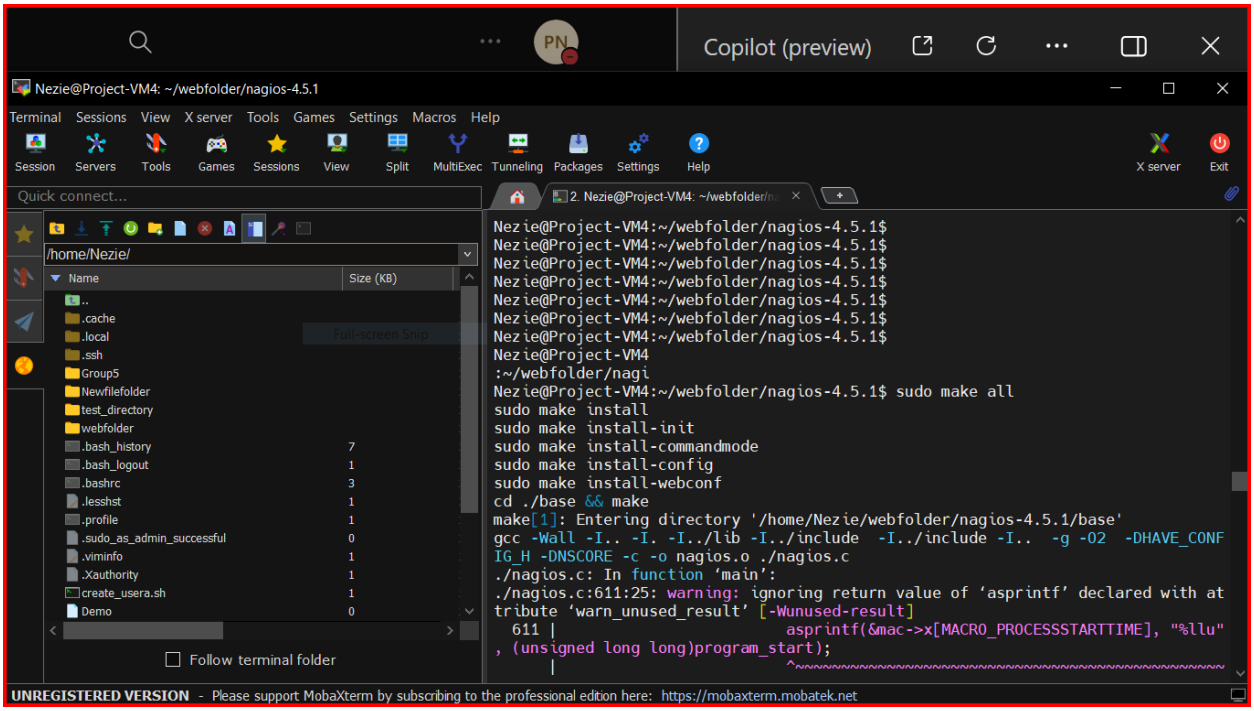


Execute the configure script: `sudo ./configure --with-httpd-conf=/etc/apache2/sites-enabled`



4. **Compile and Install Nagios:**

```
sudo make all
sudo make install
sudo make install-init
sudo make install-commandmode
sudo make install-config
sudo make install-webconf
```



5. **Create Nagios Admin User:**
   Set the Nagios admin password:

   ```
   sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
   ```