Gurjot S Khakh

Professor Torres

10/02/2025

IT 100

Lab: 7

- Copy parts A, B, and C from Canvas

Part A:

- **What are the symptoms that tell you something is wrong with the below, and how do you troubleshoot and fix it:**
  - RAM
  - CPU
  - Power Supply
  - Storage Drives

- RAM
  - Frequent Crashes & Restarts
  - Blue Screen of Death (BSOD)
  - Freezing or Lockups
  - Corrupted Files
  - Failure to Boot
  - Memory Errors in Applications
- Fixies
  - Reseat the RAM
  - Test RAM Using Diagnostic Tools
  - Test One Stick at a Time
  - Check BIOS/UEFI
  - Use Task Manager or Resource Monitor
- CPU
  - System Won't Boot
  - Overheating / High Temperatures
  - Frequent Freezing or Crashing
  - BSODs with CPU-Related Error Codes
  - Extremely Slow Performance
  - Boot Looping or Instability
  - BIOS/UEFI Doesn't Detect CPU
- Fixies
  - Check POST and Beep Codes
  - Reseat the CPU

    - Check Cooling
    - Update BIOS/UEFI
    - Test With a Known-Good Setup
    - Run Stress Tests (if system is stable enough)
- Power supply
    - Computer Doesn’t Power On
    - Random Shutdowns or Restarts
    - BSODs or Crashing Under Load
    - Fans Spin but No Display
    - Burning Smell or Sparks
    - Buzzing or Clicking Sounds
    - Peripherals or Components Not Getting Power
    - Intermittent Booting / Boot Looping
- Fixies
    - Use the Paperclip Test
    - Check With a PSU Tester
    - Swap in a Known-Good PSU
    - Check Motherboard Debug LEDs or Beep Codes
    - Monitor Voltages in BIOS or Software
- Storage devices
    - Slow Boot or System Performance
    - Frequent Freezes, Crashes, or BSODs
    - Boot Loop or "No Boot Device Found" Error
    - Corrupted Files or Inaccessible Folders
    - Missing Drive in File Explorer or BIOS
    - Clicking, Grinding, or Beeping Noises
    - S.M.A.R.T. Warnings
- Fixies
    - Check Cables and Connections
    - Enter BIOS/UEFI
    - Run SMART Diagnostic Tools
    - Run CHKDSK (Windows) or fsck (Linux/macOS)
    - Use Disk Management (Windows) or Disk Utility (macOS)
    - Try the Drive in Another PC or Adapter
    - Clone the Drive

Part B:

- **What are the symptoms that tell you something is wrong with the below, and how do you troubleshoot and fix it:**
    - Video/Display issues
    - Wired networks
    - Wireless networks

- Video/Display
  - Black Screen
  - Distorted, Flickering, or Flashing Display
  - Lines or Artifacts on Screen
  - No Signal / "Input Not Detected"
  - Dim Display or Backlight Issues
  - Wrong Resolution or Scaling Issues
  - Blue Screen of Death (BSOD) related to graphics
- Fixies
  - Check Power & Connections
  - Try connecting the monitor to a different device
  - Look for BIOS splash screen when turning on the PC.
  - Switch Display Modes
  - Driver Checks
  - Check for Overheating
  - Hardware Diagnosis
- Wired Networks
  - No Internet Connection
  - Intermittent Connection
  - Slow Network Speeds
  - Unidentified Network
  - No Ethernet Detected
  - IP Address Conflict
  - Cannot Access Local Devices
  - No Link Light
- Fixies
  - Check Physical Connections
  - Check Network Status on the Device
  - Restart Devices
  - Run Built-in Troubleshooter
  - Check Device Manager (Windows)
  - Check IP Configuration
  - Firewall / Antivirus Checks
  - Test on Another Device
  - Try a Static IP

Part C:

- After listening to this week's lecture, what are some things that you can do right now to practice your troubleshooting skills?:

I think some things that I can do to practice my troubleshooting skills is search for youtube videos of people troubleshooting their problems of devices. Another way is to ask ChatGPT to give you a troubleshooting problem and keep on practicing like that. Creating intentional problems with devices and troubleshooting them to gain more practice even on old devices. VirtualBox installing OS and troubleshooting them to make them fully functional.

Part D: SierraLab Windows

SSH using Putty and your private key with your credentials onto 207.62.230.146, port 2222. Once in, ssh to the Windowsbox.com and answer the below questions. **Password is Computersrock1**. Provides screenshots as proof of your answer.

1. Use auditpol to get a category to display audit policies
2. use the doskey to get a history of commands ran
3. Run the attrib command. What does this show?
4. Run the assoc command. What those the assoc command do?
5. Run the command to display group policies
6. Run the command to update group policies
7. Use the help command and try to run the command to list the volume information
8. Use the help command to find the command to change the title of your command prompt
9. Use the help command to find and run the command to list out the disk partitions
10. Run the check disk command from within the help center, and screenshot the output

```
hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        Success and Failure
  IPsec Driver                            No Auditing
  Other System Events                     Success and Failure
  Security State Change                   Success
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success
  Account Lockout                         Success
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           Success
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   Success and Failure
  User / Device Claims                    No Auditing
  Group Membership                        No Auditing
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
  Sensitive Privilege Use                 No Auditing
Detailed Tracking
  Process Creation                        No Auditing
  Process Termination                     No Auditing
  DPAPI Activity                          No Auditing
  RPC Events                              No Auditing
  Plug and Play Events                    No Auditing
  Token Right Adjusted Events             No Auditing
Policy Change
  Audit Policy Change                     Success
  Authentication Policy Change            Success
  Authorization Policy Change             No Auditing
  MPSSVC Rule-Level Policy Change         No Auditing
  Filtering Platform Policy Change        No Auditing
  Other Policy Change Events              No Auditing
```

Commented [GK1]: ran the command and this is the output I got

```
hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>auditpol /list /category
Category/Subcategory
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System

hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>
```

Commented [GK2]: I also ran this command which gives all audit policy categories

```
hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>doskey /history
auditpol
cls
auditpol /get /category:*
auditpol /list /category:*
audit /list /category:*
auditpol /list /category
cls
auditpol /get /category:*
auditpol /list /category:*
cls
auditpol /list /category:*
cls
auditpol /get /catefory:*
cls
auditpol /get /category:*
auditpol /list /category:*
cls
auditpol /get /category:*
auditpol /list /category:*
auditpol /list /category
cls
auditpol /list /category
doskey
cls
doskey /history
doskey /history cls
cls
dos /history
cls
doskey /hsitory
doskey /history
cls
doskey /history
```

Commented [GK3]: ran the command and also found that if you want to save command history before closing you can run the command of doskey /history > history.txt

```
hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>attrib
A   H   I          C:\Users\it100student\NTUSER.DAT
A  SH              C:\Users\it100student\ntuser.dat.LOG1
A  SH              C:\Users\it100student\ntuser.dat.LOG2
A  SH              C:\Users\it100student\NTUSER.DAT{c76cbcdb-afc9-11eb-8234-000d3aa6d50e}.TM.blf
A  SH              C:\Users\it100student\NTUSER.DAT{c76cbcdb-afc9-11eb-8234-000d3aa6d50e}.TMContainer00000000000000000001.regtrans-ms
A  SH              C:\Users\it100student\NTUSER.DAT{c76cbcdb-afc9-11eb-8234-000d3aa6d50e}.TMContainer00000000000000000002.regtrans-ms
A  SH              C:\Users\it100student\ntuser.ini

hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>
```

Commented [GK4]: this shows the list of files and folders in current directory with their attribute flags
A=Archive
H=Hidden
I= not content indexed
S= System

```
hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>assoc
.386=vxdfile
.3g2=WMP11.AssocFile.3G2
.3gp=WMP11.AssocFile.3GP
.3gp2=WMP11.AssocFile.3G2
.3gpp=WMP11.AssocFile.3GP
.5vw=wireshark-capture-file
.aac=WMP11.AssocFile.ADTS
.accountpicture-ms=accountpicturefile
.acp=wireshark-capture-file
.adt=WMP11.AssocFile.ADTS
.adts=WMP11.AssocFile.ADTS
.aif=WMP11.AssocFile.AIFF
.aifc=WMP11.AssocFile.AIFF
.aiff=WMP11.AssocFile.AIFF
.ani=anifile
.apc=wireshark-capture-file
.appcontent-ms=ApplicationContent
.application=Application.Manifest
.appref-ms=Application.Reference
.asa=aspfile
.asf=WMP11.AssocFile.ASF
.asp=aspfile
.asx=WMP11.AssocFile.ASX
.atc=wireshark-capture-file
.au=WMP11.AssocFile.AU
.avi=WMP11.AssocFile.AVI
.bat=batfile
.bfr=wireshark-capture-file
.blg=Diagnostic.Perfmon.Document
.bmp=Paint.Picture
.cab=CABFolder
.camp=campfile
.cap=wireshark-capture-file
.cat=CATFile
.cda=WMP11.AssocFile.CDA
.cdmp=cdmpfile
.cdx=aspfile
.cdxml=Microsoft.PowerShellCmdletDefinitionXML.1
.cer=CERFile
.chk=chkfile
.chm=chm.file
.cmd=cmdfile
.com=comfile
.compositefont=Windows.CompositeFont
.cpl=cplfile
.crl=CRLFile
.crt=CERFile
.css=CSSfile
.cur=curfile
.db=dbfile
.dctx=IMEDictionaryCompiler
.dctxc=IMEDictionaryCompiler
.dds=ddsfile
```

Commented [GK5]: assoc command is used to view and change file extensions associations.

```
hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>gpresult

GPRESULT [/S system [/U username [/P [password]]]] [/SCOPE scope]
         [/USER targetusername] [/R | /V | /Z] [(/X | /H) <filename> [/F]]

Description:
    This command line tool displays the Resultant Set of Policy (RSoP)
    information for a target user and computer.

Parameter List:
    /S        system           Specifies the remote system to connect to.

    /U        [domain\]user    Specifies the user context under which the
                               command should run.
                               Can not be used with /X, /H.

    /P        [password]       Specifies the password for the given user
                               context. Prompts for input if omitted.
                               Cannot be used with /X, /H.

    /SCOPE    scope            Specifies whether the user or the
                               computer settings need to be displayed.
                               Valid values: "USER", "COMPUTER".

    /USER     [domain\]user    Specifies the user name for which the
                               RSoP data is to be displayed.

    /X        <filename>       Saves the report in XML format at the
                               location and with the file name specified
                               by the <filename> parameter. (valid in Windows
                               Vista SP1 and later and Windows Server 2008 and later)

    /H        <filename>       Saves the report in HTML format at the
                               location and with the file name specified by
                               the <filename> parameter. (valid in Windows
                               at least Vista SP1 and at least Windows Server 2008)

    /F                         Forces Gpresult to overwrite the file name
                               specified in the /X or /H command.

    /R                         Displays RSoP summary data.

    /V                         Specifies that verbose information should
                               be displayed. Verbose information provides
                               additional detailed settings that have
                               been applied with a precedence of 1.

    /Z                         Specifies that the super-verbose
                               information should be displayed. Super-
                               verbose information provides additional
                               detailed settings that have been applied
                               with a precedence of 1 and higher. This
                               allows you to see if a setting was set in
                               multiple places. See the Group Policy
```

Commented [GK6]: another command that can be run is gpresult /r which gives a summary of RSoP data

```
hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>gpupdate
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.


hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>gpupdate /target:computer
Updating policy...

Computer Policy update has completed successfully.


hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>gpupdate /target:user
Updating policy...

User Policy update has completed successfully.


hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.


hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>
```

Commented [GK7]: the main command is gpupdate to update group polices but to target only the computer or the user you put /target:computer or /target:user, another one is gpupdate /force which Forces Reapplication of All Policies (even if unchanged)

```
               correctly to a disk.
VOL            Displays a disk volume label and serial number.
XCOPY          Copies files and directory trees.
WMIC           Displays WMI information inside interactive command shell.

For more information on tools see the command-line reference in the online help.

hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>vol
 Volume in drive C has no label.
 Volume Serial Number is 4C3A-51E5
```

Commented [GK8]: first ran the help command and then found the command to list volume information

```
TITLE          Sets the window title for a CMD.EXE session.
TREE           Graphically displays the directory structure of a drive or
               path.
TYPE           Displays the contents of a text file.
VER            Displays the Windows version.
VERIFY         Tells Windows whether to verify that your files are written
               correctly to a disk.
VOL            Displays a disk volume label and serial number.
XCOPY          Copies files and directory trees.
WMIC           Displays WMI information inside interactive command shell.

For more information on tools see the command-line reference in the online help.

hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>title Kali Linux

hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>
```

Commented [GK9]: ran help command then found title command and renamed CMD to Kali linux by title Kali Linux

```
hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>diskpart

Microsoft DiskPart version 10.0.20348.1

Copyright (C) Microsoft Corporation.
On computer: HIDDENLEAF

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          100 GB    35 GB
```

Commented [GK10]: ran help command then found diskpart command and within diskpart ran list disk which listed the disk partitions

```
hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>chkdsk
The type of the file system is NTFS.

WARNING!  /F parameter not specified.
Running CHKDSK in read-only mode.

Stage 1: Examining basic file system structure ...
  288256 file records processed.
File verification completed.
 Phase duration (File record verification): 34.34 seconds.
  11108 large file records processed.
 Phase duration (Orphan file record recovery): 0.00 milliseconds.
  0 bad file records processed.
 Phase duration (Bad file record checking): 0.76 milliseconds.

Stage 2: Examining file name linkage ...
  1251 reparse records processed.
  429794 index entries processed.
Index verification completed.
 Phase duration (Index verification): 1.18 minutes.
  0 unindexed files scanned.
 Phase duration (Orphan reconnection): 374.82 milliseconds.
  0 unindexed files recovered to lost and found.
 Phase duration (Orphan recovery to lost and found): 0.70 milliseconds.
  1251 reparse records processed.
 Phase duration (Reparse point and Object ID verification): 8.50 milliseconds.

Stage 3: Examining security descriptors ...
Security descriptor verification completed.
 Phase duration (Security descriptor verification): 127.18 milliseconds.
  70770 data files processed.
 Phase duration (Data attribute verification): 0.66 milliseconds.
CHKDSK is verifying Usn Journal...
  544784368 USN bytes processed.
Usn Journal verification completed.
 Phase duration (USN journal verification): 4.23 seconds.

Windows has scanned the file system and found no problems.
No further action is required.

  67417087 KB total disk space.
  28491956 KB in 182993 files.
    151324 KB in 70771 indexes.
         0 KB in bad sectors.
    890167 KB in use by the system.
     65536 KB occupied by the log file.
  37883640 KB available on disk.

      4096 bytes in each allocation unit.
  16854271 total allocation units on disk.
   9470910 allocation units available on disk.
Total duration: 1.83 minutes (110396 ms).
```

Commented [GK11]: this is the output I got after running the chkdsk command

Part E: SierraLab Linux

SSH using Putty and your private key with your credentials onto 207.62.230.146, port 2222. Once in, ssh to the Linuxbox.com and answer the below questions. **Password is Computersrock1**. Provides screenshots as proof of your answer.

1: type the command to show the first few lines of the journalctl output

2: type the command to show the last few lines of the journalctl output

3: type the command to show journalctl output in real time

4: how much disk usage in the journalctl using

5: what version of the journalctl are you using

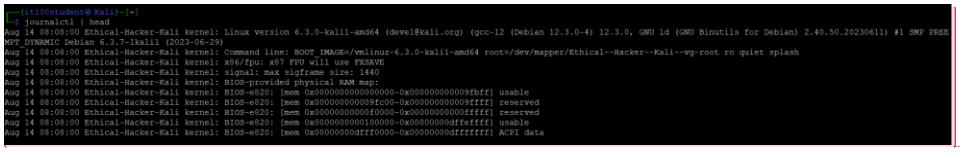
6: run the journalctl and list all ports referenced

7: run the journalctl and list all user activity except root

8: run the journalctl and list out all errors detected

9: Using the journalctl, what issues does the system have

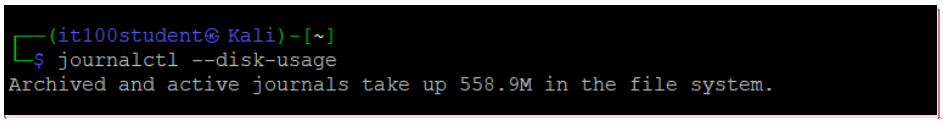
10: Using the journalctl, search only for "Listening". What are you seeing



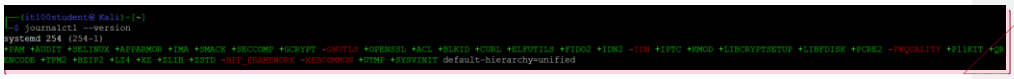
Commented [GK12]: journalctl | head limits the output to the first 10 outputs

Commented [GK13]: journalctl | tail gives the last 10 outputs of the journalctl command

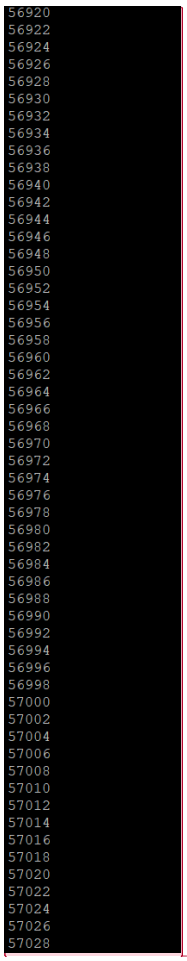
Commented [GK14]: the command is journalctl -f which means follow the new outputs in real time



Commented [GK15]: 558.9m it takes up

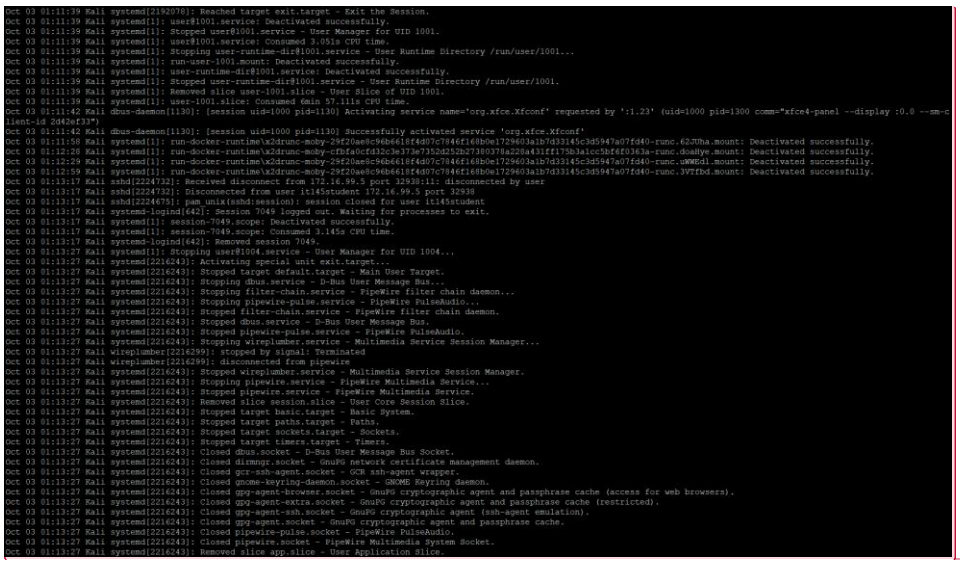


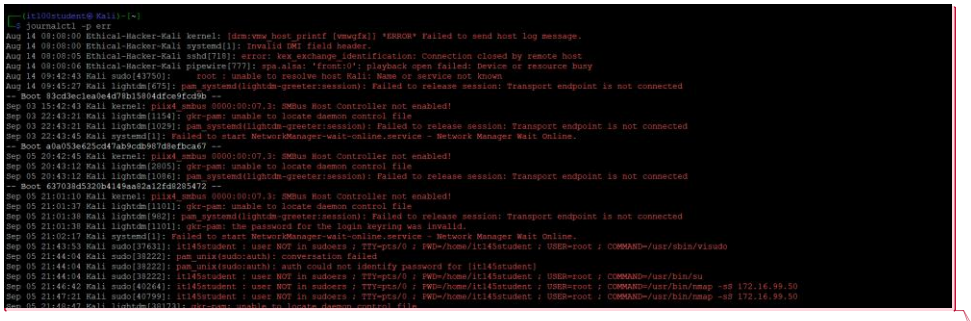
Commented [GK16]: ran journalctl --version and gave me this output and the version is 254(254-1)

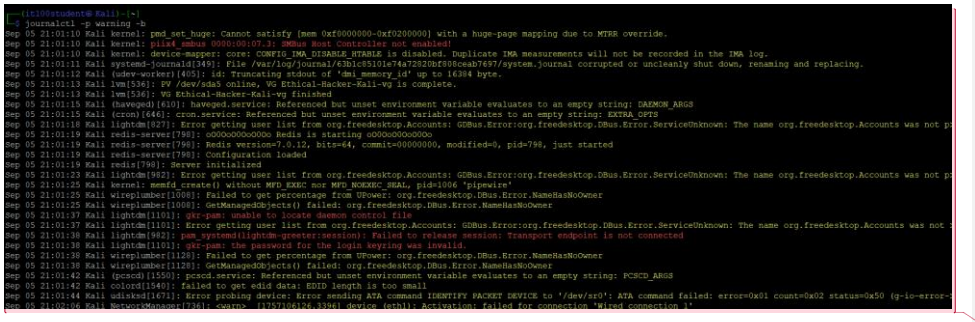


Commented [GK17]: I ran the command of journalctl | grep -Eo 'port [0-9]+' | awk '{print $2}' | sort -n | uniq. which this means it to grab the ports that journalctl is using then print them and put them in numerical order and then get rid of duplicates

Commented [GK18]: 56920
56922
56924
56926
56928
56930
56932
56934
56936
56938
56940
56942
56944
56946
56948
56950
56952
56954
56956
56958
56960
56962
56964
56966
56968
56970
56972
56974
56976
56978
56980
56982
56984
56986
56988
56990
56992
56994
56996
56998
57000
57002
57004
57006
57008
57010
57012
57014
57016
57018
57020
57022
57024
57026
57028
57030
57032
57034
57036
...







Commented [GK19]: ran the command of journalctl | grep -v "\broot\b' which excludes any root and only lists user activity

Commented [GK20]: Oct 03 01:13:28 Kali systemd[1]: user@1004.service: Deactivated successfully.
Oct 03 01:13:28 Kali systemd[1]: Stopped user@1004.service - User Manager for UID 1004.
Oct 03 01:13:28 Kali systemd[1]: user@1004.service: Consumed 2.184s CPU time.
Oct 03 01:13:28 Kali systemd[1]: Stopping user-runtime-dir@1004.service - User Runtime Directory /run/user/1004...
Oct 03 01:13:28 Kali systemd[1]: run-user-1004.mount: Deactivated successfully.
Oct 03 01:13:28 Kali systemd[1]: user-runtime-dir@1004.service: Deactivated successfully.
Oct 03 01:13:28 Kali systemd[1]: Stopped user-runtime-dir@1004.service - User Runtime Directory /run/user/1004.
Oct 03 01:13:28 Kali systemd[1]: Removed slice user-1004.slice - User Slice of UID 1004.
Oct 03 01:13:28 Kali systemd[1]: user-1004.slice: Consumed 6.849s CPU time.
Oct 03 01:13:29 Kali systemd[1]: run-docker-runtime\x2drunc-moby-29f20ae8c96b6618f4d07c7846f168b0e1729603a1b7d33145c3d5947a07fd40-runc.PrIeba.mount: Deactivated successfully.
Oct 03 01:13:59 Kali systemd[1]: run-docker-runtime\x2drunc-moby-cfbfa0cfd32c3e373e7352d252b27380378a228a431ff175b3a1cc5bf6f0363a-runc.P98ik6.mount: Deactivated successfully.
Oct 03 01:14:00 Kali systemd[1]: run-docker-runtime\x2drunc-moby-29f20ae8c96b6618f4d07c7846f168b0e1729603a1b7d33145c3d5947a07fd40-runc.O6emCR.mount: Deactivated successfully.
Oct 03 01:14:29 Kali systemd[1]: run-docker-runtime\x2drunc-moby-cfbfa0cfd32c3e373e7352d252b27380378a228a431ff175b3a1cc5bf6f0363a-runc.H0aCVJ.mount: Deactivated successfully.
Oct 03 01:14:29 Kali systemd[1]: run-docker-runtime\x2drunc-moby-29f20ae8c96b6618f4d07c7846f168b0e1729603a1b7d33145c3d5947a07fd40-runc.Y5KjfX.mount: Deactivated successfully.

Commented [GK21]: ran journalctl -p err which lists out all the errors

Commented [GK22]: Aug 14 08:08:00 Ethical-Hacker-Kali kernel: [drm:vmw_host_printf [vmwgfx]] *ERROR* Failed to send host log message.
Aug 14 08:08:00 Ethical-Hacker-Kali systemd[1]: Invalid DMI field header.
Aug 14 08:08:05 Ethical-Hacker-Kali sshd[718]: error: kex_exchange_identification: Connection closed by remote host
Aug 14 08:08:06 Ethical-Hacker-Kali pipewire[777]: spa.alsa: 'front:0': playback open failed: Device or resource busy

Commented [GK23]: ran journalctl -p warning -b which gives the warnings that are given

```
┌──(it100student㉿Kali)-[~]
└─$ journalctl -p err -b
Sep 05 21:01:10 Kali kernel: piix4_smbus 0000:00:07.3: SMBus Host Controller not enabled!
Sep 05 21:01:37 Kali lightdm[1101]: gkr-pam: unable to locate daemon control file
Sep 05 21:01:38 Kali lightdm[982]: pam_systemd(lightdm-greeter:session): Failed to release session: Transport endpoint is not connected
Sep 05 21:01:38 Kali lightdm[1101]: gkr-pam: the password for the login keyring was invalid.
Sep 05 21:02:17 Kali systemd[1]: Failed to start NetworkManager-wait-online.service - Network Manager Wait Online.
Sep 05 21:43:53 Kali sudo[37631]: it145student : user NOT in sudoers ; TTY=pts/0 ; PWD=/home/it145student ; USER=root ; COMMAND=/usr/sbin/visudo
Sep 05 21:44:04 Kali sudo[38222]: pam_unix(sudo:auth): conversation failed
Sep 05 21:44:04 Kali sudo[38222]: pam_unix(sudo:auth): auth could not identify password for [it145student]
Sep 05 21:44:04 Kali sudo[38222]: it145student : user NOT in sudoers ; TTY=pts/0 ; PWD=/home/it145student ; USER=root ; COMMAND=/usr/bin/su
Sep 05 21:46:42 Kali sudo[40264]: it145student : user NOT in sudoers ; TTY=pts/0 ; PWD=/home/it145student ; USER=root ; COMMAND=/usr/bin/nmap -sS 172.16.99.50
Sep 05 21:47:21 Kali sudo[40799]: it145student : user NOT in sudoers ; TTY=pts/0 ; PWD=/home/it145student ; USER=root ; COMMAND=/usr/bin/nmap -sS 172.16.99.50
Sep 05 21:48:47 Kali lightdm[38173]: gkr-pam: unable to locate daemon control file
Sep 05 21:48:47 Kali lightdm[37969]: pam_systemd(lightdm-greeter:session): Failed to release session: Transport endpoint is not connected
Sep 05 22:09:10 Kali lightdm[54510]: gkr-pam: unable to locate daemon control file
Sep 05 22:09:11 Kali lightdm[54336]: pam_systemd(lightdm-greeter:session): Failed to release session: Transport endpoint is not connected
Sep 10 04:19:47 Kali sudo[94954]: pam_unix(sudo:auth): conversation failed
Sep 10 04:19:47 Kali sudo[94954]: pam_unix(sudo:auth): auth could not identify password for [it145student]
Sep 10 04:19:47 Kali sudo[94954]: it145student : command not allowed ; TTY=pts/0 ; PWD=/home/it145student ; USER=root ; COMMAND=/usr/bin/cat /var/lib/dhcp/dhclient*.leases
Sep 10 04:20:41 Kali sudo[95428]: it145student : command not allowed ; TTY=pts/0 ; PWD=/home/it145student ; USER=root ; COMMAND=/usr/bin/cat /var/lib/dhcp/dhclient*.leases
Sep 10 04:21:43 Kali sudo[96181]: it145student : command not allowed ; TTY=pts/0 ; PWD=/home/it145student ; USER=root ; COMMAND=/usr/bin/cat /var/lib/dhcp/dhclient*.leases
Sep 11 03:13:29 Kali sshd[1040402]: fatal: Timeout before authentication for 172.16.99.5 port 59686
Sep 11 03:41:18 Kali sshd[1059530]: fatal: Timeout before authentication for 172.16.99.5 port 43420
Sep 11 21:12:04 Kali dhclient[1786471]: can't create /var/lib/dhcp/dhclient.leases: Permission denied
Sep 11 21:12:04 Kali dhclient[1786471]: Open a socket for LPF: Operation not permitted
Sep 11 21:12:04 Kali dhclient[1786471]:
Sep 11 21:12:04 Kali dhclient[1786471]: If you think you have received this message due to a bug rather
Sep 11 21:12:04 Kali dhclient[1786471]: than a configuration issue please read the section on submitting
Sep 11 21:12:04 Kali dhclient[1786471]: bugs on either our web page at www.isc.org or in the README file
Sep 11 21:12:04 Kali dhclient[1786471]: before submitting a bug.  These pages explain the proper
Sep 11 21:12:04 Kali dhclient[1786471]: process and the information we find helpful for debugging.
Sep 11 21:12:04 Kali dhclient[1786471]:
Sep 11 21:12:04 Kali dhclient[1786471]: exiting.
Sep 12 00:00:48 Kali sshd[1901856]: fatal: Timeout before authentication for 172.16.99.5 port 41366
Sep 12 00:42:55 Kali sudo[1933655]: it100student : command not allowed ; TTY=pts/0 ; PWD=/home/it100student ; USER=root ; COMMAND=/usr/bin/ls
Sep 12 00:45:14 Kali sudo[1935363]: it120student : command not allowed ; TTY=pts/3 ; PWD=/home/it120student ; USER=root ; COMMAND=lshw -short
Sep 12 01:27:04 Kali sudo[1966705]: it115student : command not allowed ; TTY=pts/0 ; PWD=/home/it115student ; USER=root ; COMMAND=/usr/bin/cat /var/lib/dhcp/dhclient.leases
Sep 12 01:28:38 Kali sudo[1967807]: it115student : command not allowed ; TTY=pts/0 ; PWD=/home/it115student ; USER=root ; COMMAND=/usr/bin/cat /var/lib/dhcp/dhclient.leases
Sep 12 06:01:58 Kali sudo[2157935]: it100student : command not allowed ; TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/bash
Sep 12 22:41:04 Kali sudo[2847158]: pam_unix(sudo:auth): conversation failed
Sep 12 22:41:04 Kali sudo[2847158]: pam_unix(sudo:auth): auth could not identify password for [it145student]
Sep 12 22:41:04 Kali sudo[2847158]: it145student : command not allowed ; TTY=pts/0 ; PWD=/home/it145student ; USER=root ; COMMAND=/usr/sbin/dhclient -v eth0
Sep 12 22:43:43 Kali dhclient[2849178]: can't create /var/lib/dhcp/dhclient.leases: Permission denied
Sep 12 22:43:43 Kali dhclient[2849178]: Open a socket for LPF: Operation not permitted
Sep 12 22:43:43 Kali dhclient[2849178]:
Sep 12 22:43:43 Kali dhclient[2849178]: If you think you have received this message due to a bug rather
Sep 12 22:43:43 Kali dhclient[2849178]: than a configuration issue please read the section on submitting
Sep 12 22:43:43 Kali dhclient[2849178]: bugs on either our web page at www.isc.org or in the README file
Sep 12 22:43:43 Kali dhclient[2849178]: before submitting a bug.  These pages explain the proper
Sep 12 22:43:43 Kali dhclient[2849178]: process and the information we find helpful for debugging.
Sep 12 22:43:43 Kali dhclient[2849178]:
Sep 12 22:43:43 Kali dhclient[2849178]: exiting.
```

Commented [GK24]: another one is journalctl -p err -b which only gives what is wrong no warnings

```
Oct 03 01:32:30 Kali systemd[2280750]: Listening on pipewire.socket - PipeWire Multimedia System Socket.
Oct 03 01:32:30 Kali systemd[2280750]: Listening on dbus.socket - D-Bus User Message Bus Socket.
Oct 03 03:46:33 Kali systemd[2373494]: Listening on dirmngr.socket - GnuPG network certificate management daemon.
Oct 03 03:46:33 Kali systemd[2373494]: Listening on gcr-ssh-agent.socket - GCR ssh-agent wrapper.
Oct 03 03:46:33 Kali systemd[2373494]: Listening on gnome-keyring-daemon.socket - GNOME Keyring daemon.
Oct 03 03:46:33 Kali systemd[2373494]: Listening on gpg-agent-browser.socket - GnuPG cryptographic agent and passphrase cache (access for web browsers).
Oct 03 03:46:33 Kali systemd[2373494]: Listening on gpg-agent-extra.socket - GnuPG cryptographic agent and passphrase cache (restricted).
Oct 03 03:46:33 Kali systemd[2373494]: Listening on gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation).
Oct 03 03:46:33 Kali systemd[2373494]: Listening on gpg-agent.socket - GnuPG cryptographic agent and passphrase cache.
Oct 03 03:46:33 Kali systemd[2373494]: Listening on pipewire-pulse.socket - PipeWire PulseAudio.
Oct 03 03:46:33 Kali systemd[2373494]: Listening on pipewire.socket - PipeWire Multimedia System Socket.
Oct 03 03:46:33 Kali systemd[2373494]: Listening on dbus.socket - D-Bus User Message Bus Socket.
Oct 03 03:51:16 Kali systemd[2376905]: Listening on dirmngr.socket - GnuPG network certificate management daemon.
Oct 03 03:51:16 Kali systemd[2376905]: Listening on gcr-ssh-agent.socket - GCR ssh-agent wrapper.
Oct 03 03:51:16 Kali systemd[2376905]: Listening on gnome-keyring-daemon.socket - GNOME Keyring daemon.
Oct 03 03:51:16 Kali systemd[2376905]: Listening on gpg-agent-browser.socket - GnuPG cryptographic agent and passphrase cache (access for web browsers).
Oct 03 03:51:16 Kali systemd[2376905]: Listening on gpg-agent-extra.socket - GnuPG cryptographic agent and passphrase cache (restricted).
Oct 03 03:51:16 Kali systemd[2376905]: Listening on gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation).
Oct 03 03:51:16 Kali systemd[2376905]: Listening on gpg-agent.socket - GnuPG cryptographic agent and passphrase cache.
Oct 03 03:51:16 Kali systemd[2376905]: Listening on pipewire-pulse.socket - PipeWire PulseAudio.
Oct 03 03:51:16 Kali systemd[2376905]: Listening on pipewire.socket - PipeWire Multimedia System Socket.
Oct 03 03:51:16 Kali systemd[2376905]: Listening on dbus.socket - D-Bus User Message Bus Socket.
Oct 03 04:01:00 Kali systemd[2383813]: Listening on dirmngr.socket - GnuPG network certificate management daemon.
Oct 03 04:01:00 Kali systemd[2383813]: Listening on gcr-ssh-agent.socket - GCR ssh-agent wrapper.
Oct 03 04:01:00 Kali systemd[2383813]: Listening on gnome-keyring-daemon.socket - GNOME Keyring daemon.
Oct 03 04:01:00 Kali systemd[2383813]: Listening on gpg-agent-browser.socket - GnuPG cryptographic agent and passphrase cache (access for web browsers).
Oct 03 04:01:00 Kali systemd[2383813]: Listening on gpg-agent-extra.socket - GnuPG cryptographic agent and passphrase cache (restricted).
Oct 03 04:01:00 Kali systemd[2383813]: Listening on gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation).
Oct 03 04:01:00 Kali systemd[2383813]: Listening on gpg-agent.socket - GnuPG cryptographic agent and passphrase cache.
Oct 03 04:01:00 Kali systemd[2383813]: Listening on pipewire-pulse.socket - PipeWire PulseAudio.
Oct 03 04:01:00 Kali systemd[2383813]: Listening on pipewire.socket - PipeWire Multimedia System Socket.
Oct 03 04:01:00 Kali systemd[2383813]: Listening on dbus.socket - D-Bus User Message Bus Socket.
Oct 03 06:30:55 Kali systemd[2487552]: Listening on dirmngr.socket - GnuPG network certificate management daemon.
Oct 03 06:30:55 Kali systemd[2487552]: Listening on gcr-ssh-agent.socket - GCR ssh-agent wrapper.
Oct 03 06:30:55 Kali systemd[2487552]: Listening on gnome-keyring-daemon.socket - GNOME Keyring daemon.
Oct 03 06:30:55 Kali systemd[2487552]: Listening on gpg-agent-browser.socket - GnuPG cryptographic agent and passphrase cache (access for web browsers).
Oct 03 06:30:55 Kali systemd[2487552]: Listening on gpg-agent-extra.socket - GnuPG cryptographic agent and passphrase cache (restricted).
Oct 03 06:30:55 Kali systemd[2487552]: Listening on gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation).
Oct 03 06:30:55 Kali systemd[2487552]: Listening on gpg-agent.socket - GnuPG cryptographic agent and passphrase cache.
Oct 03 06:30:55 Kali systemd[2487552]: Listening on pipewire-pulse.socket - PipeWire PulseAudio.
Oct 03 06:30:55 Kali systemd[2487552]: Listening on pipewire.socket - PipeWire Multimedia System Socket.
Oct 03 06:30:55 Kali systemd[2487552]: Listening on dbus.socket - D-Bus User Message Bus Socket.
Oct 03 06:43:21 Kali systemd[2496504]: Listening on dirmngr.socket - GnuPG network certificate management daemon.
Oct 03 06:43:21 Kali systemd[2496504]: Listening on gcr-ssh-agent.socket - GCR ssh-agent wrapper.
Oct 03 06:43:21 Kali systemd[2496504]: Listening on gnome-keyring-daemon.socket - GNOME Keyring daemon.
Oct 03 06:43:21 Kali systemd[2496504]: Listening on gpg-agent-browser.socket - GnuPG cryptographic agent and passphrase cache (access for web browsers).
Oct 03 06:43:21 Kali systemd[2496504]: Listening on gpg-agent-extra.socket - GnuPG cryptographic agent and passphrase cache (restricted).
Oct 03 06:43:21 Kali systemd[2496504]: Listening on gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation).
Oct 03 06:43:21 Kali systemd[2496504]: Listening on gpg-agent.socket - GnuPG cryptographic agent and passphrase cache.
Oct 03 06:43:21 Kali systemd[2496504]: Listening on pipewire-pulse.socket - PipeWire PulseAudio.
Oct 03 06:43:21 Kali systemd[2496504]: Listening on pipewire.socket - PipeWire Multimedia System Socket.
Oct 03 06:43:21 Kali systemd[2496504]: Listening on dbus.socket - D-Bus User Message Bus Socket.
```

Commented [GK25]: ran journalctl | grep -i "listening" what is saying is to listen in the journalctl on ports. Logs from services indicating they are Listening

- Add notes and screenshots
- Can you reproduce the lab with the questions and your screenshots with notes?
- If your boss asked you for this, did you provide the answer with context?