Gurjot Singh Khakh

Professor Torres

9/28/2025

IT 100

Lab: 6

- Copy parts A, B, and C from Canvas

Part A:

- **The computer does not turn on::**
  - 1. Identify the problem **(Minimum 10 reasons)**
  - 2. Establish a theory of possible cause
  - 3. Test the theory to determine the cause
  - 4. Establish a plan of action to resolve the problem and implement the solution
  - 5. Verify full system functionality, and if applicable, implement preventive measure
  - 6. Document findings, actions, and outcomes

Part A: 1

- Outlet
- A power stripe
- Power cable
- Power button
- Monitor
- overheating
- Video card faulty
- Loose or Disconnected Internal Cables
- RAM
- BIOS/UEFI Corruption or Misconfiguration

Part A:2

- Outlet may not have electricity
- Power stripe may not be turned on
- Power cable to computer may not be plugged in properly
- Power button was not clicked
- Monitor was not turned on

- PC was placed in closed quarters with no ventilation
- Video card may be damaged
- Internal power supply cable may be disconnected
- RAM is not fully inserted into the slot
- Overclocking CPU etc. in BIOS beyond stability

Part A: 3

- Try to plug in other cables
- Have you tried to plug in other cables in the power stripe and turn on the red button
- Are there any damages to the power button have you tried to press it on
- Is the monitor plugged in? Is the display or HDMI cable plugged in? Is it powered on?
- Where is the PC placed? Is it receiving air? Or is it in closed quarters with little to no air?
- Is the video card newly installed or old? Has this ever happened before?
- Did you open the PC and mess with the internal wiring?
- Did you install the RAM on your own and if so did you install it correctly
- Is the BIOS configuration default or did you customize it?

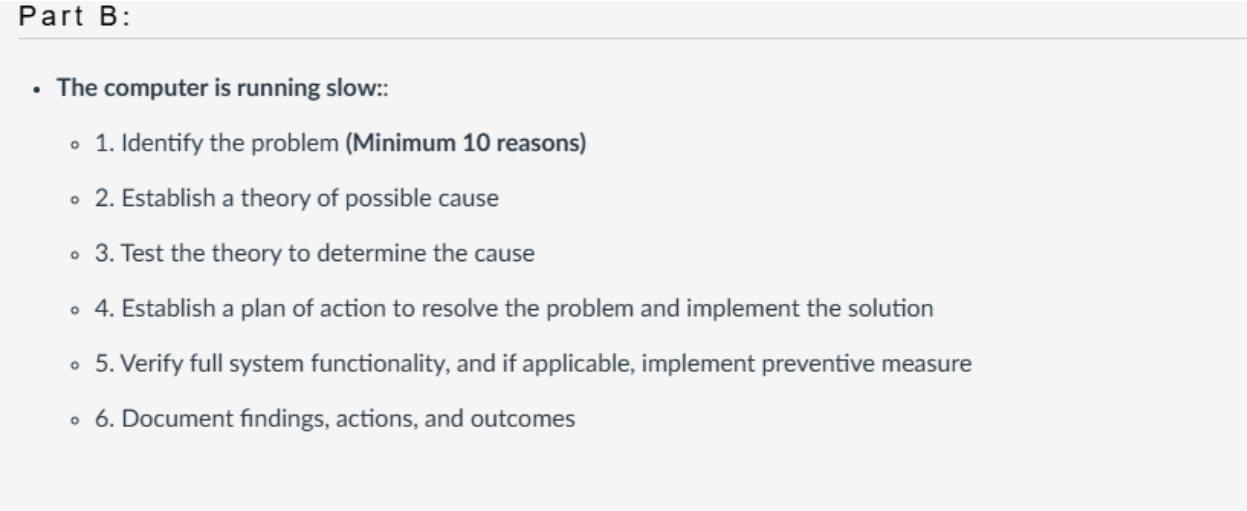
Part A: 4

- Check electricity current with multimeter on outlet
- Turn on power stripe
- Plug-in power cable to PC
- Click power button on PC
- Click the turn on button on the monitor
- Take out PC to get more air
- Replace video card
- Connect power supply cable
- Fully insert RAM into slot
- Change BIOS settings to default

Part A: 5

- Replace outlet or use another one for computer to turn on
- Replace power stripe or check if everything is turned on
- If cable for PC is still not working, then buy another one
- If power button on is broken then replacing it will be the best option
- Clean PC check it still overheats and shuts off
- Put in new video card and check if the computer turns on and check if everything is correctly working
- For power supply cable if not connected then connect it if it works then that's great but if not then get a new power supply cable
- Check if RAM is correctly fitted in and working if not then replace it and check if everything is working

- Open BIOS and put all settings to default and check if the system will boot up past the BIOS and check if everything is working
- Part A:6
- Replaced outlet
- Turned on power stripe
- Bought another power supply cable for PC
- Replaced power button
- Cleaned PC
- Put in new video card
- Internal power supply cable replaced it
- Reseated RAM



Part B: 1

- Too many background programs running
- Too many tabs opened
- Viruses
- Low disk space on system drive
- Full hard drive
- Bad RAM
- Outdated OS
- Overheating

- Old hard drive
- Too many startups' programs

Part B: 2

- 40 background systems doing something
- 50 tabs opened
- Viruses on computer
- Disk has no space on system drive
- Hard drive has too many files
- OS is running the previous one
- Computer not getting enough ventilation
- Hard drive is outdated
- Programs running in the background
- Startup programs

Part B: 3

1. Is the PC slow because of this, tried shutting them down
2. Have you tried to decrease the number of tabs or delete them
3. Have you tried to contact the manufacturer to get the viruses deleted
4. Have you checked the system information on how space you have on your system drive?
5. Have you deleted any unnecessary files from the hard drive
6. Have you checked the update log if there is a newer version available
7. Make sure all air access is open for ventilation
8. Have you tried to see how old the hard drive is
9. Turn off the programs running in the background
10. Turn off unnecessary startup programs

Part B:4

- Turn off background systems
- Delete all tabs and open only one
- Tried to delete viruses if cannot then contact manufacturer
- Delete unnecessary stuff to free up space on disk for system drive
- Delete files to free up space in hard drive
- Update OS or install new one
- Clean PC and check if it is getting ventilation
- Install new hard drive
- Shut off programs running in the background
- Shutoff startup programs

Part B: 5

1. Running faster? Shut off and see if it starts to slow down
2. Check to see if all tabs are deleted

3. Check to see if there are any viruses left
4. Check system drive and if it has enough space
5. Check hard drive and if works properly
6. Check new OS or updated one and if PC runs faster
7. Getting more air and no blockage of air
8. Check if new hard drive works properly
9. Check if all background programs are off and check if the PC is faster
10. Check if all unnecessary startup programs are off and work

Part B: 6

- Turned off background systems
- Deleted tabs
- Deleted viruses
- Checked system drive and deleted uncesseray files
- Checked hard drive
- Updated OS
- Clean PC for more ventilation
- Installed new hard drive
- Turned off any background programs
- And turned off any unnecessary startup programs running

Part C:

- **The internet is not working::**
  - 1. Identify the problem **(Minimum 10 reasons)**
  - 2. Establish a theory of possible cause
  - 3. Test the theory to determine the cause
  - 4. Establish a plan of action to resolve the problem and implement the solution
  - 5. Verify full system functionality, and if applicable, implement preventive measure
  - 6. Document findings, actions, and outcomes

Part C: 1

1. Power cable unplugged from router
2. Device too far from router
3. Router hardware failure
4. ISP outage
5. Airplane mode turned on device
6. DNS server issues

7. Firewall configuration issue
8. Too many devices on network
9. Power outage
10. Router outdated

Part C: 2

1. Someone unplugged power cable
2. Weak signal because of walls and too far of a distance
3. Router overheated
4. ISP underground cables damaged due to weather
5. Airplane mode is on, from the device
6. DNS points to the wrong server
7. Antivirus flags browser and apps as threats
8. Too many users gaing and downloading simultaneously
9. Device didn't reboot correctly after power outage
10. Check for update on router admin page

Part C: 3

1. Test if the router lights are off or blinking or not
2. Move deice closer tho the router and if the connection improves
3. Touch the router and if it is too hot from normal then power it off for a 10 mins and power it back on
4. ISP contact your ISP for service alerts in the area
5. Check on the phone if airplane mode is on and turn it off and wait for the Wi-Fi to connect
6. DNS open a website by its IP address and if the website opens by IP and not by name DNS is the issue
7. Disable antivirus and see if you could access blocked websites
8. Uses routers admin page and see how many users are using the internet
9. Routers unplug it for about 30 secs then plug it back in and power back up and see if it reconnects and works fine
10. On router admin page check if there is a update available

Part C: 4

1. Inspect if router lights are off
2. Get device closer to router
3. Power off router and dust it if dusty for more air ventilation
4. ISP check router if no internet light and then contact ISP
5. Open settings and see if airplane mode is turned on and then turn it off
6. Open DNS settings and manaully set DNS to a reliable public server
7. Turn off Antiviruis and change the configuration of it
8. Use router admin panel to see who is on the bandwidth and any unnecessary devices
9. Completely turn off router and wait for a bit and then plug it back in and see if everything runs well

10. Update firmware by router website and see if there is one for the router for the software

Part C: 5

1. Does the router have lights on and works correctly
2. Check if internet works after coming closer to the router
3. Check full functionality of the router after dusting it and powering it off and see if it overheats now
4. Contacted ISP for the outage
5. Opened settings if it was on airplane mode and turned it off
6. Opened DNS settings and changed DNS and works properly after
7. Turned off Antivirus and configured it
8. Used router admin panel to kickout some devices
9. Turned off router after a outage and internet works now
10. Updated firmware and now internet works fine

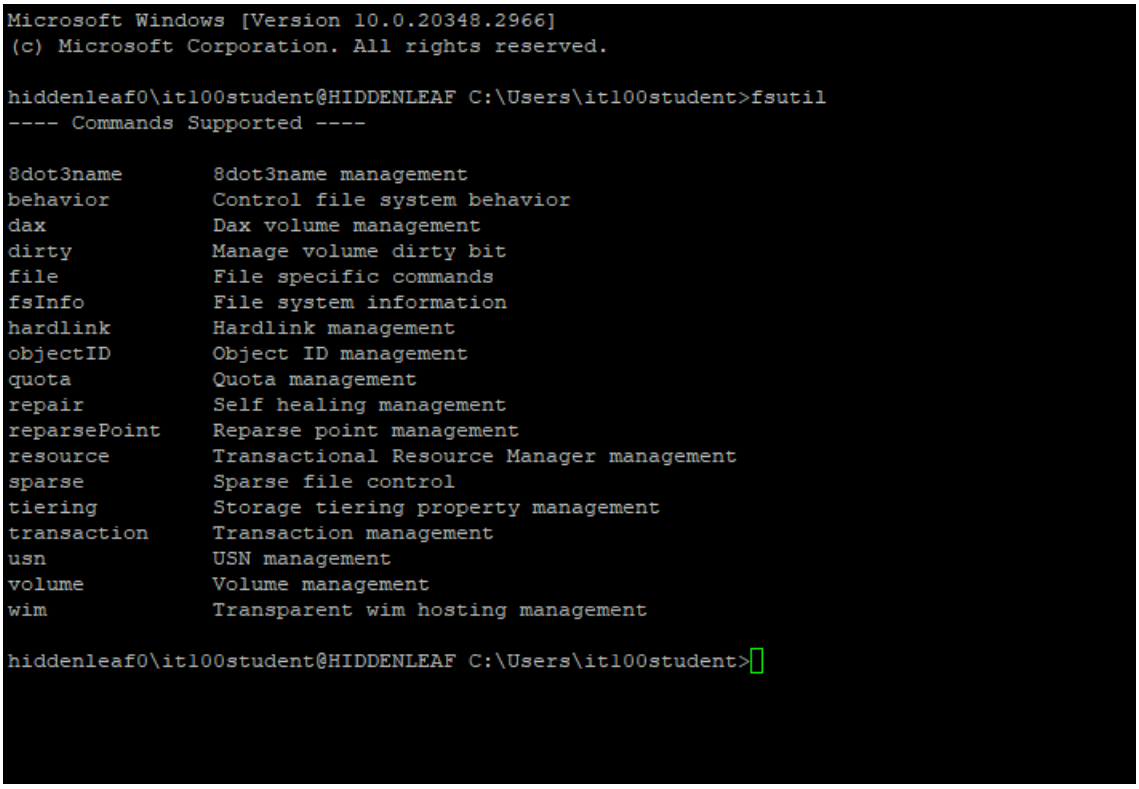
Part C: 6

1. Power cable was disconnected
2. Device was too far
3. Dusted router
4. Contacted ISP about internet
5. Turned off airplane mode
6. Changed DNS
7. Configured antivirus
8. Router admin panel to kickout unnecessary devices
9. router works now because I turned it off after a power outage
10. Firmware is up to date now internet works fine

Part D: SierraLab: ssh to Windows Box

- Log on via SSH to our SierraLab network (207.62.230.146:2222).
- Use the password you set up with your public/private key
- Ensure that your putty is setup to use your private key
- Once you log on, ssh to the Windowsbox (ssh it100student@windowsbox.com)
- **Password is Computersrock1**
- Answer the below questions with screenshots

1. Use the fsutil to display system information
2. Use schtasks to display scheduled tasks
3. Use the query command to query user
4. Use the dispdiag to generate the display adapter diagnostics. Than use the type command to view it
5. View the contents of the hosts file. What is this for?
6. View the contents of the networks file. What is this for?
7. View the contents of the protocol file. What is this for?
8. View the contents of the services file. What is this for?
9. View the contents of the lmhosts.sam file. What is this for?
10. Try to access the SAM file. What occured and why did it occur?



```
hiddenleaf0\itl00student@HIDDENLEAF C:\Users\itl00student>schtasks

Folder: \
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
CreateExplorerShellUnelevatedTask        N/A                    Ready
MicrosoftEdgeUpdateTaskMachineCore       9/28/2025 11:26:55 AM  Ready
MicrosoftEdgeUpdateTaskMachineUA         9/27/2025 6:56:55 PM   Ready
npcapwatchdog                            N/A                    Ready

Folder: \GoogleSystem
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \GoogleSystem\GoogleUpdater
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
GoogleUpdaterTaskSystem141.0.7376.0{6C07 9/27/2025 6:54:26 PM   Ready
GoogleUpdaterTaskSystem142.0.7416.0{1985 9/27/2025 7:13:09 PM   Ready

Folder: \Microsoft
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\OneCore
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Windows
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
Server Initial Configuration Task        N/A                    Disabled

Folder: \Microsoft\Windows\.NET Framework
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
.NET Framework NGEN v4.0.30319           N/A                    Ready
.NET Framework NGEN v4.0.30319 64        N/A                    Ready
.NET Framework NGEN v4.0.30319 64 Critic N/A                    Disabled
.NET Framework NGEN v4.0.30319 Critical  N/A                    Disabled

Folder: \Microsoft\Windows\Active Directory Rights Management Services Client
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
AD RMS Rights Policy Template Management N/A                    Disabled
AD RMS Rights Policy Template Management N/A                    Ready
```

```
Microsoft Windows [Version 10.0.20348.2966]
(c) Microsoft Corporation. All rights reserved.

hiddenleaf0\itl00student@HIDDENLEAF C:\Users\itl00student>query user
 USERNAME              SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
 student                                   1  Disc     20+03:20  9/1/2025 2:15 PM

hiddenleaf0\itl00student@HIDDENLEAF C:\Users\itl00student>
```

```
Microsoft Windows [Version 10.0.20348.2966]
(c) Microsoft Corporation. All rights reserved.

hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>cd "C:\Program Files\Intel\Display\"
The system cannot find the path specified.

hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>dispdiag
Dump file: C:\Users\it100student\DispDiag-20250928-150436-2708-328.dat

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

```
hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>type C:\Users\it100student\DispDiag-20250928-150436-2708-328.dat
!820348.fe_release.210507-1500
|O►►QO  ►Q  ■  ♥O╪!O¡1¡VMware, Inc..VMware Virtual Platform►>Microsoft Basic Display Adapter0(Standard display types)¡MicrosoftÇiú┼ö├QQ|O
-PCI\CC_0300√<Microsoft Basic Display Driver0(Standard display types)¡MicrosoftÇiú┼ö├QQ|O
"ROOT\BasicDisplay ☺'¡©vW╚└♦chrome.exe►♦‼©m►╞Zy►©►└vW╚└♦Å
∂7ƒQÇ[♥ç© ©Ç8♦Ç8♦ ©©    ►Ç8♦$♥©©Ç8♦Ç8♦Y■/'¡©vW╚└♦chrome.exe►♦‼©►m►δZy►©►└vW╚└♦Å
∂7ƒQÇ[♥ç© ©Ç8♦Ç8♦ ©©    ►Ç8♦$♥©©Ç8♦Ç8♦Y■/'¡©vW╚└♦chrome.exe►♦‼©◄m►
[y►©►└vW╚└♦Å
∂7ƒQÇ[♥ç© ©Ç8♦Ç8♦ ©©    ►Ç8♦$♥©©Ç8♦Ç8♦Y■/'¡©vW╚└♦chrome.exe►♦‼©¡m►)[y►©►└vW╚└♦Å
∂7ƒQÇ[♥ç© ©Ç8♦Ç8♦ ©©    ►Ç8♦$♥©©Ç8♦Ç8♦Y■/'¡©vW╚└♦chrome.exe►♦‼©‼m►H[y►©►└vW╚└♦Å
∂7ƒQÇ[♥ç© ©Ç8♦Ç8♦ ©©    ►Ç8♦$♥©©Ç8♦Ç8♦Y■/'¡©▌o═╗└♦chrome.exe►♦‼©¶m►l[y►©►└▌o═╗└♦Å
∂7ƒQÇ[♥ç© ©Ç8♦Ç8♦ ©©    ►Ç8♦$♥©©Ç8♦Ç8♦Y■/'¡©▌o═╗└♦chrome.exe►♦‼©§m►ï[y►©►└▌o═╗└♦Å
∂7ƒQÇ[♥ç© ©Ç8♦Ç8♦ ©©    ►Ç8♦$♥©©Ç8♦Ç8♦Y■/'¡©▌o═╗└♦chrome.exe►♦‼©—m►¬[y►©►└▌o═╗└♦Å
∂7ƒQÇ[♥ç© ©Ç8♦Ç8♦ ©©    ►Ç8♦$♥©©Ç8♦Ç8♦Y■/'¡©▌o═╗└♦chrome.exe►♦‼©¡m►╒[y►©►└▌o═╗└♦Å
∂7ƒQÇ[♥ç© ©Ç8♦Ç8♦ ©©    ►Ç8♦$♥©©Ç8♦Ç8♦Y■/'¡©▌o═╗└♦chrome.exe►♦‼©¶m►╪[y►©►└▌o═╗└♦Å
∂7ƒQÇ[♥ç© ©Ç8♦Ç8♦ ©©    ►Ç8♦$♥©©Ç8♦Ç8♦Y■/'¡©▌o═╗└♦chrome.exe►♦‼©¡m►\y►©►└▌o═╗└♦Å
∂7ƒQÇ[♥ç© ©Ç8♦Ç8♦ ©©    ►Ç8♦$♥©©Ç8♦Ç8♦Y■/'¡©8Ç┐╚└♦chrome.exe►♦‼©
hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>
```

```
hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student> type C:\Windows\System32\drivers\etc\hosts
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
172.16.99.2     linuxbox.com
172.16.99.4     windowsbox.com

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

```
hiddenleaf0\itl00student@HIDDENLEAF C:\Users\itl00student>type C:\Windows\Systems32\drivers\etc\networks
The system cannot find the path specified.

hiddenleaf0\itl00student@HIDDENLEAF C:\Users\itl00student> type C:\Windows\System32\drivers\etc\networks
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This file contains network name/network number mappings for
# local networks. Network numbers are recognized in dotted decimal form.
#
# Format:
#
# <network name>  <network number>     [aliases...]  [#<comment>]
#
# For example:
#
#    loopback     127
#    campus       284.122.107
#    london       284.122.108

loopback                127

hiddenleaf0\itl00student@HIDDENLEAF C:\Users\itl00student>
```

```
hiddenleaf0\itl00student@HIDDENLEAF C:\Users\itl00student>type C:\Windows\System32\drivers\etc\protocol
# Copyright (c) 1993-2006 Microsoft Corp.
#
# This file contains the Internet protocols as defined by various
# RFCs.  See http://www.iana.org/assignments/protocol-numbers
#
# Format:
#
# <protocol name>  <assigned number>  [aliases...]   [#<comment>]

ip          0     IP            # Internet protocol
icmp        1     ICMP          # Internet control message protocol
ggp         3     GGP           # Gateway-gateway protocol
tcp         6     TCP           # Transmission control protocol
egp         8     EGP           # Exterior gateway protocol
pup         12    PUP           # PARC universal packet protocol
udp         17    UDP           # User datagram protocol
hmp         20    HMP           # Host monitoring protocol
xns-idp     22    XNS-IDP       # Xerox NS IDP
rdp         27    RDP           # "reliable datagram" protocol
ipv6        41    IPv6          # Internet protocol IPv6
ipv6-route  43    IPv6-Route    # Routing header for IPv6
ipv6-frag   44    IPv6-Frag     # Fragment header for IPv6
esp         50    ESP           # Encapsulating security payload
ah          51    AH            # Authentication header
ipv6-icmp   58    IPv6-ICMP     # ICMP for IPv6
ipv6-nonxt  59    IPv6-NoNxt    # No next header for IPv6
ipv6-opts   60    IPv6-Opts     # Destination options for IPv6
rvd         66    RVD           # MIT remote virtual disk
```

```
hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>type C:\Windows\System32\drivers\etc\services
# Copyright (c) 1993-2004 Microsoft Corp.
#
# This file contains port numbers for well-known services defined by IANA
#
# Format:
#
# <service name>  <port number>/<protocol>  [aliases...]   [#<comment>]
#

echo                7/tcp
echo                7/udp
discard             9/tcp    sink null
discard             9/udp    sink null
systat             11/tcp    users                 #Active users
systat             11/udp    users                 #Active users
daytime            13/tcp
daytime            13/udp
qotd               17/tcp    quote                 #Quote of the day
qotd               17/udp    quote                 #Quote of the day
chargen            19/tcp    ttytst source         #Character generator
chargen            19/udp    ttytst source         #Character generator
ftp-data           20/tcp                          #FTP, data
ftp                21/tcp                          #FTP. control
ssh                22/tcp                          #SSH Remote Login Protocol
telnet             23/tcp
smtp               25/tcp    mail                  #Simple Mail Transfer Protocol
time               37/tcp    timserver
time               37/udp    timserver
rlp                39/udp    resource              #Resource Location Protocol
nameserver         42/tcp    name                  #Host Name Server
nameserver         42/udp    name                  #Host Name Server
nicname            43/tcp    whois
domain             53/tcp                          #Domain Name Server
domain             53/udp                          #Domain Name Server
bootps             67/udp    dhcps                 #Bootstrap Protocol Server
bootpc             68/udp    dhcpc                 #Bootstrap Protocol Client
tftp               69/udp                          #Trivial File Transfer
gopher             70/tcp
finger             79/tcp
http               80/tcp    www www-http          #World Wide Web
hosts2-ns          81/tcp                          #HOSTS2 Name Server
hosts2-ns          81/udp                          #HOSTS2 Name Server
kerberos           88/tcp    krb5 kerberos-sec     #Kerberos
kerberos           88/udp    krb5 kerberos-sec     #Kerberos
hostname          101/tcp    hostnames             #NIC Host Name Server
iso-tsap          102/tcp                          #ISO-TSAP Class 0
rtelnet           107/tcp                          #Remote Telnet Service
pop2              109/tcp    postoffice            #Post Office Protocol - Version 2
pop3              110/tcp                          #Post Office Protocol - Version 3
```

```
hiddenleaf0\itl00student@HIDDENLEAF C:\Users\itl00student>type C:\Windows\System32\drivers\etc\Lmhosts.sam
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample LMHOSTS file used by the Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to computernames
# (NetBIOS) names.  Each entry should be kept on an individual line.
# The IP address should be placed in the first column followed by the
# corresponding computername. The address and the computername
# should be separated by at least one space or tab. The "#" character
# is generally used to denote the start of a comment (see the exceptions
# below).
#
# This file is compatible with Microsoft LAN Manager 2.x TCP/IP lmhosts
# files and offers the following extensions:
#
#      #PRE
#      #DOM:<domain>
#      #INCLUDE <filename>
#      #BEGIN_ALTERNATE
#      #END_ALTERNATE
#      \0xnn (non-printing character support)
#
# Following any entry in the file with the characters "#PRE" will cause
# the entry to be preloaded into the name cache. By default, entries are
# not preloaded, but are parsed only after dynamic name resolution fails.
#
# Following an entry with the "#DOM:<domain>" tag will associate the
# entry with the domain specified by <domain>. This affects how the
# browser and logon services behave in TCP/IP environments. To preload
# the host name associated with #DOM entry, it is necessary to also add a
# #PRE to the line. The <domain> is always preloaded although it will not
# be shown when the name cache is viewed.
#
# Specifying "#INCLUDE <filename>" will force the RFC NetBIOS (NBT)
# software to seek the specified <filename> and parse it as if it were
# local. <filename> is generally a UNC-based name, allowing a
# centralized lmhosts file to be maintained on a server.
# It is ALWAYS necessary to provide a mapping for the IP address of the
# server prior to the #INCLUDE. This mapping must use the #PRE directive.
# In addtion the share "public" in the example below must be in the
# LanManServer list of "NullSessionShares" in order for client machines to
# be able to read the lmhosts file successfully. This key is under
# \machine\system\currentcontrolset\services\lanmanserver\parameters\nullsessionshares
# in the registry. Simply add "public" to the list found there.
#
# The #BEGIN_ and #END_ALTERNATE keywords allow multiple #INCLUDE
# statements to be grouped together. Any single successful include
# will cause the group to succeed.
#
```

```
hiddenleaf0\itl00student@HIDDENLEAF C:\Users\itl00student>C:\Windows\System32\config\SAM
'C:\Windows\System32\config\SAM' is not recognized as an internal or external command,
operable program or batch file.

hiddenleaf0\itl00student@HIDDENLEAF C:\Users\itl00student> C:\Windows\System32\config\SAM
'C:\Windows\System32\config\SAM' is not recognized as an internal or external command,
operable program or batch file.

hiddenleaf0\itl00student@HIDDENLEAF C:\Users\itl00student> type C:\Windows\System32\drivers\etc\SAM
The system cannot find the file specified.

hiddenleaf0\itl00student@HIDDENLEAF C:\Users\itl00student>C:\Windows\System32\config\SAM
'C:\Windows\System32\config\SAM' is not recognized as an internal or external command,
operable program or batch file.
```

Part E: SierraLab: ssh to Linux Box

- Log on via SSH to our SierraLab network (207.62.230.146:2222).
- Use the password you set up with your public/private key
- Ensure that your putty is setup to use your private key
- Once you log on, ssh to the Linuxbox (ssh it100student@linuxbox.com)
- **Password is Computersrock1**

1: cd to the /var/log location

2: within the log area type the dmesg command

3: run dmesg and ask for only "eth" info. What is the new name of the eth0

4: run dmesg command. What details can you find about the eth1

5: run dmesg command. What has been disabled

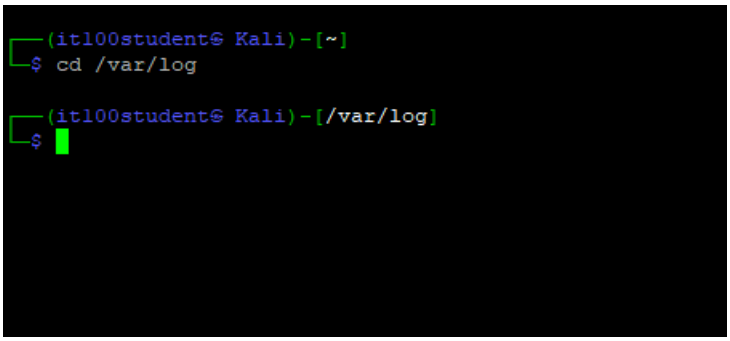
6: what hardare info can you get from the dmesg command

7: using the man pages, run dmesg and show kernel messages

8: run the dmesg -H command and save the output to your Documents folder as “yourl last name” (take your time)

9: go to your Documents directory, cat the content of “your last name” and display only pid info

10: From your Documents directory use different switches for the ls command to find out as much info as you can about the files



```
┌──(itl00student㉿Kali)-[/var/log]
└─$ dmesg
[    0.000000] Linux version 6.3.0-kali1-amd64 (devel@kali.org) (gcc-12 (Debian 12.3.0-4) 12.3.0, GNU ld (GNU Binutils for Debian) 2.40.50.20230611) #1 SMP PREEMPT_DYNAMIC Debia
n 6.3.7-1kali1 (2023-06-29)
[    0.000000] Command line: BOOT_IMAGE=/vmlinuz-6.3.0-kali1-amd64 root=/dev/mapper/Ethical--Hacker--Kali--vg-root ro quiet splash
[    0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
[    0.000000] x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
[    0.000000] x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'compacted' format.
[    0.000000] signal: max sigframe size: 1776
[    0.000000] BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009f7ff] usable
[    0.000000] BIOS-e820: [mem 0x000000000009f800-0x000000000009ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000000dc000-0x00000000000fffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000000100000-0x00000000bfedffff] usable
[    0.000000] BIOS-e820: [mem 0x00000000bfee0000-0x00000000bfefefff] ACPI data
[    0.000000] BIOS-e820: [mem 0x00000000bfeff000-0x00000000bfefffff] ACPI NVS
[    0.000000] BIOS-e820: [mem 0x00000000bff00000-0x00000000bfffffff] usable
[    0.000000] BIOS-e820: [mem 0x00000000f0000000-0x00000000f7ffffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fffe0000-0x00000000ffffffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000100000000-0x000000043fffffff] usable
[    0.000000] NX (Execute Disable) protection: active
[    0.000000] SMBIOS 2.7 present.
[    0.000000] DMI: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 11/12/2020
[    0.000000] vmware: hypercall mode: 0x00
[    0.000000] Hypervisor detected: VMware
[    0.000000] vmware: TSC freq read from hypervisor : 2994.374 MHz
[    0.000000] vmware: Host bus clock speed read from hypervisor : 66000000 Hz
[    0.000000] vmware: using clock offset of 8991818333 ns
[    0.000012] tsc: Detected 2994.374 MHz processor
[    0.001691] e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
[    0.001694] e820: remove [mem 0x000a0000-0x000fffff] usable
[    0.001699] last_pfn = 0x440000 max_arch_pfn = 0x400000000
[    0.001723] x86/PAT: Configuration [0-7]: WB  WC  UC- UC  WB  WP  UC- WT
[    0.001761] e820: update [mem 0xc0000000-0xffffffff] usable ==> reserved
[    0.001766] last_pfn = 0xc0000 max_arch_pfn = 0x400000000
[    0.004569] found SMP MP-table at [mem 0x000f6a70-0x000f6a7f]
[    0.004582] Using GB pages for direct mapping
[    0.004856] RAMDISK: [mem 0x2e959000-0x334a3fff]
[    0.004862] ACPI: Early table checksum verification disabled
[    0.004865] ACPI: RSDP 0x00000000000F6A00 000024 (v02 PTLTD )
[    0.004869] ACPI: XSDT 0x00000000BFEEEA0F 00005C (v01 INTEL  440BX    06040000 VMW  01324272)
[    0.004875] ACPI: FACP 0x00000000BFEFEE73 0000F4 (v04 INTEL  440BX    06040000 PTL  000F4240)
[    0.004879] ACPI: DSDT 0x00000000BFEEEC95 0101DE (v01 PTLTD  Custom   06040000 MSFT 03000001)
```

```
┌──(itl00student㉿Kali)-[/var/log]
└─$ dmesg | grep -i 'eth'
[    1.664953] pcnet32: PCnet/PCI II 79C970A at 0x2000, 00:0c:29:70:00:58 assigned IRQ 18
[    1.665304] pcnet32: eth0: registered as PCnet/PCI II 79C970A
[    1.665681] pcnet32: PCnet/PCI II 79C970A at 0x2080, 00:0c:29:70:00:62 assigned IRQ 19
[    1.665923] pcnet32: eth1: registered as PCnet/PCI II 79C970A
[    1.665963] pcnet32: 2 cards_found
--
[   12.422129] NET: Registered PF_VSOCK protocol family
[   14.533628] pcnet32 0000:02:00.0 eth0: link up
[   14.950208] pcnet32 0000:02:01.0 eth1: link up
[   15.206815] NET: Registered PF_QIPCRTR protocol family
--
[   77.499408] Initializing XFRM netlink socket
[   78.503610] docker0: port 1(vethc1a025a) entered blocking state
[   78.503619] docker0: port 1(vethc1a025a) entered disabled state
[   78.504514] vethc1a025a: entered allmulticast mode
[   78.504578] vethc1a025a: entered promiscuous mode
[   78.504915] docker0: port 1(vethc1a025a) entered blocking state
[   78.504920] docker0: port 1(vethc1a025a) entered forwarding state
[   78.504942] IPv6: ADDRCONF(NETDEV_CHANGE): docker0: link becomes ready
[   78.505034] docker0: port 1(vethc1a025a) entered disabled state
[   78.505884] br-339414195aeb: port 1(veth8333407) entered blocking state
[   78.505890] br-339414195aeb: port 1(veth8333407) entered disabled state
[   78.506624] veth8333407: entered allmulticast mode
[   78.506682] veth8333407: entered promiscuous mode
[   78.507569] br-339414195aeb: port 1(veth8333407) entered blocking state
[   78.507577] br-339414195aeb: port 1(veth8333407) entered forwarding state
[   78.507629] br-339414195aeb: port 1(veth8333407) entered disabled state
[   78.511210] br-355ee7945a88: port 1(veth4cbb037) entered blocking state
[   78.511216] br-355ee7945a88: port 1(veth4cbb037) entered disabled state
[   78.511232] veth4cbb037: entered allmulticast mode
[   78.511293] veth4cbb037: entered promiscuous mode
[   78.513472] br-355ee7945a88: port 1(veth4cbb037) entered blocking state
[   78.513478] br-355ee7945a88: port 1(veth4cbb037) entered forwarding state
[   78.513499] IPv6: ADDRCONF(NETDEV_CHANGE): br-355ee7945a88: link becomes ready
[   78.513566] br-355ee7945a88: port 1(veth4cbb037) entered disabled state
[   78.521318] br-internal: port 1(veth4a3e3d4) entered blocking state
[   78.521324] br-internal: port 1(veth4a3e3d4) entered disabled state
[   78.521338] veth4a3e3d4: entered allmulticast mode
[   78.521387] veth4a3e3d4: entered promiscuous mode
[   78.522286] br-internal: port 1(veth4a3e3d4) entered blocking state
[   78.522292] br-internal: port 1(veth4a3e3d4) entered forwarding state
[   78.522314] IPv6: ADDRCONF(NETDEV_CHANGE): br-internal: link becomes ready
[   78.522501] br-internal: port 1(veth4a3e3d4) entered disabled state
[   78.577896] br-339414195aeb: port 2(veth08e13ba) entered blocking state
[   78.577905] br-339414195aeb: port 2(veth08e13ba) entered disabled state
[   78.577922] veth08e13ba: entered allmulticast mode
[   78.577994] veth08e13ba: entered promiscuous mode
[   78.582653] br-339414195aeb: port 2(veth08e13ba) entered blocking state
```

```
┌──(itl00student㉿ Kali)-[/var/log]
└─$ dmesg | grep -i eth1
[    1.665923] pcnet32: eth1: registered as PCnet/PCI II 79C970A
[   14.950208] pcnet32 0000:02:01.0 eth1: link up
[   81.495308] eth0: renamed from veth138ac22
[   83.776854] eth0: renamed from veth1lea5bd
[   83.852824] eth0: renamed from veth1460624

┌──(itl00student㉿ Kali)-[/var/log]
```

```
┌──(itl00student㉿ Kali)-[/var/log]
└─$ dmesg | grep -i 'disable'
[    0.000000] NX (Execute Disable) protection: active
[    0.004862] ACPI: Early table checksum verification disabled
[    0.068151] Yama: disabled by default; enable with sysctl kernel.yama.*
[    0.069083] Speculative Store Bypass: Mitigation: Speculative Store Bypass disabled via prctl
[    0.128097] audit: initializing netlink subsys (disabled)
[    0.261196] ACPI: PCI: Interrupt link LNKB disabled
[    1.173952] amd_pstate: driver load is disabled, boot with specific mode to enable this
[    1.267095] evm: security.SMACK64 (disabled)
[    1.267096] evm: security.SMACK64EXEC (disabled)
[    1.267097] evm: security.SMACK64TRANSMUTE (disabled)
[    1.267098] evm: security.SMACK64MMAP (disabled)
[    1.960262] sd 0:0:0:0: [sda] Write cache: disabled, read cache: enabled, doesn't support DPO or FUA
[    2.337378] device-mapper: core: CONFIG_IMA_DISABLE_HTABLE is disabled. Duplicate IMA measurements will not be recorded in the IMA log.
[    6.123449] systemd-journald[349]: Collecting audit messages is disabled.
[   78.503619] docker0: port 1(vethc1a025a) entered disabled state
[   78.505034] docker0: port 1(vethc1a025a) entered disabled state
[   78.505890] br-339414195aeb: port 1(veth8333407) entered disabled state
[   78.507629] br-339414195aeb: port 1(veth8333407) entered disabled state
[   78.511216] br-355ee7945a88: port 1(veth4cbb037) entered disabled state
[   78.513566] br-355ee7945a88: port 1(veth4cbb037) entered disabled state
[   78.521324] br-internal: port 1(veth4a3e3d4) entered disabled state
[   78.522501] br-internal: port 1(veth4a3e3d4) entered disabled state
[   78.577905] br-339414195aeb: port 2(veth08e13ba) entered disabled state
[   78.582721] br-339414195aeb: port 2(veth08e13ba) entered disabled state
[   78.916464] br-339414195aeb: port 3(vethdf5c130) entered disabled state
[   78.916805] br-339414195aeb: port 3(vethdf5c130) entered disabled state
[   78.919510] br-internal: port 2(veth03e144d) entered disabled state
[   78.919770] br-internal: port 2(veth03e144d) entered disabled state
[   79.138107] br-internal: port 3(veth7195f2b) entered disabled state
[   79.149667] br-internal: port 3(veth7195f2b) entered disabled state
[   79.150748] br-339414195aeb: port 4(veth819e8dc) entered disabled state
[   79.584226] br-339414195aeb: port 4(veth819e8dc) entered disabled state
[   79.588784] br-internal: port 4(vethdf6cec3) entered disabled state
[   79.589642] br-internal: port 4(vethdf6cec3) entered disabled state
[   80.009294] br-339414195aeb: port 5(vethadaa110) entered disabled state
[   80.608242] br-339414195aeb: port 5(vethadaa110) entered disabled state
[   80.619523] br-internal: port 5(veth7ea0c31) entered disabled state
[   80.619736] br-internal: port 5(veth7ea0c31) entered disabled state
[   80.853896] br-internal: port 6(veth514f370) entered disabled state
[   80.854164] br-internal: port 6(veth514f370) entered disabled state
```

```
┌──(itl00student㉿ Kali)-[~]
└─$ dmesg | grep -i 'cpu'
[    0.017044] smpboot: Allowing 2 CPUs, 0 hotplug CPUs
[    0.021612] setup_percpu: NR_CPUS:8192 nr_cpumask_bits:2 nr_cpu_ids:2 nr_node_ids:1
[    0.021975] percpu: Embedded 63 pages/cpu s221184 r8192 d28672 u1048576
[    0.021979] pcpu-alloc: s221184 r8192 d28672 u1048576 alloc=1*2097152
[    0.021982] pcpu-alloc: [0] 0 1
[    0.052299] SLUB: HWalign=64, Order=0-3, MinObjects=0, CPUs=2, Nodes=1
[    0.061130] rcu:     RCU restricting CPUs from NR_CPUS=8192 to nr_cpu_ids=2.
[    0.061134] rcu: Adjusting geometry for rcu_fanout_leaf=16, nr_cpu_ids=2
[    0.088237] smpboot: CPU0: AMD EPYC 7302 16-Core Processor (family: 0x17, model: 0x31, stepping: 0x0)
[    0.089281] smp: Bringing up secondary CPUs ...
[    0.089433] .... node  #0, CPUs:      #1
[    0.004051] smpboot: CPU 1 Converting physical 2 to logical package 1
[    0.004051] smpboot: CPU 1 Converting physical 2 to logical die 1
[    0.090303] smp: Brought up 1 node, 2 CPUs
[    0.128352] cpuidle: using governor ladder
[    0.128358] cpuidle: using governor menu
[    1.174000] ledtrig-cpu: registered to indicate activity on CPUs
[    1.691804] cryptd: max_cpu_qlen set to 1000
```

```
┌──(itl00student㉿Kali)-[~]
└─$ man dmesg

     -f, --facility list
         Restrict output to the given (comma-separated) list of facilities. For example:

         dmesg --facility=daemon

         will print messages from system daemons only. For all supported facilities see the --help output.

     -H, --human
         Enable human-readable output. See also --color, --reltime and --nopager.

     -J, --json
         Use JSON output format. The time output format is in "sec.usec" format only, log priority level is not decoded by default (use --decode to split into facility
         and priority), the other options to control the output format or time format are silently ignored.

     -k, --kernel
         Print kernel messages.

     -L, --color[=when]
         Colorize the output. The optional argument when can be auto, never or always. If the when argument is omitted, it defaults to auto. The colors can be disabled;
         for the current built-in default see the --help output. See also the COLORS section below.

     -l, --level list
         Restrict output to the given (comma-separated) list of levels. For example:

         dmesg --level=err,warn

         will print error and warning messages only. For all supported levels see the --help output.

         Appending a plus + to a level name also includes all higher levels. For example:

         dmesg --level=err+

         will print levels err, crit, alert and emerg.

         Prepending it will include all lower levels.

     -n, --console-level level
         Set the level at which printing of messages is done to the console. The level is a level number or abbreviation of the level name. For all supported levels see
         the --help output.

         For example, -n 1 or -n emerg prevents all messages, except emergency (panic) messages, from appearing on the console. All levels of messages are still written
         to /proc/kmsg, so syslogd(8) can still be used to control exactly where kernel messages appear. When the -n option is used, dmesg will not print or clear the
         kernel ring buffer.

     --noescape
         The unprintable and potentially unsafe characters (e.g., broken multi-byte sequences, terminal controlling chars, etc.) are escaped in format \x<hex> for
         security reason by default. This option disables this feature at all. It's usable for example for debugging purpose together with --raw. Be careful and don't use
         it by default.
```

```
┌──(itl00student㉿Kali)-[~]
└─$ dmesg -H > ~/Documents/khakh

┌──(itl00student㉿Kali)-[~]
└─$ ls ~/Documents
arnold      Brown.txt  Lastname  Melpati.txt  Vinyard.log       como          khakh        smith      yourlastname
ondarenko  LNU.txt    Melpati   Turner       YourLastName.txt  erickson.txt  russell.log  trett.txt  yourlastname.log

┌──(itl00student㉿Kali)-[~]
└─$ cat
```

```
┌──(itl00student㉿Kali)-[~]
└─$ cat ~/Documents/khakh | grep -Eo 'pid=[0-9]+'
pid=1006
pid=2078
```

```
┌──(itl00student㉿Kali)-[~/Documents]
└─$ ls -alh --time-style=long-iso
total 1.6M
drwxr-xr-x 2 itl00student itl00student 4.0K 2025-09-29 00:57 .
drwx------ 8 itl00student itl00student 4.0K 2025-09-29 01:00 ..
-rw-r--r-- 1 itl00student itl00student 104K 2025-09-25 21:07 Arnold
-rw-r--r-- 1 itl00student itl00student 104K 2025-09-27 01:08 Bondarenko
-rw-r--r-- 1 itl00student itl00student 104K 2025-09-26 00:45 Brown.txt
-rw-r--r-- 1 itl00student itl00student 104K 2025-09-28 09:16 LNU.txt
-rw-r--r-- 1 itl00student itl00student 104K 2025-09-25 21:21 Lastname
-rw-r--r-- 1 itl00student itl00student 104K 2025-09-25 09:27 Melpati
-rw-r--r-- 1 itl00student itl00student 104K 2025-09-26 00:24 Melpati.txt
-rw-r--r-- 1 itl00student itl00student 104K 2025-09-28 00:42 Turner
-rw-r--r-- 1 itl00student itl00student 104K 2025-09-25 21:05 Vinyard.log
-rw-r--r-- 1 itl00student itl00student 104K 2025-09-28 09:13 YourLastName.txt
-rw-r--r-- 1 itl00student itl00student 104K 2025-09-25 08:48 como
-rw-r--r-- 1 itl00student itl00student 104K 2025-09-26 00:42 erickson.txt
-rw-r--r-- 1 itl00student itl00student 104K 2025-09-29 01:01 khakh
-rw-r--r-- 1 itl00student itl00student    0 2025-09-26 00:48 russell.log
-rw-r--r-- 1 itl00student itl00student 104K 2025-09-29 00:57 smith
-rw-r--r-- 1 itl00student itl00student 104K 2025-09-28 22:44 trett.txt
-rw-r--r-- 1 itl00student itl00student    5 2025-09-26 00:47 yourlastname
-rw-r--r-- 1 itl00student itl00student    0 2025-09-26 00:49 yourlastname.log
```

- 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?