Gurjot S Khakh

Professor Torres

9/21/2025

IT 100

Lab:5

- Copy parts A, B, and C from Canvas

Part A:

- Find the port numbers for the below ports, state what they do, and how you connect/use these ports:
  - FTP
  - SSH
  - Telnet
  - SMTP
  - DNS
  - DHCP
  - HTTP
  - POP3
  - NetBIOS/NetBT
  - IMAP
  - SNMP
  - LDAP
  - HTTPS
  - SMB/CIFS
  - RDP

- Part A:
- FTP: 20/21, File Transfer Protocol, 21 issues commands and receives responses and 20 is for transferring the acutal data during a FTP session, connect to an FTP server and the server manages control channel on 21 and data channel on 20
- SSH: 22, Secure Shell, 22 allows a way to securely connect and manage a remote computer over an unsecure network, use a client program for example SSH client that allows a connection to a server that has SSH server listening on port 22
- Telnet: 23, Transmission Control Protocol, used to remote command-line access to network devices and servers, use telnet client from CMD to connect to a Telnet server

- SMTP: 25, Simple Mail Transfer Protocol, server to server email communications to rely on messages between Mail Transfer agents (MTAs), open CMD use the telnet command and the server address then 25 and you will see a greeting message from the server if it works
- DNS: 53, Domain Name System, its a translation for machines, from readable domain names into machine readable IP addresses, configure a DNS server on your OS and then open port 53 on your firewall and change the settings to allos incoming and outgoing connections on port 53 through firewall, the devices that need to use DNS you have to configure them to lead them to your new DNS servers IP address
- DHCP: 67/68, Dynamic Host Configuration Protocol, uses a process called DORA (Discover, Offer, Request, Acknowledge), device sends a discover message to find a DHCP server, the server sends a response with a offer, the device then sends a request for the offered IP address and the server sends a message to confirm the lease and provide network configurations details, 67 used by DHCP servers to listen to client requests while port 68 is used by DHCP clients to send requests to servers
- HTTP: 80, Hypertext Transfer Protocol, a set of rules that web browsers and server communicate exchange data, works on request-response cycle, a clietn sends an HTTP request to a web server sends back a HTTP response containing the requested information, type a websites URL into a web browser to access the HTTP service running on a servers port 80
- POP3: 110(unsecure unencrypted connections) or 995(secure encrypted connections), Post Office Protocol 3, this is an email protocol which allows downloads for emails from a server to a user's local device even when offline then that deletes the email from the server thereafter which frees up space for the server, go to email providers settings for POP3 enable POP in the webmail then configure email client select POP, enter server information, choose the port and enable encryption
- NetBIOS/NetBT: 137(name services), 138(datagram services) 139(session services), Network Basic Input/Output System, for LANs mapps human-readable names to IP addresses for name resolution, datagram communication and session establishment, go to network adapters properties in windows selsect the IPv4 and click the properties then go to advanced settings then go the WINS tab select enable NETBIOS over TCP/IP

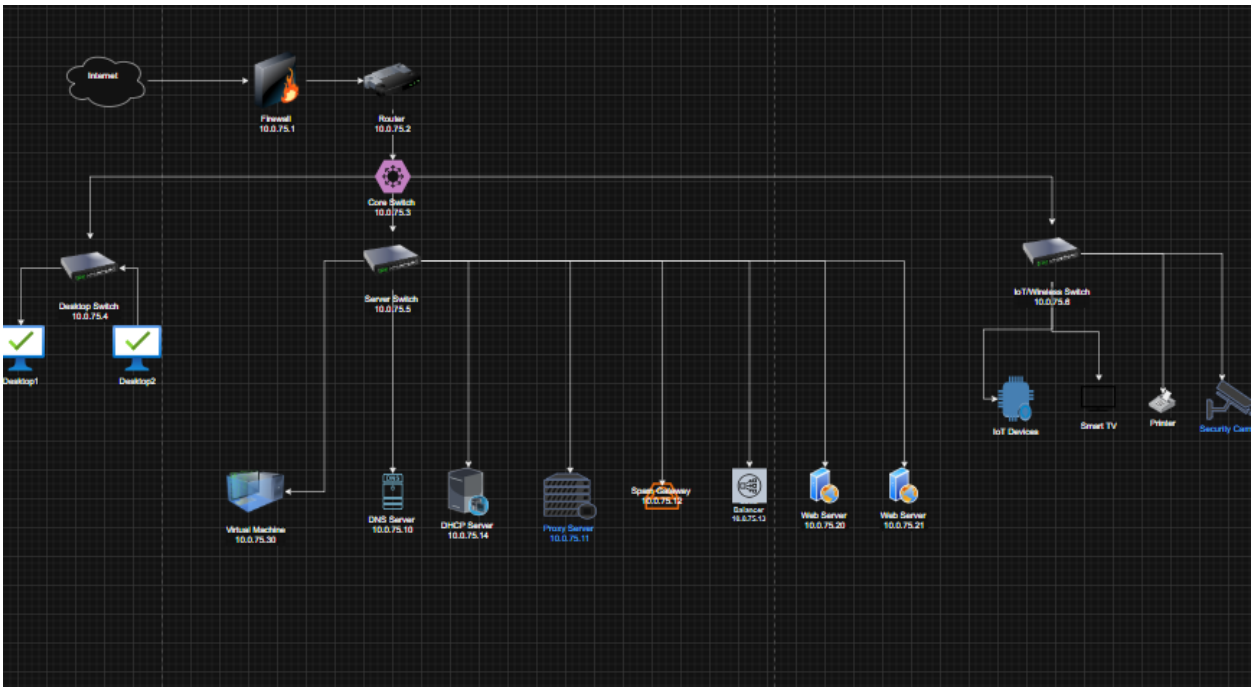
- IMAP: 143(unsecure connections unencrypted connections), 993(secure encrypted connections), Internet Message Access Protocol, allows you to store your messages a remote mail server while lets you access and manage and synchronize your emails across Mutiple devices and locations, access your email client go to settings and for advanced settings then input server details enter your IMAP IP address and add a colon followed by the port number after your hostname and then provide your credentials and select encryption and then sign in and test it, it is recommended to use port 993 because it is encrypted
- SNMP: 161(for requests and responses), 162(traps and notifications sent from the agent to the manager), Simple Network Management Protocol, allows network admins to monitor and manage network devices for example routers, switches and printers from a center location, turn on SNMP on the agent that you want to manage, configure the agent to listen on port 161 and also configure the agents security settings and then configure a SNMP manager on a server and make it use port 161 and listen to port 161 and then make sure the firewall is configured to allow UDP traffic on port 161 and 162 on both devices
- LDAP: 389(unsecure and unencrypted communication) 636(Secure and encrypted communication), Lightweight Directory Access Protocol, client needs access to information it sends an LDAP query to a server listening on port 389, then the server processes the request and sends back the relevant data, get the IP address of the server running LDAP directory, make it listen on port 389 and then Distinguished Name which is a starting point for directory tree for your searches and then authentication credentials
- HTTPS: 443, Hypertext Transfer Protocol Secure, a secure communication between a web browser and a website server protecting sensitive data like passwords and credit card information, one way to test is using CMD and using the telnet command for example telnet www.google.com 443 and it will test the connection another way for web browers is simply just by typing https before a websites domain name
- SMB/CIFS:445, (Server Message Block), (Common Internet File System), carries SMB protocol traffic for files, printers and other resources sharing on a network, mostly in Windows environments, on host computer enables file and printer sharing then on windows enable network discovery and then file and printer sharing will automaticall configure the necessary firewall rules to enable port 445 on the LAN

- RDP: 3389, Remote Desktop Protocol, this enables remote access and control of windows computers, first go to windows settings and enable remote desktop and then for the firewall configure it to allow it, system properties then go the remote desktop and then allow remote connections and then enable RDP and then configure firewall

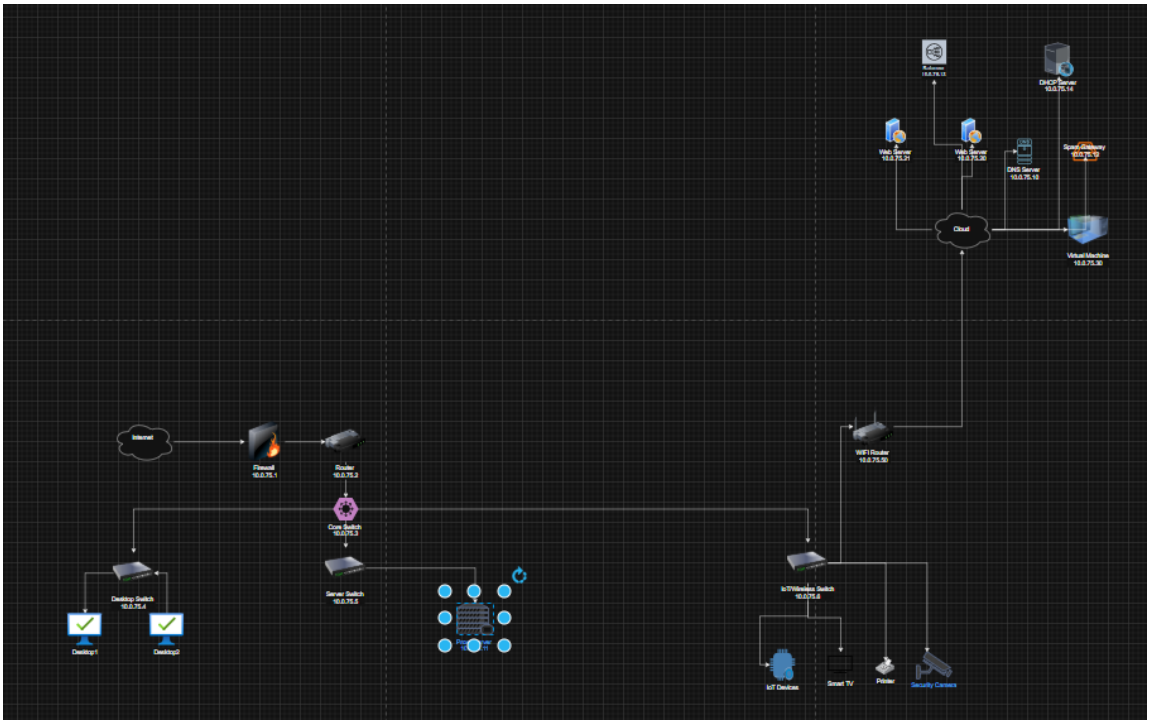
Part B:

- Using the online network diagram software https://app.diagrams.net/, draw 2 network diagrams. One diagram should have all of the below components in your local area network. The second diagram should show what you have moved to the cloud, with what is left over. Ensure that you give your opinion/view as to what is happening:
  - Router
  - Switch
  - Server
  - Desktop
  - Wireless router
  - DNS and DHCP server
  - Web server
  - Load balancer
  - Cloud services (AWS, office365)
  - Virtual machines
  - Spam gateways
  - Proxy server
  - IoT systems
  - Subnet range for your systems: 10.0.75.0/24

First diagram LAN:



Second Diagram:



Part C:

- Using your internet service provider as a reference, determine the network speeds in your house/apartment.
  - what options are available, what are the speeds
  - what can you do at each speed
- compare the above information for home and for business
  - What additional features are there for businesses
  - Why are business services so expensive

- Home network speeds:
- WLAN 5Ghz gets 1733 Mbps
- WLAN 2.4GHz gets 216 Mbps
- LAN gets 100M/Full
- Ethernet WAN 1000M/Full
- For each speed can do a lot of things for example 10-30 Mbps which is great for video calls great for 1 or 2 people
- 50-100 Mbps great for households that have many devices
- 200-300 top notch for households with a lot of devices
- 500-600 Mbps almost do everything at once if many devices are wired using 5 GHz
- Business Internet:
- WLAN 2.4GHz: several hundred Mbps under pretty good conditions
- WLAN 5GHz: Higher speeds throughput supports wider channels this is the newer so it will be more speed effective
- Small business: download speeds 50-200 Mbps, upload speeds 10-50 Mbps
- Medium business: download speeds 200-500 Mbps, upload speeds 50-500 Mbps
- Large business: download speeds 5-100+ Gbps, upload speeds: often very similar to download speeds
- Advanced security systems, Network Management and Monitoring, Better hardware/Coverage, User Management and control, Multiple SSID, backup units in place for reliability, Professional support and service level agreements, Guest WIFI
- They are more expensive for a quite few reasons for example, if the Wi-Fi goes down the service provider starts working on it right then and there, speeds are more faster than home internet, there is a guaranteed of uptime, also there are dedicated internet Access and low contended connections, more advanced network features, 24/7 business support and really fast response time, offers more customization.

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 wmic to view the serial number
2. Run the below command and explain the output: wmic cpu get caption, name, deviceid, numberofcores, maxclockspeed, status
3. Utilize wmic to list the total system memory
4. Utilize wmic to get hard drive partition details
5. Utilize wmic to get a list of all install products/software
6. Utilize wmic to get full system information
7. Utilize wmic to find updates applied
8. Utilize wmic to get a list of local accounts
9. List the help center for wmic
10. Use wmic to get the OS build and version

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

hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>wmic bios get serialnumber
SerialNumber
VMware-56 4d c0 01 fa 84 dd 75-e0 13 f0 9a 58 18 56 06


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

```
hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>wmic cpu get Caption, Name, DeviceID, NumberofCores, MaxClockSpeed, Status
Caption                           DeviceID  MaxClockSpeed  Name                              NumberOfCores  Status
AMD64 Family 23 Model 49 Stepping 0  CPU0      2994           AMD EPYC 7302 16-Core Processor  1              OK
AMD64 Family 23 Model 49 Stepping 0  CPU1      2994           AMD EPYC 7302 16-Core Processor  1              OK


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

```
hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>wmic computersystem get totalphysicalmemory
TotalPhysicalMemory
17179332608


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

```
hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>wmic partition get DeviceID, Name, Size, Type
DeviceID              Name                  Size          Type
Disk #0, Partition #0  Disk #0, Partition #0  104857600     Installable File System
Disk #0, Partition #1  Disk #0, Partition #1  69035098112   Installable File System
Disk #0, Partition #2  Disk #0, Partition #2  650117120     Unknown


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

```
hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>wmic product get name,version,vendor
Name                                                        Vendor                  Version
Microsoft Visual C++ 2022 X86 Additional Runtime - 14.38.33135  Microsoft Corporation  14.38.33135
Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.40.33816     Microsoft Corporation  14.40.33816
OpenSSH                                                     Microsoft Corporation   9.8.1.0
Wazuh Agent                                                 Wazuh, Inc.             4.11.2
7-Zip 24.08 (x64 edition)                                   Igor Pavlov             24.08.00.0
Microsoft Visual C++ 2022 X64 Additional Runtime - 14.40.33816  Microsoft Corporation  14.40.33816
Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.38.33135     Microsoft Corporation  14.38.33135


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

```
Host Name:                 HIDDENLEAF
OS Name:                   Microsoft Windows Server 2022 Standard
OS Version:                10.0.20348 N/A Build 20348
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Primary Domain Controller
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00453-60004-11857-AA860
Original Install Date:     10/4/2024, 3:45:33 PM
System Boot Time:          9/14/2025, 8:07:33 PM
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
                           [02]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 11/12/2020
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     16,383 MB
Available Physical Memory: 13,262 MB
Virtual Memory: Max Size:  18,815 MB
Virtual Memory: Available: 15,984 MB
Virtual Memory: In Use:    2,831 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    hiddenleaf.local
Logon Server:              N/A
Hotfix(s):                 3 Hotfix(s) Installed.
                           [01]: KB5046265
                           [02]: KB5048654
                           [03]: KB5044414
Network Card(s):           2 NIC(s) Installed.
                           [01]: Intel(R) 82574L Gigabit Network Connection
                                 Connection Name: Ethernet0
                                 Status:          Hardware not present
                           [02]: Intel(R) 82574L Gigabit Network Connection
                                 Connection Name: Ethernet1
                                 DHCP Enabled:    Yes
                                 DHCP Server:     172.16.99.1
                                 IP address(es)
                                 [01]: 172.16.99.4
                                 [02]: fe80::6ae9:3c12:9e35:ead6
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```

```
hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>wmic qfe list
Caption                                     CSName      Description      FixComments  HotFixID   InstallDate  InstalledBy          InstalledOn  Name  ServicePackInEffect  Status

http://support.microsoft.com/?kbid=5046265  HIDDENLEAF  Update                        KB5046265              NT AUTHORITY\SYSTEM  12/15/2024

https://support.microsoft.com/help/5048654  HIDDENLEAF  Security Update               KB5048654              NT AUTHORITY\SYSTEM  12/15/2024

                                            HIDDENLEAF  Security Update               KB5044414              NT AUTHORITY\SYSTEM  12/14/2024



hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>wmic qfe list full


Caption=http://support.microsoft.com/?kbid=5046265
CSName=HIDDENLEAF
Description=Update
FixComments=
HotFixID=KB5046265
InstallDate=
InstalledBy=NT AUTHORITY\SYSTEM
InstalledOn=12/15/2024
Name=
ServicePackInEffect=
Status=


Caption=https://support.microsoft.com/help/5048654
CSName=HIDDENLEAF
Description=Security Update
FixComments=
HotFixID=KB5048654
InstallDate=
InstalledBy=NT AUTHORITY\SYSTEM
InstalledOn=12/15/2024
Name=
ServicePackInEffect=
Status=


Caption=
CSName=HIDDENLEAF
Description=Security Update
FixComments=
HotFixID=KB5044414
InstallDate=
InstalledBy=NT AUTHORITY\SYSTEM
InstalledOn=12/14/2024
Name=
ServicePackInEffect=
Status=
```

```
hiddenleaf0\it100student@HIDDENLEAF C:\Users\it100student>wmic UserAccount where "LocalAccount=True" get Name
No Instance(s) Available.



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

```
hiddenleaf0\itl00student@HIDDENLEAF C:\Users\itl00student>wmic /?

WMIC is deprecated.

[global switches] <command>

The following global switches are available:
/NAMESPACE          Path for the namespace the alias operate against.
/ROLE               Path for the role containing the alias definitions.
/NODE               Servers the alias will operate against.
/IMPLEVEL           Client impersonation level.
/AUTHLEVEL          Client authentication level.
/LOCALE             Language id the client should use.
/PRIVILEGES         Enable or disable all privileges.
/TRACE              Outputs debugging information to stderr.
/RECORD             Logs all input commands and output.
/INTERACTIVE        Sets or resets the interactive mode.
/FAILFAST           Sets or resets the FailFast mode.
/USER               User to be used during the session.
/PASSWORD           Password to be used for session login.
/OUTPUT             Specifies the mode for output redirection.
/APPEND             Specifies the mode for output redirection.
/AGGREGATE          Sets or resets aggregate mode.
/AUTHORITY          Specifies the <authority type> for the connection.
/?[:<BRIEF|FULL>]   Usage information.

For more information on a specific global switch, type: switch-name /?


The following alias/es are available in the current role:
ALIAS                   - Access to the aliases available on the local system
BASEBOARD               - Base board (also known as a motherboard or system board) management.
BIOS                    - Basic input/output services (BIOS) management.
BOOTCONFIG              - Boot configuration management.
CDROM                   - CD-ROM management.
COMPUTERSYSTEM          - Computer system management.
CPU                     - CPU management.
CSPRODUCT               - Computer system product information from SMBIOS.
DATAFILE                - DataFile Management.
DCOMAPP                 - DCOM Application management.
DESKTOP                 - User's Desktop management.
DESKTOPMONITOR          - Desktop Monitor management.
DEVICEMEMORYADDRESS     - Device memory addresses management.
DISKDRIVE               - Physical disk drive management.
DISKQUOTA               - Disk space usage for NTFS volumes.
DMACHANNEL              - Direct memory access (DMA) channel management.
ENVIRONMENT             - System environment settings management.
FSDIR                   - Filesystem directory entry management.
GROUP                   - Group account management.
IDECONTROLLER           - IDE Controller management.
Press any key to continue, or press the ESCAPE key to stop
```

```
hiddenleaf0\itl00student@HIDDENLEAF C:\Users\itl00student>wmic os get Caption, Version, BuildNumber
BuildNumber  Caption                                  Version
20348        Microsoft Windows Server 2022 Standard  10.0.20348


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

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: type the comand to get a list of running processes

2: type the command to see real time processes running

3: type the command to show how long the system has been up

4 type the command to show kernel info

5: type the command to show how much total memory is in the systems

6: type the command to show processor details on the system

7: type the command to show all user accounts on the system

8: type the command to show all hard drive partitions on the system

9: type the command to show any wireless interfaces on the system

10: type the command to show any and all pci devices connected

```
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.0  21616 13428 ?        Ss   Sep05  11:50 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    Sep05   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   Sep05   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   Sep05   0:00 [rcu_par_gp]
root           5  0.0  0.0      0     0 ?        I<   Sep05   0:00 [slub_flushwq]
root           6  0.0  0.0      0     0 ?        I<   Sep05   0:00 [netns]
root           8  0.0  0.0      0     0 ?        I<   Sep05   0:00 [kworker/0:0H-events_highpri]
root          10  0.0  0.0      0     0 ?        I<   Sep05   0:00 [mm_percpu_wq]
root          11  0.0  0.0      0     0 ?        I    Sep05   0:00 [rcu_tasks_kthread]
root          12  0.0  0.0      0     0 ?        I    Sep05   0:00 [rcu_tasks_rude_kthread]
root          13  0.0  0.0      0     0 ?        I    Sep05   0:00 [rcu_tasks_trace_kthread]
root          14  0.0  0.0      0     0 ?        S    Sep05   2:25 [ksoftirqd/0]
root          15  0.0  0.0      0     0 ?        I    Sep05  10:30 [rcu_preempt]
root          16  0.0  0.0      0     0 ?        S    Sep05   0:08 [migration/0]
root          17  0.0  0.0      0     0 ?        S    Sep05   0:00 [idle_inject/0]
root          19  0.0  0.0      0     0 ?        S    Sep05   0:00 [cpuhp/0]
root          20  0.0  0.0      0     0 ?        S    Sep05   0:00 [cpuhp/1]
root          21  0.0  0.0      0     0 ?        S    Sep05   0:00 [idle_inject/1]
root          22  0.0  0.0      0     0 ?        S    Sep05   0:08 [migration/1]
root          23  0.0  0.0      0     0 ?        S    Sep05   1:44 [ksoftirqd/1]
root          28  0.0  0.0      0     0 ?        S    Sep05   0:00 [kdevtmpfs]
root          29  0.0  0.0      0     0 ?        I<   Sep05   0:00 [inet_frag_wq]
root          30  0.0  0.0      0     0 ?        S    Sep05   0:00 [kauditd]
root          31  0.0  0.0      0     0 ?        S    Sep05   0:02 [khungtaskd]
root          32  0.0  0.0      0     0 ?        S    Sep05   0:00 [oom_reaper]
root          34  0.0  0.0      0     0 ?        I<   Sep05   0:00 [writeback]
root          35  0.0  0.0      0     0 ?        S    Sep05   0:40 [kcompactd0]
root          36  0.0  0.0      0     0 ?        SN   Sep05   0:00 [ksmd]
root          38  0.0  0.0      0     0 ?        SN   Sep05   0:13 [khugepaged]
root          39  0.0  0.0      0     0 ?        I<   Sep05   0:00 [kintegrityd]
root          40  0.0  0.0      0     0 ?        I<   Sep05   0:00 [kblockd]
root          41  0.0  0.0      0     0 ?        I<   Sep05   0:00 [blkcg_punt_bio]
root          42  0.0  0.0      0     0 ?        I<   Sep05   0:00 [tpm_dev_wq]
root          43  0.0  0.0      0     0 ?        I<   Sep05   0:00 [edac-poller]
root          44  0.0  0.0      0     0 ?        I<   Sep05   0:00 [devfreq_wq]
root          45  0.0  0.0      0     0 ?        I<   Sep05   0:00 [kworker/1:1H-kblockd]
root          46  0.0  0.0      0     0 ?        S    Sep05   0:00 [kswapd0]
root          53  0.0  0.0      0     0 ?        I<   Sep05   0:00 [kthrotld]
root          55  0.0  0.0      0     0 ?        S    Sep05   0:00 [irq/24-pciehp]
root          56  0.0  0.0      0     0 ?        S    Sep05   0:00 [irq/25-pciehp]
root          57  0.0  0.0      0     0 ?        S    Sep05   0:00 [irq/26-pciehp]
```

```
top - 04:44:29 up 16 days,  7:43,  4 users,  load average: 0.24, 0.12, 0.10
Tasks: 428 total,   1 running, 427 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.8 us,  1.2 sy,  0.0 ni, 96.7 id,  1.0 wa,  0.0 hi,  0.3 si,  0.0 st
MiB Mem :  15993.2 total,   5171.0 free,   8138.0 used,   2978.9 buff/cache
MiB Swap:    976.0 total,    976.0 free,      0.0 used.   7855.3 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
    613 root      20   0  315892  13684   7552 S   0.3   0.1  18:22.09 vmtoolsd
   1319 kali      20   0  426752  41696  22848 S   0.3   0.3  43:56.96 panel-13-cpugra
   3393 root      20   0  720520  19896   8192 S   0.3   0.1   1:59.60 containerd-shim
   3584 root      20   0  720776  18932   8192 S   0.3   0.1   6:08.32 containerd-shim
   4815 kali      20   0 6839656 425856  28032 S   0.3   2.6  23:42.65 java
   7186 it100st+  20   0  398748 179996  32896 S   0.3   1.1  40:37.85 node
   7268 root      20   0  276336  23484  17536 S   0.3   0.1   0:46.99 apache2
3753865 it100st+  20   0    8740   5120   2944 R   0.3   0.0   0:00.08 top
      1 root      20   0   21616  13428   9332 S   0.0   0.1  11:51.13 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.30 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 slub_flushwq
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 netns
      8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
     10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
     11 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_kthread
     12 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_rude_kthread
     13 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_trace_kthread
     14 root      20   0       0      0      0 S   0.0   0.0   2:25.12 ksoftirqd/0
     15 root      20   0       0      0      0 I   0.0   0.0  10:31.23 rcu_preempt
     16 root      rt   0       0      0      0 S   0.0   0.0   0:08.50 migration/0
     17 root     -51   0       0      0      0 S   0.0   0.0   0:00.00 idle_inject/0
     19 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
     20 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/1
     21 root     -51   0       0      0      0 S   0.0   0.0   0:00.00 idle_inject/1
     22 root      rt   0       0      0      0 S   0.0   0.0   0:08.63 migration/1
     23 root      20   0       0      0      0 S   0.0   0.0   1:44.51 ksoftirqd/1
     28 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kdevtmpfs
     29 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 inet_frag_wq
     30 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kauditd
     31 root      20   0       0      0      0 S   0.0   0.0   0:02.76 khungtaskd
     32 root      20   0       0      0      0 S   0.0   0.0   0:00.00 oom_reaper
     34 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 writeback
     35 root      20   0       0      0      0 S   0.0   0.0   0:40.56 kcompactd0
     36 root      25   5       0      0      0 S   0.0   0.0   0:00.00 ksmd
     38 root      39  19       0      0      0 S   0.0   0.0   0:13.52 khugepaged
     39 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kintegrityd
     40 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kblockd
     41 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 blkcg_punt_bio
     42 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 tpm_dev_wq
     43 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 edac-poller
     44 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 devfreq_wq
     45 root       0 -20       0      0      0 I   0.0   0.0   0:00.21 kworker/1:1H-kblockd
```

```
┌──(it100student㉿Kali)-[~]
└─$ uptime
 04:46:53 up 16 days,  7:45,  4 users,  load average: 0.02, 0.07, 0.08

┌──(it100student㉿Kali)-[~]
└─$ uptime -s
2025-09-05 21:01:04

┌──(it100student㉿Kali)-[~]
└─$ uptime -p
up 2 weeks, 2 days, 7 hours, 46 minutes

┌──(it100student㉿Kali)-[~]
└─$ cat /proc/uptime
1410404.09 2722782.11

┌──(it100student㉿Kali)-[~]
└─$
```

```
┌──(it100student㉿Kali)-[~]
└─$ uname
Linux

┌──(it100student㉿Kali)-[~]
└─$ uname -a
Linux Kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) x86_64 GNU/Linux

┌──(it100student㉿Kali)-[~]
└─$ uname -r
6.3.0-kali1-amd64

┌──(it100student㉿Kali)-[~]
└─$
```

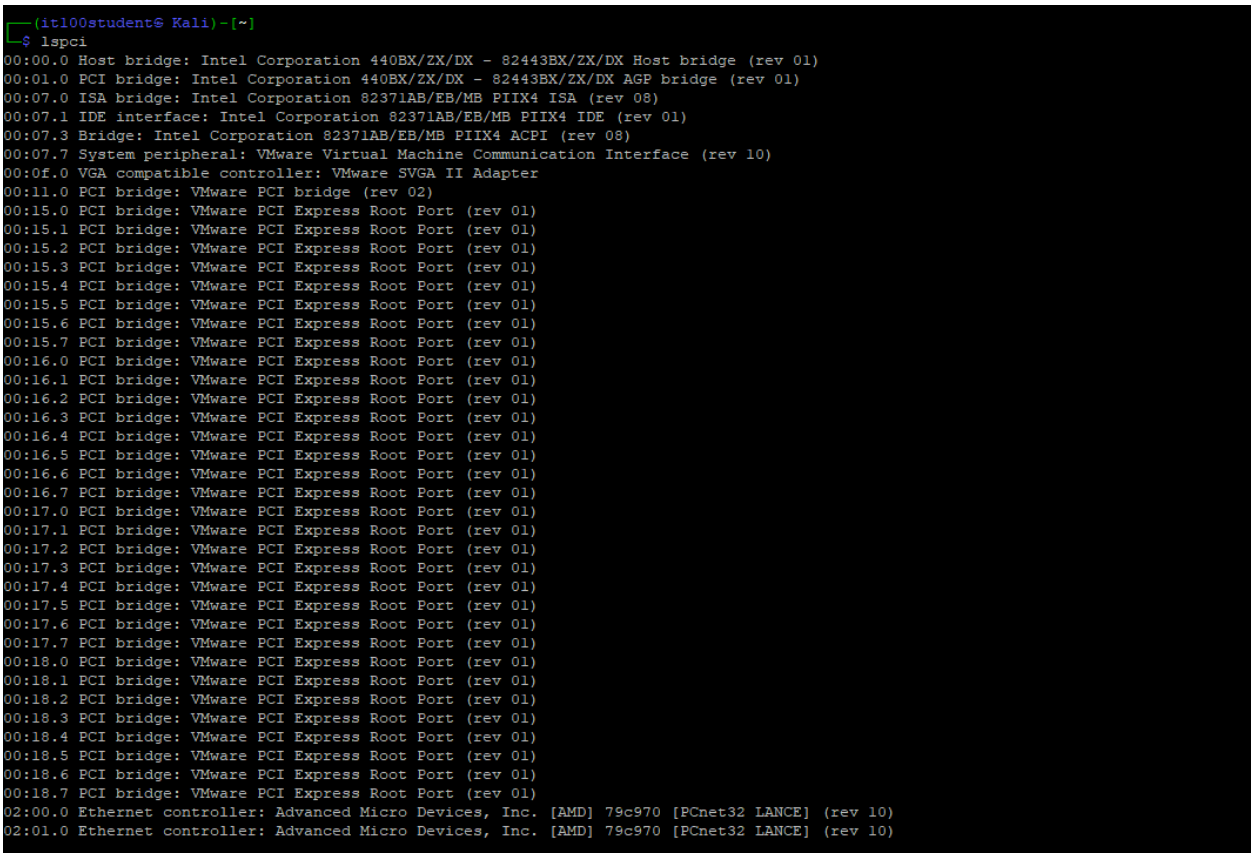
```
┌──(it100student㉿Kali)-[~]
└─$ free -h -t
               total        used        free      shared  buff/cache   available
Mem:            15Gi       8.0Gi       5.0Gi        43Mi       2.9Gi       7.7Gi
Swap:          975Mi          0B       975Mi
Total:          16Gi       8.0Gi       6.0Gi

┌──(it100student㉿Kali)-[~]
└─$ cat /proc/meminfo
MemTotal:       16377080 kB
MemFree:         5286760 kB
MemAvailable:    8035756 kB
Buffers:          711076 kB
Cached:          1811548 kB
SwapCached:            0 kB
Active:          1730920 kB
Inactive:        8483944 kB
Active(anon):       4096 kB
Inactive(anon):  7652276 kB
Active(file):    1726824 kB
Inactive(file):   831668 kB
Unevictable:         112 kB
Mlocked:             112 kB
SwapTotal:        999420 kB
SwapFree:         999420 kB
Zswap:                 0 kB
Zswapped:              0 kB
Dirty:               268 kB
Writeback:             0 kB
AnonPages:       7654248 kB
Mapped:           557468 kB
Shmem:             45016 kB
KReclaimable:     527980 kB
Slab:             637436 kB
SReclaimable:     527980 kB
SUnreclaim:       109456 kB
KernelStack:       17936 kB
```

```
┌──(it100student㉿Kali)-[~]
└─$ lscpu
Architecture:            x86_64
  CPU op-mode(s):        32-bit, 64-bit
  Address sizes:         43 bits physical, 48 bits virtual
  Byte Order:            Little Endian
CPU(s):                  2
  On-line CPU(s) list:   0,1
Vendor ID:               AuthenticAMD
  Model name:            AMD EPYC 7302 16-Core Processor
    CPU family:          23
    Model:               49
    Thread(s) per core:  1
    Core(s) per socket:  1
    Socket(s):           2
    Stepping:            0
    BogoMIPS:            5988.74
    Flags:               fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 syscall nx mmxext fxsr_opt pdpelgb rdtscp lm constant_
                         tsc rep_good nopl tsc_reliable nonstop_tsc cpuid extd_apicid tsc_known_freq pni pclmulqdq ssse3 fma cx16 sse4_1 sse4_2 x2apic movbe popcnt aes xsave avx
                          f16c rdrand hypervisor lahf_lm extapic cr8_legacy abm sse4a misalignsse 3dnowprefetch osvw ssbd ibpb vmmcall fsgsbase bmi1 avx2 smep bmi2 rdseed adx sm
                         ap clflushopt clwb sha_ni xsaveopt xsavec clzero arat overflow_recov succor
Virtualization features:
  Hypervisor vendor:     VMware
  Virtualization type:   full
Caches (sum of all):
  L1d:                   64 KiB (2 instances)
  L1i:                   64 KiB (2 instances)
  L2:                    1 MiB (2 instances)
  L3:                    256 MiB (2 instances)
NUMA:
  NUMA node(s):          1
  NUMA node0 CPU(s):     0,1
Vulnerabilities:
  Itlb multihit:         Not affected
  L1tf:                  Not affected
  Mds:                   Not affected
  Meltdown:              Not affected
  Mmio stale data:       Not affected
  Retbleed:              Mitigation; untrained return thunk; SMT disabled
  Spec store bypass:     Mitigation; Speculative Store Bypass disabled via prctl
  Spectre v1:            Mitigation; usercopy/swapgs barriers and __user pointer sanitization
  Spectre v2:            Mitigation; Retpolines, IBPB conditional, STIBP disabled, RSB filling, PBRSB-eIBRS Not affected
  Srbds:                 Not affected
  Tsx async abort:       Not affected

┌──(it100student㉿Kali)-[~]
└─$ cat /proc/cpuinfo
processor       : 0
vendor_id       : AuthenticAMD
cpu family      : 23
```

```
┌──(itl00student㉿Kali)-[~]
└─$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
mysql:x:100:107:MySQL Server,,,:/nonexistent:/bin/false
tss:x:101:108:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
redsocks:x:103:109::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:104:65534::/var/spool/rwho:/usr/sbin/nologin
_gophish:x:105:111::/var/lib/gophish:/usr/sbin/nologin
iodine:x:106:65534::/run/iodine:/usr/sbin/nologin
messagebus:x:107:112::/nonexistent:/usr/sbin/nologin
miredo:x:108:65534::/var/run/miredo:/usr/sbin/nologin
redis:x:109:115::/var/lib/redis:/usr/sbin/nologin
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
mosquitto:x:111:117::/var/lib/mosquitto:/usr/sbin/nologin
tcpdump:x:112:119::/nonexistent:/usr/sbin/nologin
sshd:x:113:65534::/run/sshd:/usr/sbin/nologin
_rpc:x:114:65534::/run/rpcbind:/usr/sbin/nologin
dnsmasq:x:115:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
statd:x:116:65534::/var/lib/nfs:/usr/sbin/nologin
avahi:x:117:123:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
stunnel4:x:996:996:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
Debian-snmp:x:118:124::/var/lib/snmp:/bin/false
_gvm:x:119:125::/var/lib/openvas:/usr/sbin/nologin
speech-dispatcher:x:120:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
sslh:x:121:126::/nonexistent:/usr/sbin/nologin
postgres:x:122:127:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
pulse:x:123:129:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
inetsim:x:124:131::/var/lib/inetsim:/usr/sbin/nologin
lightdm:x:125:132:Light Display Manager:/var/lib/lightdm:/bin/false
geoclue:x:126:133::/var/lib/geoclue:/usr/sbin/nologin
```

```
┌──(itl00student㉿Kali)-[~]
└─$ lsblk
NAME                                  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda                                     8:0    0   75G  0 disk
|-sda1                                  8:1    0  487M  0 part /boot
|-sda2                                  8:2    0    1K  0 part
`-sda5                                  8:5    0 38.6G  0 part
  |-Ethical--Hacker--Kali--vg-root   254:0    0 37.6G  0 lvm  /
  `-Ethical--Hacker--Kali--vg-swap_1 254:1    0  976M  0 lvm  [SWAP]
sr0                                    11:0    1 1024M  0 rom

┌──(itl00student㉿Kali)-[~]
└─$ fdisk -l
fdisk: invalid option -- 'l'
Try 'fdisk --help' for more information.

┌──(itl00student㉿Kali)-[~]
└─$ sudo fdisk -l
[sudo] password for itl00student:
Sorry, user itl00student is not allowed to execute '/usr/sbin/fdisk -l' as root on Kali.vm.

┌──(itl00student㉿Kali)-[~]
└─$ df -h
Filesystem                                Size  Used Avail Use% Mounted on
udev                                      7.8G     0  7.8G   0% /dev
tmpfs                                     1.6G  2.3M  1.6G   1% /run
/dev/mapper/Ethical--Hacker--Kali--vg-root   37G   27G  8.6G  76% /
tmpfs                                     7.9G     0  7.9G   0% /dev/shm
tmpfs                                     5.0M     0  5.0M   0% /run/lock
/dev/sda1                                 455M   96M  335M  23% /boot
tmpfs                                     1.6G  120K  1.6G   1% /run/user/1000
tmpfs                                     1.6G  112K  1.6G   1% /run/user/125
tmpfs                                     1.6G  108K  1.6G   1% /run/user/1001

┌──(itl00student㉿Kali)-[~]
└─$
```

```
┌──(itl00student㉿Kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

br-339414195aeb  no wireless extensions.

br-355ee7945a88  no wireless extensions.

br-internal  no wireless extensions.

docker0   no wireless extensions.

veth8333407  no wireless extensions.

vethc1a025a  no wireless extensions.

veth4cbb037  no wireless extensions.

veth4a3e3d4  no wireless extensions.

veth08e13ba  no wireless extensions.

veth03e144d  no wireless extensions.

vethdf5c130  no wireless extensions.

veth7195f2b  no wireless extensions.

veth819e8dc  no wireless extensions.

vethdf6cec3  no wireless extensions.

vethadaa110  no wireless extensions.

veth7ea0c31  no wireless extensions.

veth514f370  no wireless extensions.
```



- 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?