# The Hong Kong University of Science and Technology

**School of Engineering**

**Department of Computer Science and Engineering**

Industrial Training Course:

USTM17 – Linux System Administration (Workbook)

|  |  |
| --- | --- |
| Student Name: |  |
| Student ID: |  |
| Department: |  |
| Group: |  |

# Lab Information Sheet

**DO NOT** have food or drink in the lab at any time.

|  |  |
| --- | --- |
| Local hostname |  |
| IP address (ipv4) |  |
| IP address (ipv6) |  |
| Ethernet network interface name |  |
| Network address / Netmask  *Format: [IP address] / [number]* |  |
| Root password |  |

NOTE

1. Use the root account with an **extreme** caution, because what you can do as a root user will affect your classmates

# Section 1: General Concepts in Networking

## Task 1.1 (Lesson 3)

You are given a Class B IP address and are to create a subnetwork mask using high order bits of host-id field of the address.

For each given number of high order bits of the host-id field in the table below, determine the:

* Dotted decimal notation of the subnetwork mask
* Binary value of the subnetwork number

|  |  |  |
| --- | --- | --- |
| **Number of Host-id Bits** | **Subnetwork Mask** | **Binary Value of Subnet Number** |
| 0 | 255.255.0.0 | 0000 0000 |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |
| 6 |  |  |
| 7 |  |  |
| 8 | 255.255.255.0 | 1111 1111 |

## Task 1.2 (Lesson 3)

Given the IP address 143.89.14.7 (ustsu1.ust.hk) and subnet masks of 255.255.252.0, determine the following:

|  |  |
| --- | --- |
| Network Address |  |

## Task 1.3 (Lesson 4)

Use ip link to display information about the network interface on your machines. What are the network interfaces? **Write down the network interfaces. You are not required to take screenshots.**

Use ip address (or ip addr in short) to display IP address (IPv4) of the network interfaces. What are the IP addresses? **Write down the IP addresses of the interfaces.**

Use ip route show to display entries in the routing table. The entry default via X is the default route, where X is the default gateway. What is the default gateway? **Write down the default gateway.**

Find out the currently assigned DNS servers in the file /etc/resolv.conf. What is the DNS server(s) assigned?

## Task 1.4 (Lesson 3)

The ping command can be used to check network connectivity, by sending ICMP (Internet Control Message Protocol) packets.

Use ping to **www.google.com** (Press CTRL+C to stop). **Write down the command you used.**

The ARP (Address Resolution Protocol) table can be displayed using ip neigh show. The ARP table contains cached replies from ARP, which are mappings from network address (IP address) to link-layer address (MAC address). What are the entries in the ARP table? **Write down the entries in the ARP table.**

## Task 1.5 (Lesson 4)

Routing table provides information for packet forwarding, which is necessary when the destination of a packet does not reside in the same network of the source. Routing table can be modified and queried using subcommands of ip route.

Before you proceed, verify the network connectivity (using ping) to the following three hosts (use ping to IP address). **If you are stuck in this task, reset the VM and restart.**

* 143.89.44.244 (eesvr4.ece.ust.hk)
* 143.89.7.44 (smtp.ust.hk)
* 143.89.41.171 (coffee.cse.ust.hk)

Remove the default route. **Write down the command you used.** Verify the connectivity is lost.

Add route to ECE network 143.89.44.0/24. **Write down the command you used.** Verify the connectivity to 143.89.44.244 only.

Add route to the host 143.89.7.44 only. **Write down the command you used.** Verify the connectivity.

Delete the above two routes and add route to CSE network 143.89.40.0/22. **Write down the commands you used.** Verify the connectivity to 143.89.41.171 only.

Restore the default routing table. **Write down the commands you used.** Verify using ip route show.

## Task 1.6 (Lesson 4)

Use traceroute -I to the following hosts:

* webhost2.ece.ust.hk
* smtp.ust.hk
* coffee.cse.ust.hk
* www.ust.hk
* www.gov.hk
* www.google.com

Figure out the network topology with respect to the above hosts. **Represent each (available) intermediate node with a box.** An example, info7.cse.ust.hk, is done for you.



## Task 1.7 (Lesson 4)

Wireshark is a useful utility for capturing and showing network traffic (packets). The command-line program is tshark.

**Write down the command** to capture and display all packets on a network interface. **You are not required to show the output from tshark**.

**Write down the command** to configure tshark to write the capture to file.

**Write down the command** to ask tshark to read the capture from file.

**Write down the command** to filter only ICMP packets (ping messages).

**Write down the command** to filter HTTP traffic (TCP port 80).

**Write down the command** to configure tshark to display source IP, source port, destination IP and destination port only.

**Write down the command** to configure tshark to customize output to show headers and use space as separator.

# Section 2: Firewall

## Task 2.1 (Lesson 8)

The firewall can be configured using firewall-cmd.

Verify the firewall daemon is running, by the command   
systemctl status firewalld.

List out the currently allowed services. What are the services allowed by the firewall? **Write down the command you used and list out the currently allowed services.**

The list of services supported by firewall-cmd is given by firewall-cmd --list-services.

Block SSH traffic in the firewall. **Write down the command you used.**

Allow SSH traffic in the firewall. **Write down the command you used.**

## Task 2.2 (Lesson 8)

To achieve a more fine-grained control of packet filtering, nftables is a good choice.

List out the tables of nftables. **Write down the command you used and the list of tables.**

List out the chains and the underlying rules of the table ip filter. **Write down the command you used and the output.**

Add a rule to drop all ICMP packets. **Write down the command you used.** Verify that ping no longer works.

Add a rule to drop all outgoing HTTP traffic. **Write down the command you used.** Verify this with wget.

List out the chains and the underlying rules of the table ip filter. **Write down the output.**

Remove all rules by flushing the table ip filter. **Write down the command you used.**

# Section 3: Domain Name System

## Task 3.1 (Lesson 5)

Start the DNS server by the following command:  
systemctl start named.

Edit the configuration file /etc/named.conf:

1. Configure the DNS server to listen on all interfaces and all IP addresses, change:

listen-on port 53 { 127.0.0.1; };

listen-on-v6 port 53 { ::1; };

to:

listen-on port 53 { any; };

listen-on-v6 port 53 { any; };

1. Add the local network to allow-query. For example,

allow-query { localhost; 143.89.130.0/24; };

1. Add a forward zone before zone "." IN, replace ITSC\_LOGIN with your ITSC login name.

zone "<ITSC\_LOGIN>.cse.ust.hk" IN {

type master;

file "<ITSC\_LOGIN>.db";

allow-update { none; };

allow-query { any; };

};

1. Add a backward zone after the forward zone, replace ITSC\_LOGIN with your ITSC login name.

zone "1.168.192.in-addr.arpa" IN {

type master;

file "<ITSC\_LOGIN>.rev";

allow-update { none; };

allow-query { any; };

};

Create a file for the forward zone at /var/named/<ITSC\_LOGIN>.db. Replace 143.89.130.89 with your IP address.

$TTL 86400

@ IN SOA dns.<ITSC\_LOGIN>.cse.ust.hk. <ITSC\_LOGIN>.ust.hk. (

2020011800 ;Serial

3600 ;Refresh

1800 ;Retry

604800 ;Expire

86400 ;Minimum TTL

)

;Name Server Information

@ IN NS dns.<ITSC\_LOGIN>.cse.ust.hk.

;IP Address for Name Server

dns IN A ***143.89.130.89***

;A Record for the following Host name

www IN A 192.168.1.10

mail IN A 192.168.1.20

;CNAME Record

ftp IN CNAME www.<ITSC\_LOGIN>.cse.ust.hk.

Create a file for the backward zone at /var/named/<ITSC\_LOGIN>.rev.

$TTL 86400

@ IN SOA dns.<ITSC\_LOGIN>.cse.ust.hk. <ITSC\_LOGIN>.ust.hk. (

2020011800 ;Serial

3600 ;Refresh

1800 ;Retry

604800 ;Expire

86400 ;Minimum TTL

)

;Name Server Information

@ IN NS dns.<ITSC\_LOGIN>.cse.ust.hk.

;PTR Record IP address to Hostname

10 IN PTR www.testuser.cse.ust.hk.

Restart the DNS server by the following command:  
systemctl restart named.

Edit the /etc/resolv.conf to use the DNS server on the local machine. **Add the line in bold. Replace 143.89.130.252 with your IP address.**

search cse.ust.hk

***nameserver 143.89.130.252***

nameserver 143.89.129.254

nameserver 143.89.40.46

## Task 3.2 (Lesson 5)

Use nslookup to query the DNS for the host www.<ITSC\_LOGIN>.cse.ust.hk. **Write down the command you used and the output.**

Use nslookup to query the DNS for the host mail.<ITSC\_LOGIN>.cse.ust.hk. **Write down the command you used and the output.**

Use nslookup to query the DNS for the host ftp.<ITSC\_LOGIN>.cse.ust.hk. **Write down the command you used and the output.**

Use nslookup to query the DNS for the host 192.168.1.10. **Write down the command you used and the output.**

# Section 4: Directory Services

## Task 4.1 (Lesson 6)

Download the latest release of OpenLDAP from <https://www.openldap.org/software/download/>

For example,

# wget \

https://www.openldap.org/software/download/OpenLDAP/openldap-release/openldap-2.4.52.tgz

Extract the source tar file and change directory into it.

# tar -xf openldap-2.4.52.tgz

# cd openldap-2.4.52

Configure the source.

# ./configure --with-cyrus-sasl --with-tls=openssl \

--enable-overlays=mod --enable-backends=mod \

--disable-perl --disable-ndb --enable-crypt \

--enable-modules --enable-dynamic --enable-syslog \

--enable-debug --enable-local \

--enable-spasswd --disable-sql

Compile the source.

# make depend

# make

Install the source.

# make install

Create ldap user and group, and fix permission.

# groupadd -g 55 ldap

# useradd -g 55 -u 55 -s /sbin/nologin -d /var/lib/ldap \

-c "OpenLDAP server" ldap

# chown ldap:ldap /usr/local/var/run

Create systemd unit file, /etc/systemd/system/slapd.service.  
**Note: All configuration files are available at /root/openldap. These can be simply copied to the desired locations.**

[Unit]

Description=OpenLDAP Server Daemon

After=syslog.target network-online.target

[Service]

Type=forking

PIDFile=/usr/local/var/run/slapd.pid

EnvironmentFile=/etc/sysconfig/slapd

ExecStart=/usr/local/libexec/slapd -u ldap -g ldap -h ${SLAPD\_URLS} $SLAPD\_OPTIONS

[Install]

WantedBy=multi-user.target

Create environment file for the systemd unit file, /etc/sysconfig/slapd.

SLAPD\_OPTIONS="-F /usr/local/etc/openldap/slapd.d"

SLAPD\_URLS="ldapi:/// ldap:/// ldaps:///"

Create certificates, leave everything blank (press Enter) except Common Name. Find out the hostname using hostname, for example, vml1wk089.cse.ust.hk. Enter the hostname for Common Name.

# openssl req -days 500 -newkey rsa:4096 -keyout \  
 /etc/ssl/certs/ldapkey.pem -nodes -sha256 -x509 -out \  
 /etc/ssl/certs/ldapcert.pem

Fix permission and create CA certificate.

# chown ldap:ldap /etc/ssl/certs/ldapkey.pem

# chmod 400 /etc/ssl/certs/ldapkey.pem

# cat /etc/ssl/certs/ldapcert.pem >> \  
 /etc/ssl/certs/cacerts.pem

Load the systemd unit.

# systemctl daemon-reload

Edit configuration file, /usr/local/etc/openldap/slapd.ldif.

dn: cn=config

objectClass: olcGlobal

cn: config

olcArgsFile: /usr/local/var/run/slapd.arg

olcPidFile: /usr/local/var/run/slapd.pid

olcTLSCACertificateFile: /etc/ssl/certs/cacerts.pem

olcTLSCertificateFile: /etc/ssl/certs/ldapcert.pem

olcTLSCertificateKeyFile: /etc/ssl/certs/ldapkey.pem

olcTLSCipherSuite: TLSv1.2:HIGH:!aNULL:!eNULL

olcTLSProtocolMin: 3.3

dn: cn=schema,cn=config

objectClass: olcSchemaConfig

cn: schema

dn: cn=module,cn=config

objectClass: olcModuleList

cn: module

olcModulepath: /usr/local/libexec/openldap

olcModuleload: back\_mdb.la

include: file:///usr/local/etc/openldap/schema/core.ldif

include: file:///usr/local/etc/openldap/schema/cosine.ldif

include: file:///usr/local/etc/openldap/schema/nis.ldif

include: file:///usr/local/etc/openldap/schema/inetorgperson.ldif

include: file:///usr/local/etc/openldap/schema/ppolicy.ldif

dn: olcDatabase=frontend,cn=config

objectClass: olcDatabaseConfig

objectClass: olcFrontendConfig

olcDatabase: frontend

olcPasswordHash: {SSHA}

olcAccess: to \* by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage by \* none

dn: olcDatabase=config,cn=config

objectClass: olcDatabaseConfig

olcDatabase: config

olcRootDN: cn=config

olcAccess: to \* by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage by \* none

Create configuration directory.

# cd /usr/local/etc/openldap/

# mkdir slapd.d || rm -rf slapd.d/\*

Load the configuration file and fix permission.

# cd /usr/local/etc/openldap/

# slapadd -n 0 -F slapd.d -l slapd.ldif

# chown -R ldap:ldap slapd.d

# chmod -R o-rwx slapd.d

You should see no error from the output.

[root@vml1wk089 openldap]# slapadd -n 0 -F slapd.d -l slapd.ldif

\_#################### 100.00% eta none elapsed none fast!

Closing DB...

Start the service.

# systemctl start slapd

Verify that the OpenLDAP server is running.

# systemctl status slapd

Check the journal if errors occurred.

# journalctl -xe

## Task 4.2 (Lesson 6)

Change into the home directory.

# cd

Generate a password hash using slappasswd.

Create a file for database configuration, databases.ldif. Replace PASSWD\_HASH by the hash generated by slappasswd (enter the root login password).

dn: olcDatabase=mdb,cn=config

objectClass: olcDatabaseConfig

objectClass: olcMdbConfig

olcDatabase: mdb

olcSuffix: dc=cse,dc=ust,dc=hk

olcRootDN: cn=admin,dc=cse,dc=ust,dc=hk

olcRootPW: PASSWD\_HASH

olcDbDirectory: /var/lib/ldap

olcDbIndex: objectClass,uid,uidNumber,gidNumber eq

olcDbMaxSize: 10485760

olcAccess: to attrs=userPassword

by self write

by anonymous auth

by dn.subtree="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage

by \* none

olcAccess: to attrs=shadowLastChange by self write

by dn.subtree="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage

by dn.subtree="ou=system,dc=cse,dc=ust,dc=hk" read

by \* none

olcAccess: to dn.subtree="ou=system,dc=cse,dc=ust,dc=hk" by dn.subtree="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage

by \* none

olcAccess: to dn.subtree="dc=cse,dc=ust,dc=hk" by dn.subtree="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage

by users read

by \* none

Add the database configuration.

# ldapadd -Y EXTERNAL -H ldapi:/// -f databases.ldif

Create a file for directory configuration, directories.ldif.

dn: dc=cse,dc=ust,dc=hk

objectClass: dcObject

objectClass: organization

objectClass: top

o: CSE

dc: cse

dn: ou=groups,dc=cse,dc=ust,dc=hk

objectClass: organizationalUnit

objectClass: top

ou: groups

dn: ou=users,dc=cse,dc=ust,dc=hk

objectClass: organizationalUnit

objectClass: top

ou: users

dn: ou=system,dc=cse,dc=ust,dc=hk

objectClass: organizationalUnit

objectClass: top

ou: system

Add the directory configuration.

# ldapadd -Y EXTERNAL -H ldapi:/// -f directories.ldif

Generate a password hash using slappasswd.

Create a file for proxy user, proxy.ldif. Replace PASSWD\_HASH by the hash generated by slappasswd (enter the root login password).

dn: cn=osproxy,ou=system,dc=cse,dc=ust,dc=hk

objectClass: organizationalRole

objectClass: simpleSecurityObject

cn: osproxy

userPassword: PASSWD\_HASH

description: OS proxy for resolving UIDs/GIDs

Add the proxy user.

# ldapadd -Y EXTERNAL -H ldapi:/// -f proxy.ldif

Create a file for test user, testuser.ldif.

dn: cn=testgroup,ou=groups,dc=cse,dc=ust,dc=hk

objectClass: posixGroup

cn: testgroup

gidNumber: 5000

memberUid: testuser

dn: uid=testuser,ou=users,dc=cse,dc=ust,dc=hk

objectClass: posixAccount

objectClass: shadowAccount

objectClass: inetOrgPerson

cn: First Name

sn: Last Name

uid: testuser

uidNumber: 5000

gidNumber: 5000

homeDirectory: /home/testuser

loginShell: /bin/sh

gecos: Full Name

Add the test user.

# ldapadd -Y EXTERNAL -H ldapi:/// -f testuser.ldif

Set password for test user. Enter the root login password.

# ldappasswd -Y EXTERNAL -H ldapi:/// -S \  
"uid=testuser,ou=users,dc=cse,dc=ust,dc=hk"

## Task 4.3 (Lesson 6)

Configure SSSD.

# authselect select --force sssd

Create the SSSD configuration file /etc/sssd/sssd.conf. Replace LDAP\_PASSWORD by the password (NOT the hash!) of the proxy user.

[sssd]

services = nss, pam

# Which SSSD services are started.

# A separate process for each service is started

#debug\_level = 9

# The amount of detail in the logs. Uncomment this and adjust as needed.

# Level 9 is the most detailed level available.

domains = cse

# A list of domains to check when a client makes a request. They are

# checked in the oder listed. The domains listed must have a matching

# configuration section in the format [domain/domainname]

[pam]

# The verbosity of output and logging related to PAM requests. Uncomment

# and adjust as needed. As with the main section, 9 is maximum verbosity.

#pam\_verbosity = 9

#debug\_level = 9

[domain/cse]

cache\_credentials = true

# This enables or disables credential caching. I.e. after successfully

# authenticating a user, the credentials will be stored locally. If the

# domain is unavailable, users will still be able to login using the

# cached information.

#account\_cache\_expiration = 0

# By default, the credential cache never expires. If you want sssd to

# remove cached credentials, this option will cause them to expire

# after the number of days it is set to.

#debug\_level = 9

# The verbosity of this domains log file.

id\_provider = ldap

# SSSD can resolve user information from a number of different sources

# such as LDAP, local files, and Active Directory. This option sets

# the domain's source of identity information.

#auth\_provider = ldap

# As with identity providers, SSSD can authenticate in a variety of ways.

# By default, SSSD will use the value of id\_provider.

access\_provider = ldap

# The access provider controls the source for determining who is allowed

# to access the system. Even if a user successfully authenticates, if they

# don't meet the criteria provider by the access provider, they will be

# denied access.

ldap\_access\_order = filter

ldap\_access\_filter = (objectClass=posixAccount)

# These define the criteria the access provider uses to control who

# is allowed to login. In this case, any user that matches the

# LDAP filter in this example will be allowed access. Any entry

# that has an objectClass of posixAccount will be allowed access.

ldap\_uri = ldaps://localhost

# The URI(s) of the directory server(s) used by this domain.

ldap\_search\_base = dc=cse,dc=ust,dc=hk

# The LDAP search base you want SSSD to use when looking

# for entries. There are options for search bases for various types

# of searches, such as users. Read the sssd-ldap man page for details.

ldap\_tls\_cacert = /etc/ssl/certs/cacerts.pem

# The file containing CA certificates you want sssd to trust.

ldap\_tls\_cipher\_suite = HIGH

# The TLS ciphers you wish to use. SSSD uses OpenSSL style cipher

# suites

ldap\_default\_bind\_dn = cn=osproxy,ou=system,dc=cse,dc=ust,dc=hk

# The DN used to search your directory with. It must have read access to

# everything your system needs.

ldap\_default\_authtok = LDAP\_PASSWORD

# The password of the bind DN.

ldap\_tls\_reqcert = never

# This defines how sssd will handle server certificates. Demand means

# that we are requiring the host portion of the URI to match the

# certificate's subject or an SAN, the current time is within the valid

# times on the certificate, and that it's signing chain ends with a CA

# in the file defined by ldap\_tls\_cacert.

Fix permission.

# chmod 600 /etc/sssd/sssd.conf

Restart SSSD service.

# systemctl restart sssd

Verify the test user exists in the directory.

[root@vml1wk089 ~]# id testuser

uid=5000(testuser) gid=5000(testgroup) groups=5000(testgroup)

Create home directory for the test user, and fix permission.

# mkdir /home/testuser

# chown testuser:testgroup /home/testuser

Verify you can login as the test user. Use the password you set for the test user.  
Note: You may need to enter “yes” to accept the SSH key.

# ssh -l testuser localhost

# Section 5: Network File System

## Task 5.1 (Lesson 7)

Start the NFS server by the following command:  
systemctl start nfs-server

Create three directories **with root account**,

* /data
* /data/shareA
* /data/shareB

Write the below content to /etc/exports. Replace 143.89.130.89 with your IP address.

* /data/shareA is shared with rw permission
* /data/shareB is shared with rw permission and no\_root\_squash

/data/shareA 143.89.130.89(rw)

/data/shareB 143.89.130.89(rw,no\_root\_squash)

Export the directories with the exportfs command:  
exportfs -arv   
**Write down the output.**

Display the available exported directories with the showmount command:  
showmount -e 143.89.130.89   
Replace 143.89.130.89 with your IP address. **Write down the output.**

## Task 5.2 (Lesson 7)

Create two directories,

* /mnt/shareA
* /mnt/shareB

Mount the NFS shares **with root account** using the following commands:  
mount -t nfs 143.89.130.89:/data/shareA /mnt/shareA  
mount -t nfs 143.89.130.89:/data/shareB /mnt/shareB

Verify that you **cannot** create a file in /mnt/shareA by the following command:  
touch /mnt/shareA/testfile

Verify that you **can** create a file in /mnt/shareB by the following command:  
touch /mnt/shareB/testfile

What is the reason? How can you solve this **without modifying /etc/exports**?

# Section 6: Miscellaneous Topics (Lesson 9)

Use the find command to display a list of all files owned by root with set-uid permission bit set. (**Use Linux man page, i.e. man find, command to check its syntax**)

Use the find command to display a list of all world-writable files.

Use the find command to display a list of all files owned by users that have the same uid as the root user. (Note: uid is different from set-uid)

What file permission does the system assign to you when creating non-executable files and directory?

How could the systems make use of the UMASK variable in file permission? (Hint: Try the umask command)

# Section 7: Administrate a Remote Machine (Lesson 10)

On the server-side (i.e., the remote Linux virtual machine)

Record down the current ipv4 address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The official CentOS 8 support is recently expired. The dnf software repositories are temporarily moved to a new destination. Run the following commands before running the dnf command:

|  |
| --- |
| sed -i -e "s|mirrorlist=|#mirrorlist=|g" /etc/yum.repos.d/CentOS-\*  sed -i -e "s|#baseurl=http://mirror.centos.org|baseurl=http://vault.centos.org|g" /etc/yum.repos.d/CentOS-\* |

Run the following commands to setup the GNU screen software:

* The first command is to install an addition software repository EPEL (Extra Packages for Enterprise Linux) for the dnf package manager
* The second command is to install a software called GNU Screen

|  |
| --- |
| dnf install epel-release -y  dnf install screen -y |

On the client-side (i.e., your current laptop/desktop computer)

Write down the command to remote login to the Linux virtual machine:

* If you are using Mac, you can open the Terminal App
* If you are using Windows, you can use the software “putty”
* If you prefer to use a GUI tool in Windows, capture a screenshot to demonstrate that you can remote login to the Linux VM.

|  |
| --- |
|  |

You can type in the command screen --version to verify the installation

Write down the output in the following box:

|  |
| --- |
|  |

Type in the following command to start a new screen session:

* Note: You need to type in a capital letter S

screen -S ustm17\_session

After the previous command, type in the following command to check the current screen sessions

screen -ls

Write down the output in the following box:

|  |
| --- |
|  |

Open a simple text editor (e.g., nano), type in the following few lines. For example:

Graphical user interface, text

Description automatically generated

**DON’T** save the file. Close the Terminal App (in Mac) or putty (in Windows) to disconnect with the remote machine.

**Re-connect** to the remote machine again.

Type in the following command to check the current screen sessions

screen -ls

Write down the output in the following box:

|  |
| --- |
|  |

Type in the command to restore the detached screen session (Hint: screen -r [name of the detached screen session]). What is your observation?

|  |
| --- |
|  |