

CMAC 3990 – Systems Administration and Operations

Fall 2025 – Section 200

Assignment 2 – 35 points

You have been tasked to deploy a new virtual machine. Log in to your new VM and make a few changes, to allow for easier and more secure management and administration of the new server within the current server environment. All connections must be from within the CS network or through a proxy/VPN.

Replace the two octothorpes with your 2-digit class number (##)

IP Address: 147.64.243.1## (01-25)

Hostname: cmac3990-1##.cs.edinboro.edu (01-25)

OOB Connection (VNC): localhost:559## (01-25)

Default root password: Edinboro-325!

Open an OOB connection to your server, log in as root, and configure your network (5 points):

- nmcli con down enp1s0
- nmcli con mod enp1s0 ipv4.method manual ipv4.addresses 147.64.243.1##/23
- nmcli con mod enp1s0 ipv4.gateway 147.64.242.1
- nmcli con mod enp1s0 ipv4.dns "8.8.8.8,8.8.4.4"
- nmcli con up enp1s0

Change root password (2 points):

- passwd root

Disable all other network interfaces (3 points):

- nmcli con mod enp8s0 connection.autoconnect no
- nmcli con down enp8s0
- nmcli con mod enp9s0 connection.autoconnect no
- nmcli con down enp9s0
- nmcli con mod enp10s0 connection.autoconnect no
- nmcli con down enp10s0

Set your servers hostname (2 points):

- hostnamectl set-hostname cmac3990-1##.cs.edinboro.edu

Create a new account named “user” and set a password (2 points):

- useradd user
- passwd user

Create new username and password for yourself (change to your own unique username!) (2 points):

- useradd yourself
- passwd yourself

Give yourself sudo (1 point):

- Create a new file with the following line at `/etc/sudoers.d/users` file (replace with your username!):
`yourself ALL=(ALL) ALL`

Update your system using DNF (1 point):

- `dnf update`

Install some extra packages with DNF (3 points):

- `dnf install bind-utils nano net-tools sendmail s-nail wget`

Start and enable the sendmail service to allow email assignment submissions (1 point):

- `systemctl enable --now sendmail`

Create a private ssh key for the local root user – accept all default settings (2 points):

- `ssh-keygen`

Import professor's public key to root users `/root/.ssh/authorized_keys` file (ssh key is all one line!) (2 points):

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGC4OIbDfbmWdA9j83ajTlvErVNqM1z6lp4b3hfJf1izgwHMDWqlg/IK/xl2kVyzR6Dj
AHTP4IhcDLjjXwJhfQHhvBGQgc+9862bjyv1zh+7uyT8umS5E/SHhoz4UprhOHO3RCde/V4p1JdTTC/PIVE4Xmv3y/dgEbTm
HBgNl/hysEMv1AgQJO2f03g5Jj6veBvwGVuUcdnj/H9eQV+mtnhlr07OLEgXOFxGGGPaxJk8xabYOQmONwvFXLoleuljgw0O
pjLYlwFZ5B8YMEw8jo673G45u5ZJh2kgL6zoMpqMWZ9SpekHZLdbNbFKsrlTsZX08krwV+P1paPqB7gQ0CyjVgGTh9i1Ke1v
0uQS8gijZIo/1EY2sSgg7rxRMrNUccrc59AfBnq35Q5EWpUHDLMkzoQkq0j/FeWduD2uZXiScKEwOM5NmoUwBLPXBa18r1ph
PUdB1YWBKDhD+wdDWf9SSnUphHHXyUSFrKGpBq0TIpvQjjzkSThpjz6SacyJ7IM= root@cmac3990-
110.cs.edinboro.edu
```

Permissions must be correct on the `authorized_keys` file! (600; -rw-----)

- `chmod 600 /root/.ssh/authorized_keys`

You can use the `wget` or `curl` command to download the key file directly from:

<https://jpatalon.cs.edinboro.edu/cmact3990/classfiles/root@cmact3990-110.pubkey>

Disable ssh password logins for user root (allow only key based root ssh login) (2 points):

- This will allow password-less key based logins for root and disable password logins for root:
`/etc/ssh/sshd_config` file:
`PermitRootLogin prohibit-password`

Validate your network is working as expected:

- Ping commands:
`o ping -qc 1 google.com`
- Good ping results:

```
[root@csci425-101 assignment2check]# ping -qc1 google.com
PING google.com (172.217.3.14) 56(84) bytes of data.

--- google.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 12.614/12.614/12.614/0.000 ms
```

Update system (1 point):

- RHEL 9 based systems use DNF:
 - o `dnf update`

Reboot your system (1 point):

- Before logging out or rebooting, make sure you can login as your user account and su to become root!
 - o `reboot`

Ensure you can still ping resources after reboot:

- `ping -qc1 google.com`

Create a tunnel to work with OOB connections remotely (if necessary):

- Create an SSH connection to `jpatalon.cs.edinboro.edu` and open a dynamic socks proxy on port `555##`, with a local port forward on port `559##` to `csvm1.cs.edinboro.edu` port `559##`
- You can create a shortcut, or save settings with ssh
 - o `ssh -p 54321 -L 559##:147.64.242.113:559## -D 555## cs_student@jpatalon.cs.edinboro.edu`
 - Replace the `##` with your 2 digit number!
 - o Forward Firefox through Options - Advanced – Network – Connection Settings
 - Manual proxy config, SOCKS v5 Host 127.0.0.1, Port 555##, Remote DNS enabled
 - Open a VNC connection to `localhost:559##` to access your OOB console connection

Create a document explaining what you did in this exercise and upload it in D2L to the Dropbox folder HW2. (5 points)

Download and run the check script using the following five commands:

```
cd /tmp
rm -rf /tmp/assignment2check.sh
wget https://jpatalon.cs.edinboro.edu/cmac3990/classfiles/assignment2check.sh
chmod a+x /tmp/assignment2check.sh
/tmp/assignment2check.sh
```