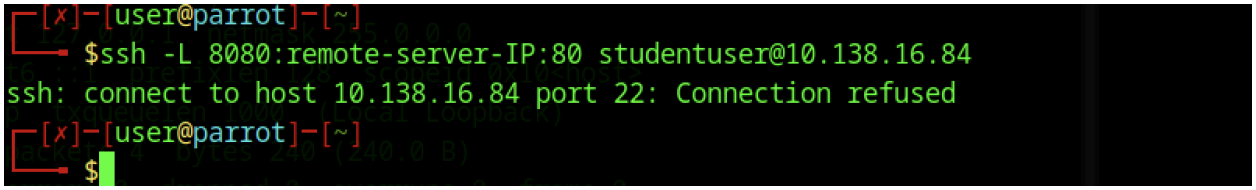
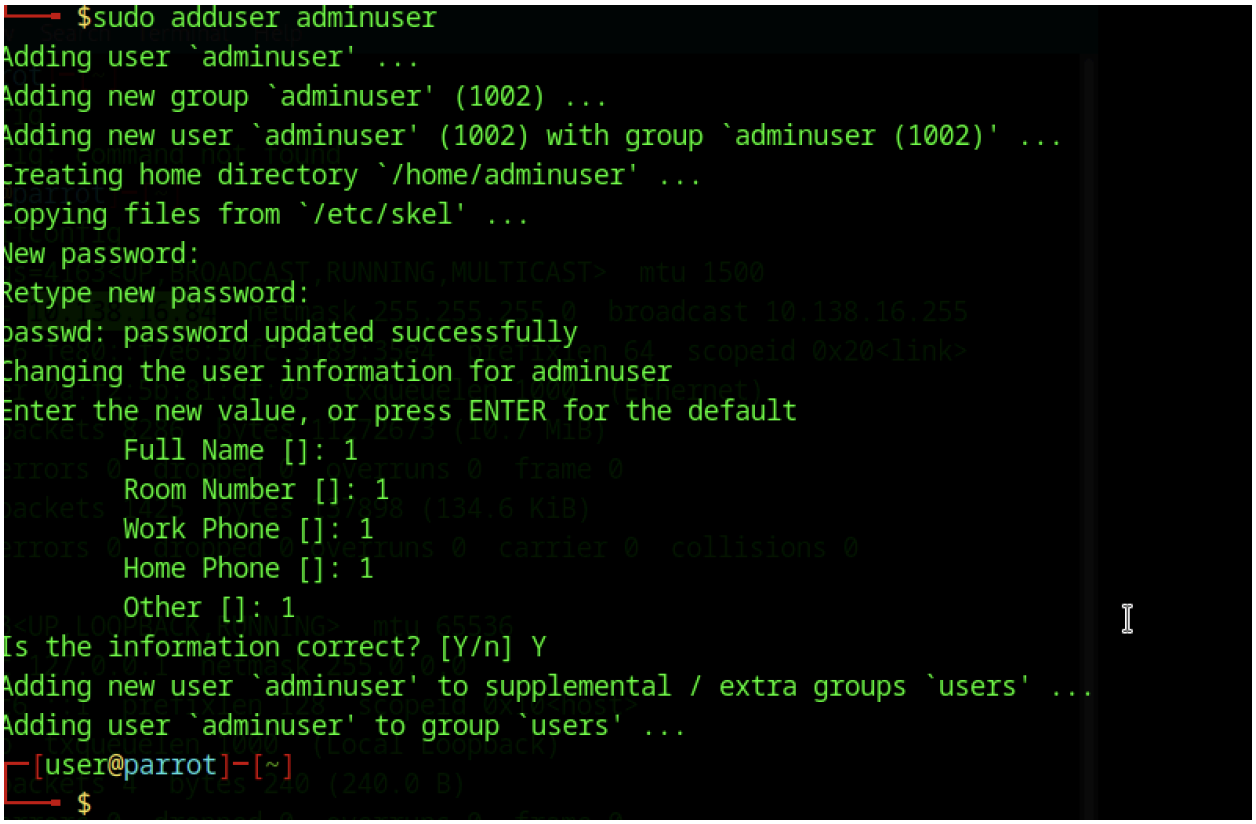
```
┌─[user@parrot]─[~]
└──╼ $sudo ufw enable
Firewall is active and enabled on system startup
┌─[user@parrot]─[~]
└──╼ $sudo ufw allow ssh
Rule added
Rule added (v6)
┌─[user@parrot]─[~]
└──╼ $sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)

┌─[user@parrot]─[~]
└──╼ $
```

```
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for studentuser
Enter the new value, or press ENTER for the default
        Full Name []: 1
        Room Number []: 1
        Work Phone []: 1
        Home Phone []: 1
        Other []: 1
Is the information correct? [Y/n] Y
Adding new user `studentuser' to supplemental / extra groups `users' ...
Adding user `studentuser' to group `users' ...
┌─[user@parrot]─[~]
└──╼ $ssh studentuser@10.138.16.84
ssh: connect to host 10.138.16.84 port 22: Connection refused
┌─[✗]─[user@parrot]─[~]
└──╼ $
```





Network Access & Authentication

Overview
This document outlines the implementation captured in the provided screenshots showing Network Access Control, identity-based access, and user creation for role-based access control.

A. Implement Network Access Control

Step 1: Enable UFW (Uncomplicated Firewall)
Screenshot (4:50:01 PM) shows:

1. UFW enabled: `sudo ufw enable`

2. SSH access rule added: `sudo ufw allow ssh`
3. Status verification: `sudo ufw status` showing:
    - Port 22/tcp open for IPv4 and IPv6
    - Firewall active

Significance: Confirms proper firewall configuration to allow SSH while blocking other traffic.

B. Identity-Based Access

Step 2: Create New Users

Screenshot (4:59:13 PM) - adminuser creation:

1. User added: `sudo adduser adminuser`
2. Successful password set after verification
3. Added to supplemental 'users' group

Screenshot (4:57:30 PM) - studentuser creation:

1. Initial password mismatch error ("Sorry, passwords do not match")
2. Successful retry with matching passwords

Step 3: SSH Login Attempt

Screenshot (4:57:30 PM) shows:

1. Connection attempt: `ssh studentuser@10.138.16.84`
2. Result: "Connection refused" (SSH service not running/accessible)

Missing: Screenshot of successful SSH login after service configuration.

C. Site-to-Site VPN/SSH Tunnel

Not visible in provided screenshots

Screenshot (4:58:43 PM) shows failed tunnel attempt:

1. Command: `ssh -L 8080:remote-server-IP:80 studentuser@10.138.16.84`
2. Same "Connection refused" error as basic SSH

Documentation Needed: Working VPN/tunnel screenshot showing secure connection between networks.

D. Role-Based Access Control (RBAC)

Step 1: User Creation

Screenshots show:

1. Two users created:
    - `studentuser` (4:57:30 PM)
    - `adminuser` (4:59:13 PM)
2. Both added to 'users' group