■■ Project 2: Cloud Server Hardening & Secure Access (Quick Setup Guide)

Student: Vishal Sundi

Platform: Microsoft Azure (Free Student Credits)

■ Quick Setup Commands

Create admin user:

```
sudo adduser adminuser && sudo usermod -aG sudo adminuser
```

Grant sudo privileges:

```
echo 'adminuser ALL=(ALL) NOPASSWD:ALL' | sudo tee
/etc/sudoers.d/adminuser
```

Disable root SSH login:

```
sudo sed -i 's/^#*PermitRootLogin.*/PermitRootLogin no/'
/etc/ssh/sshd_config && sudo systemctl restart ssh
```

Generate SSH key:

```
ssh-keygen -t rsa -b 4096
```

Copy SSH key to server:

```
ssh-copy-id adminuser@
```

Configure UFW:

```
sudo apt install ufw -y && sudo ufw allow OpenSSH && sudo ufw enable &&
sudo ufw status verbose
```

Install Fail2Ban:

```
sudo apt install fail2ban -y && sudo systemctl enable fail2ban && sudo
systemctl start fail2ban
```

Check Fail2Ban logs:

```
sudo fail2ban-client status sshd && sudo cat /var/log/fail2ban.log | grep
Ban
```

Enable Auditd:

```
sudo apt install auditd -y && sudo systemctl enable auditd && sudo
ausearch -m USER_LOGIN,USER_CMD
```

(Bonus) Install Wazuh Agent:

```
curl -sO https://packages.wazuh.com/4.x/apt/wazuh-agent-4.x.deb && sudo
WAZUH_MANAGER='' dpkg -i wazuh-agent-4.x.deb && sudo systemctl start
wazuh-agent
```