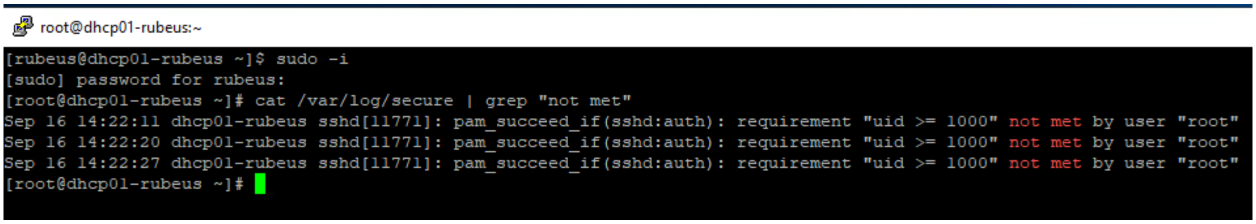
# Securing SSH

💣Allowing remote access to a known user account like Administrator or Root is a terrible idea! It allows an attacker to conduct an exhaustive attack using dictionaries of passwords against these known user accounts.

A security best practice is to disable Remote access as root.

Using your friends at ~~Google~~ DuckDuckGo, figure out how to disable SSH root user access to dhcp01 (Hint: this should involve a small edit to a single file). Prove you have done this correctly by conducting a test via PuTTY or Powershell SSH on a Windows OS to remote onto dhcp01 using SSH via root.

Deliverable 1. Once you are convinced that root can no longer login, provide a screenshot that shows how this failure was captured in the logs:



```
[rubeus@dhcp01-rubeus ~]$ sudo -i
[sudo] password for rubeus:
[root@dhcp01-rubeus ~]# cat /var/log/secure | grep "not met"
Sep 16 14:22:11 dhcp01-rubeus sshd[11771]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
Sep 16 14:22:20 dhcp01-rubeus sshd[11771]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
Sep 16 14:22:27 dhcp01-rubeus sshd[11771]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
[root@dhcp01-rubeus ~]# 
```

Deliverable 2. Figure out how to determine what root’s uid (user id) is. What is it and based on the logs, what logic is used to prevent root's login?

Deliverable 3. Provide a link to a tech-journal entry on how you secured SSH from remote root access on Centos.