Secure Linux Server Hardening & Audit

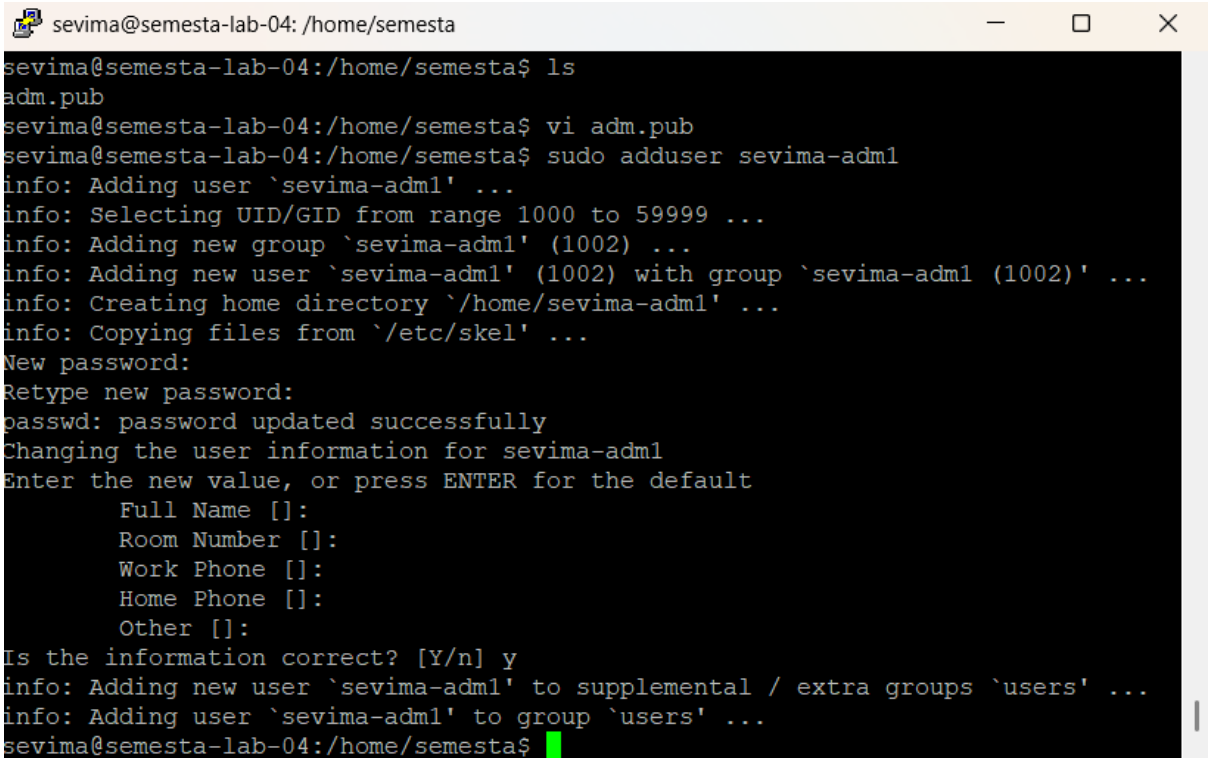
Nama : Rakadian Audiga Pratama

Bidang : DevOps

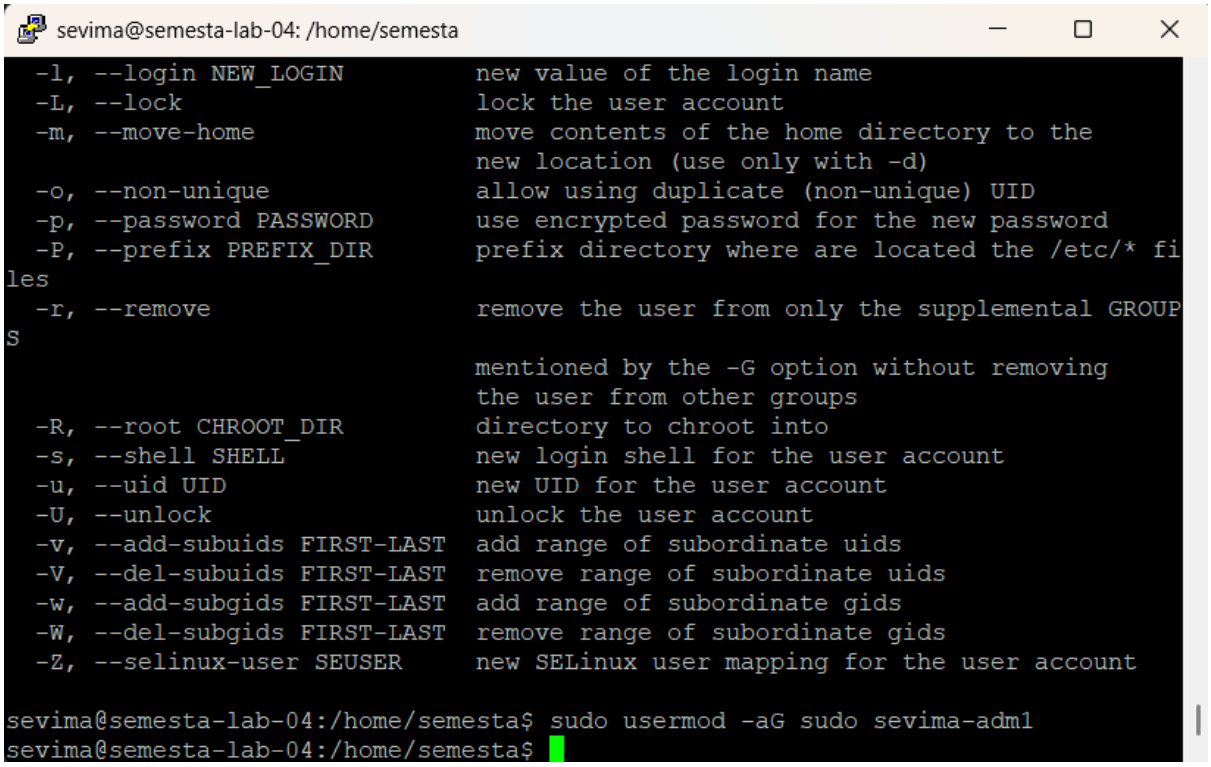
Langkah-langkah

1. Membuat user dengan akses sudo menggnuankan password dan pubkey

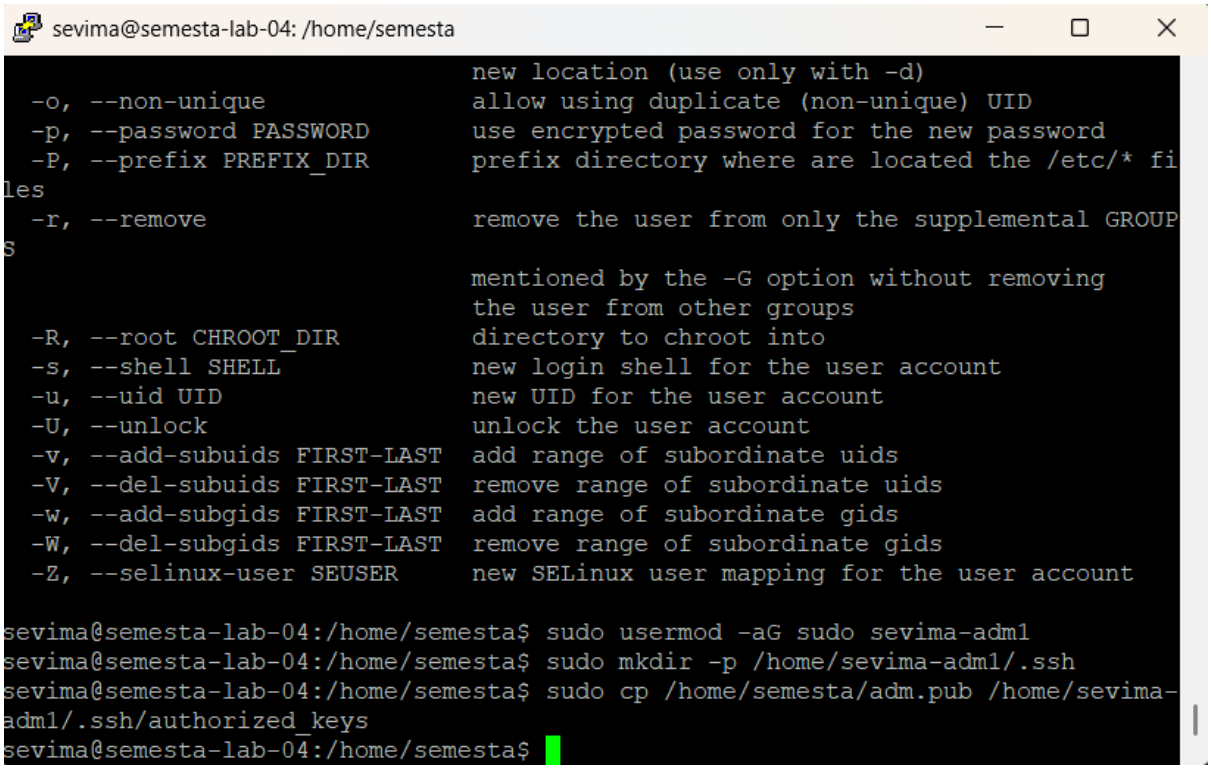
Langkah pertama adalah membuat user baru menggunakan sudo adduser

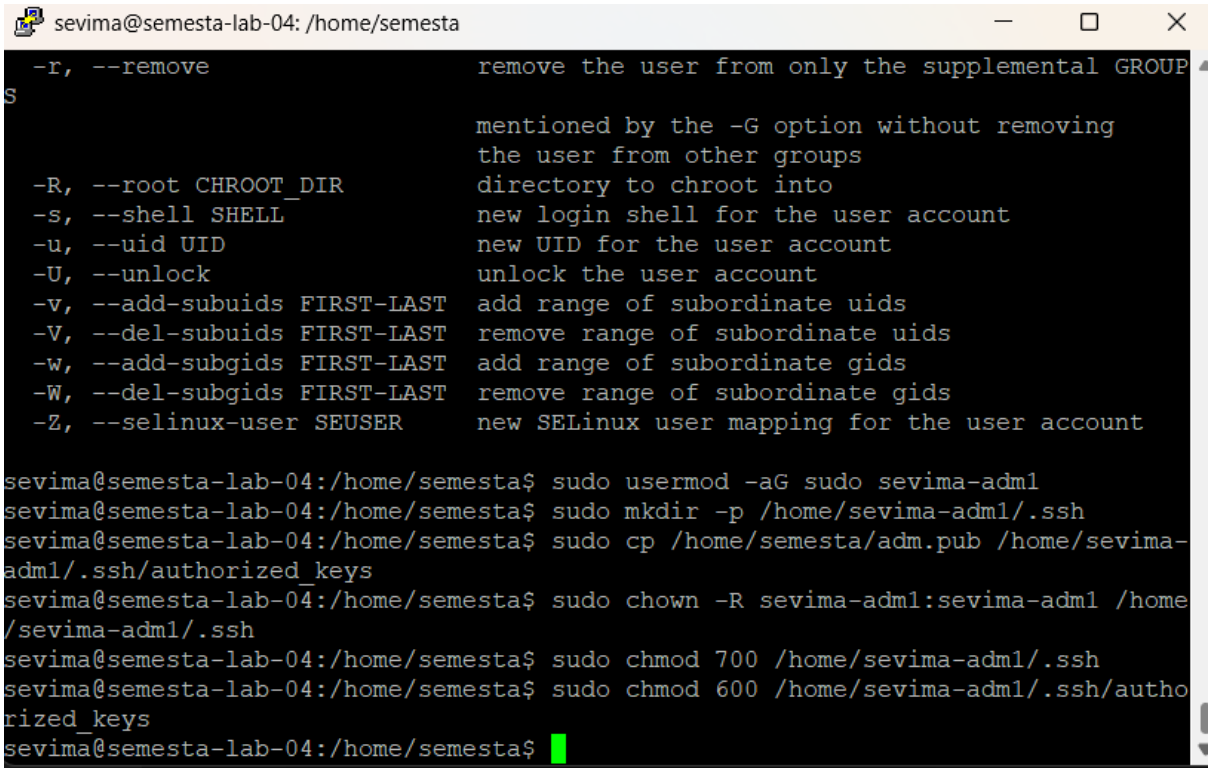


Kemudian menambahkan user tsb ke grup sudo



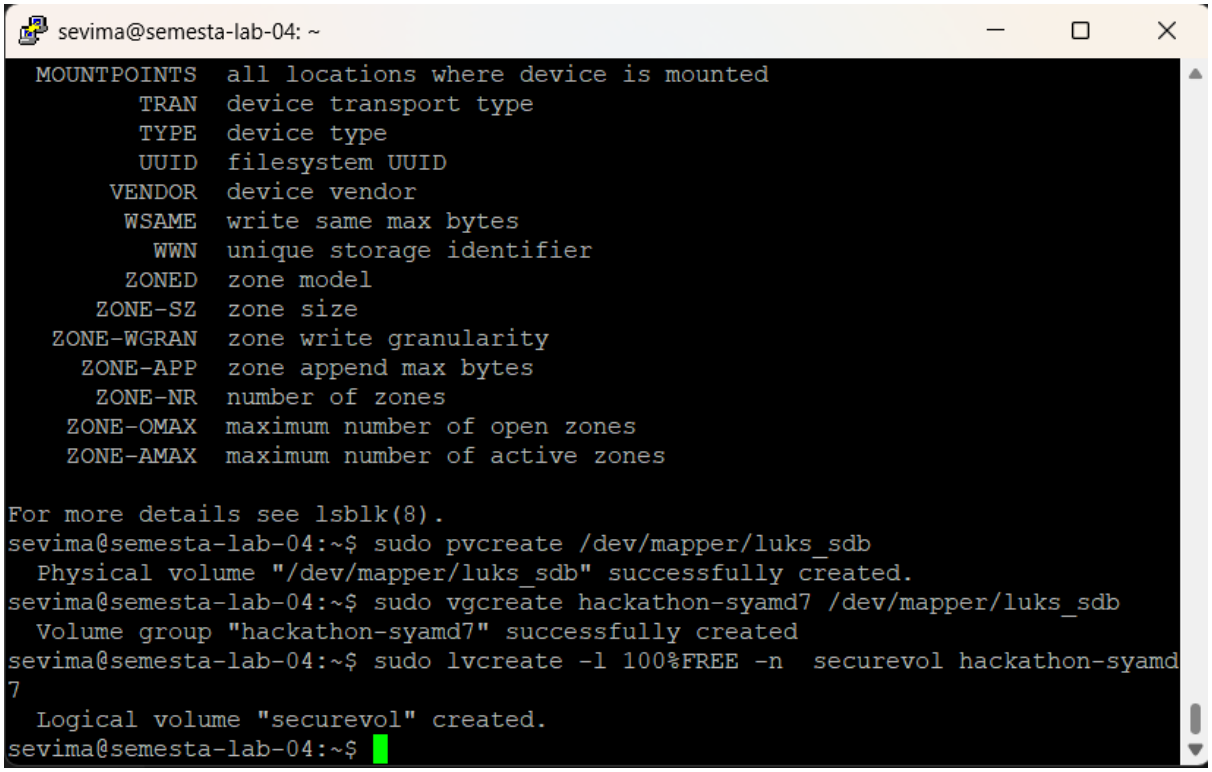
Dilanjutkan membuat direktori ssh untuk user baru dan mengcopy pubkey dan set permission untuk sudo



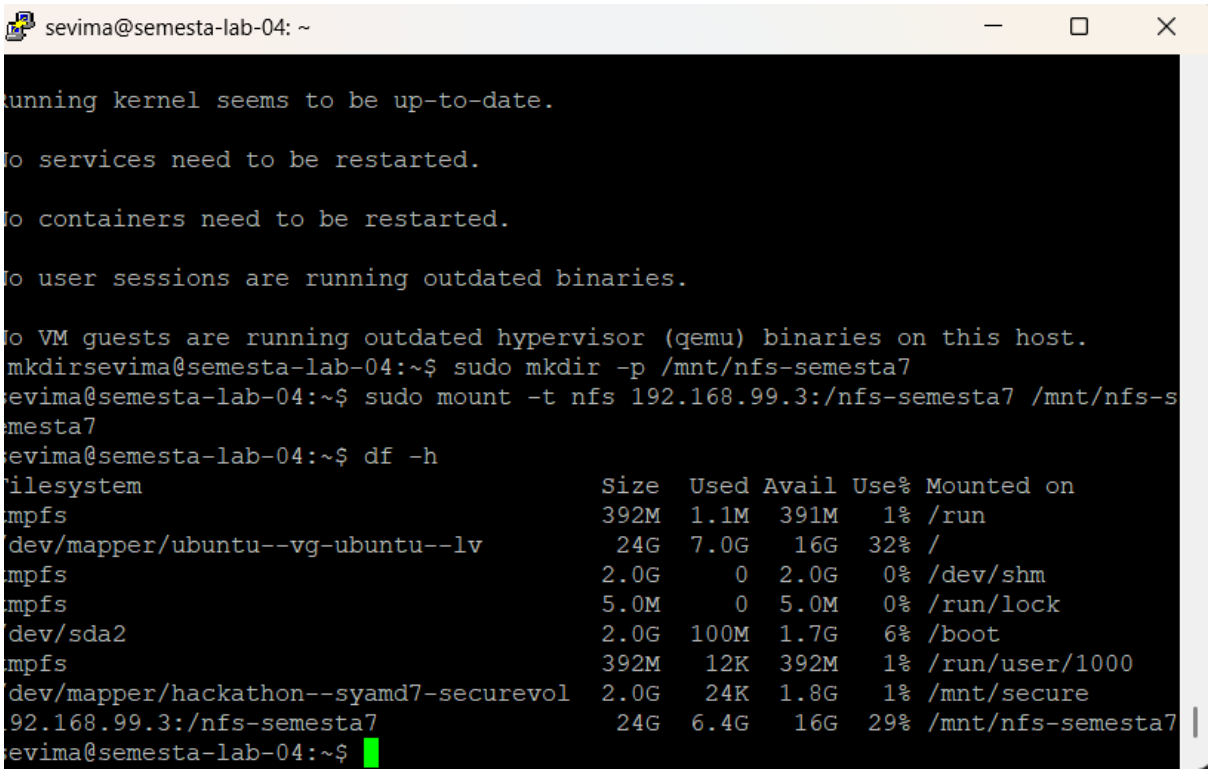


2. Membuat lvm dari sdb dan dienkripsi

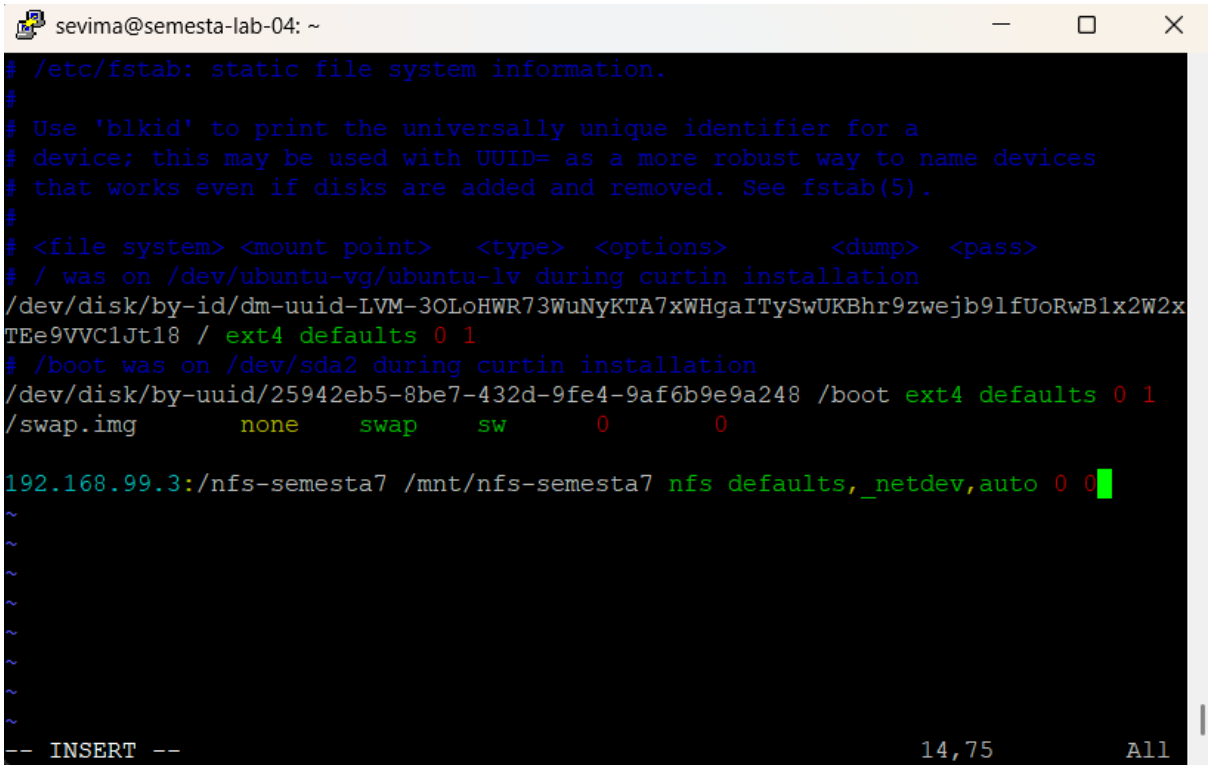
Encrypt menggunakan luksformat dan volume nya diberi nama hackthon-syamd7



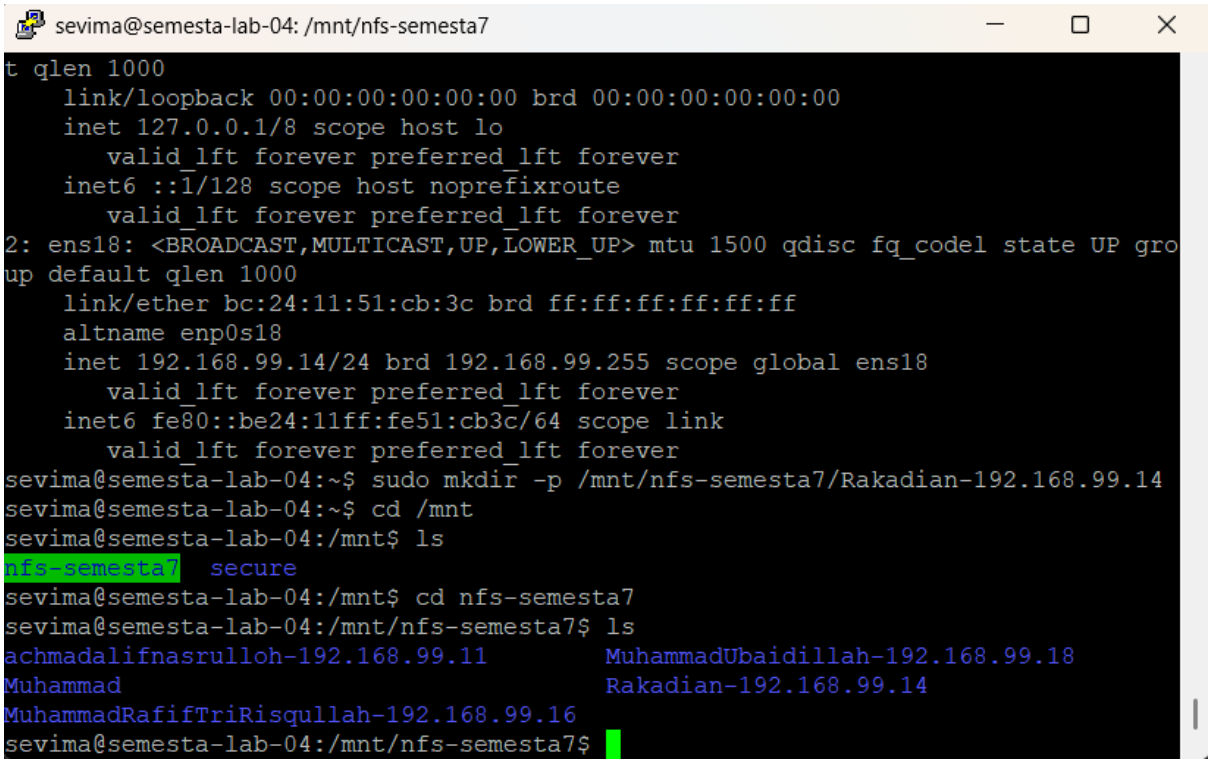
Kemudian membuat mount point/nfs source dengan nama folder nfs-semesta7



Kemudian menambahkan ke /etc/fstab agar auto-mpount saat ter-restart dengan mengedit file /etc/fstab



Kemudian yang terakhir membuat folder pada nfs yang sudah dikonfigurasikan dengan nama peserta-ipserver



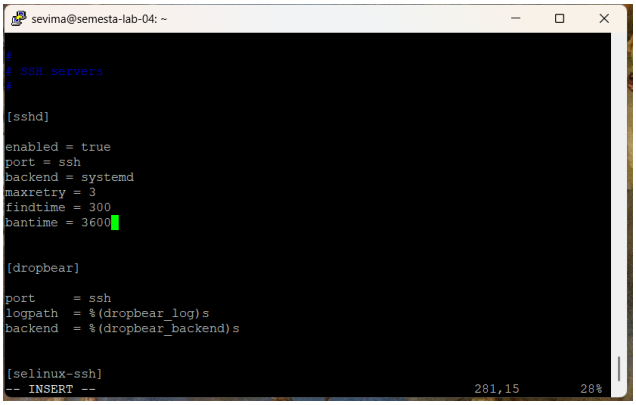
3. awdawdawd

4. Root login masih diizinkan

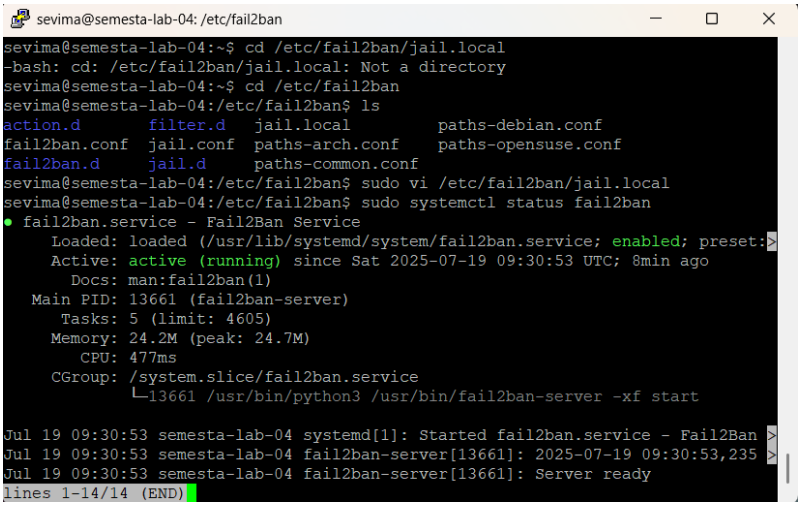
Permasalahan ini terdapat di konfigurasi ssh daemon yang Dimana root user dapat login melalui ssh. Untuk merubahnya, yang harus dilakukan adalah merubah PermitLoginRoot yes menjadi PermitLoginRoot no.

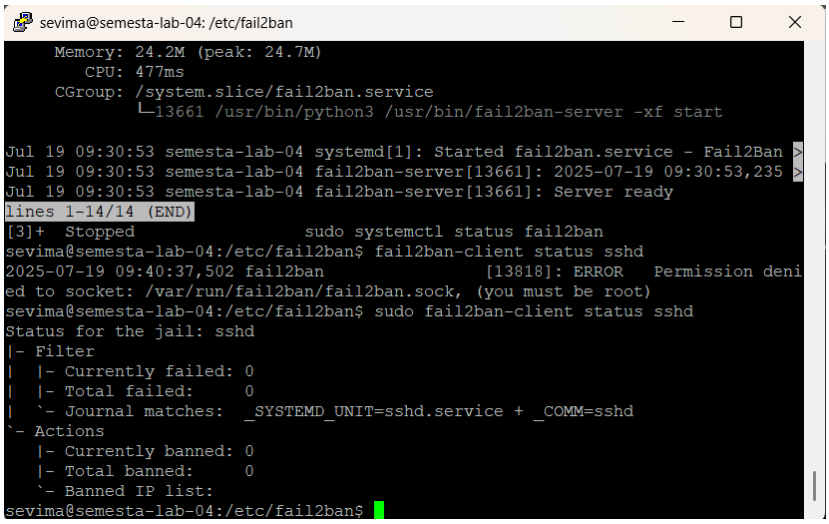
5. Pembatasan terhadap login gagal

Untuk permasalahan ini dapat menggunakan tool tambahan, yakni fail2ban yang akan meng-ban Alamat IP jika ada aktivitas mencurigakan seperti login gagal berulang. Fail2ban akan berjalan secara otomatis setelah mengatur konfigurasi nya. Buat konfigutasi seperti ini:



Lalu cek status fail2ban apakah sudah berjalan.

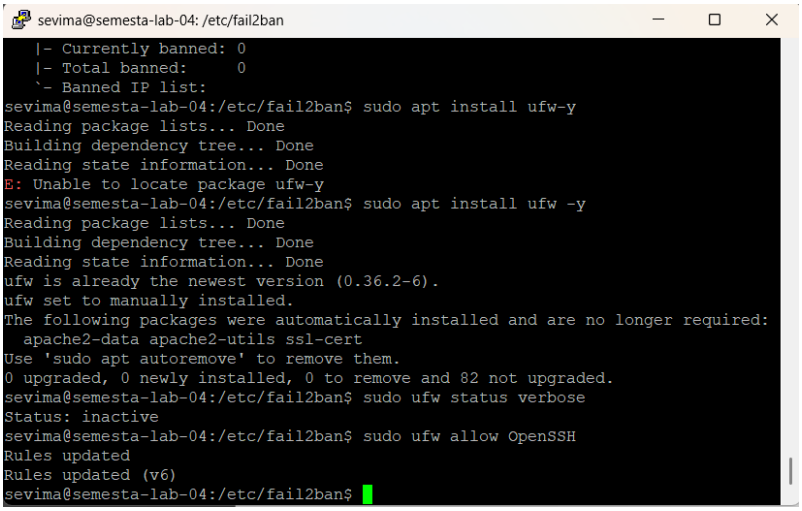




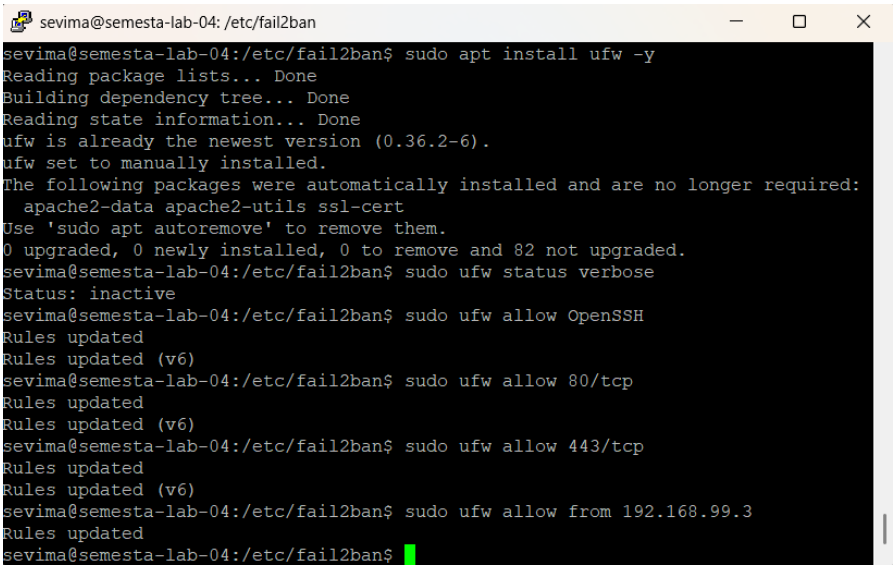
Seperti di gambar, status fail2ban sudah aktif. Jadi jika ada yang mecncoba login dan gagal 3 kali, akan ter-ban selama 1 jam.

6. Konfigurasi firewall

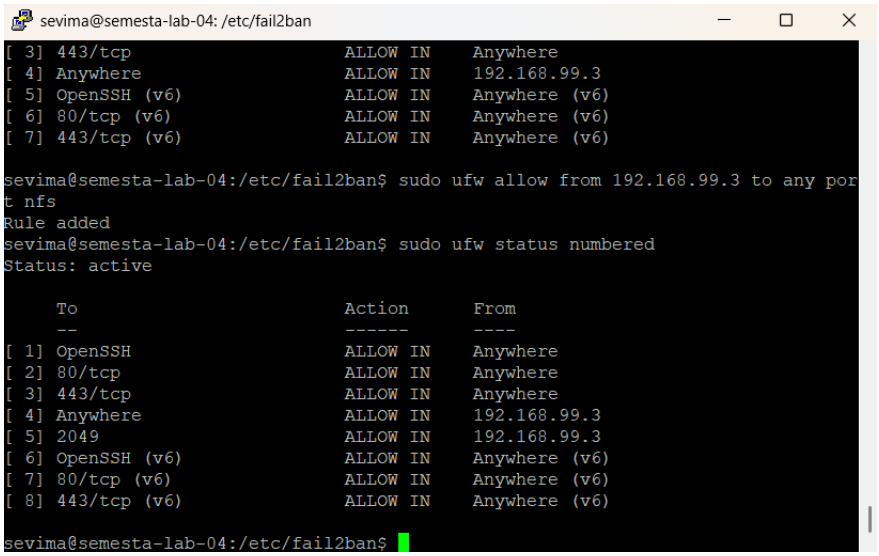
Untuk mengonfigurasi firewall, bisa menggunakan ufw (uncomplicated firewall). Langkah pertama adalah mengizinkan akses melalui ssh.



Kemudian mengizinkan akses http, https, dan nfs yang sudah disediakan.

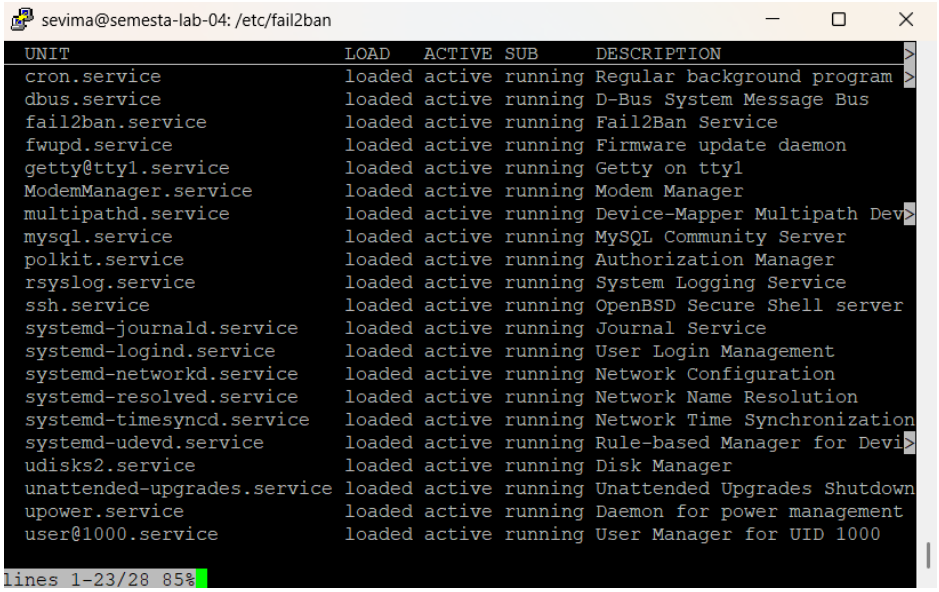


Jika sudah, jalankan firewall dan cek status firewall. Gambar dibawah adalah contoh jika firewall sudah berjalan.

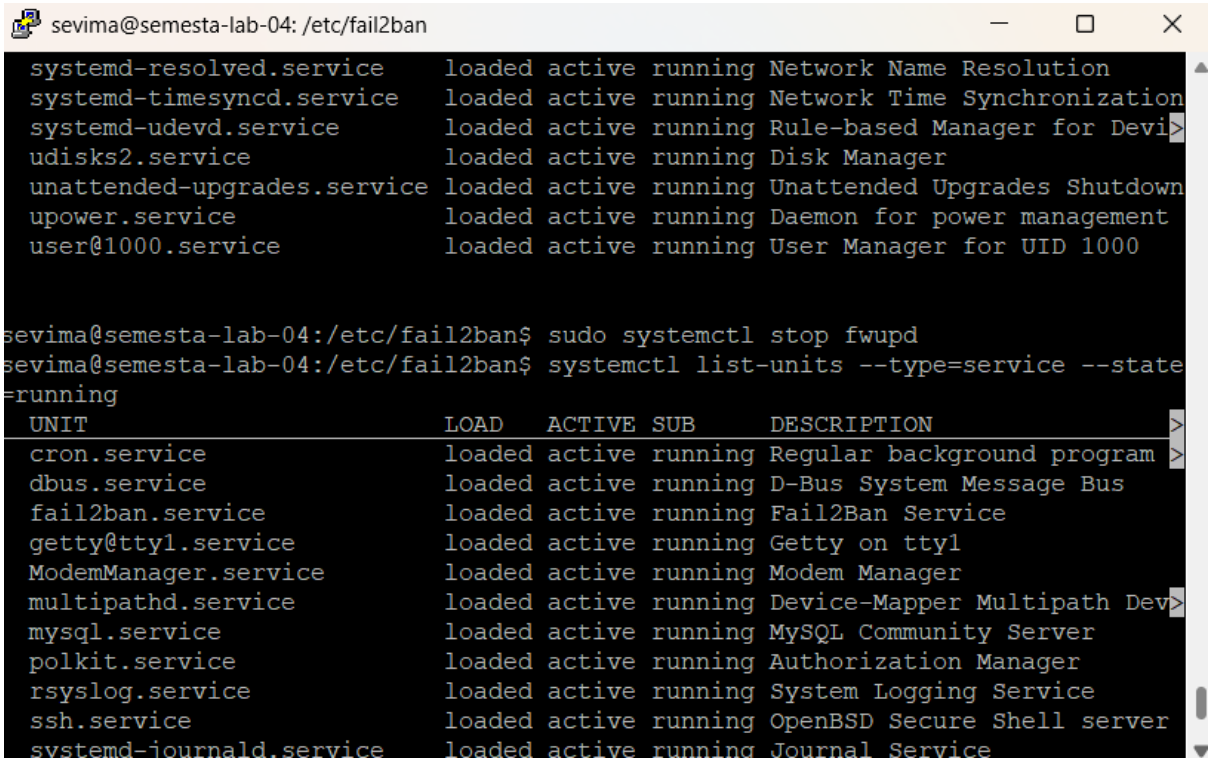


7. Service yang tidak digunakan masih berjalan

Untuk mengecek service yang sedang berjalan, bisa menggunakan command systemctl list-units –type=service –state=running, lalu akan muncul list seperti dibawah:



Jika sudah muncul, pengguna dapat menentukan service trivial mana saja yang ingin di-stop. Fwupd dapat distop karena kita tidak perlu untuk mengupdate firmware otomatis, jadi bukan service penting sehingga bisa di-stop.



8. Sistem log tersentralisasi dan aturan audit aktif

9. Konfigurasi NFS
10. Pembatasan penggunaan resource