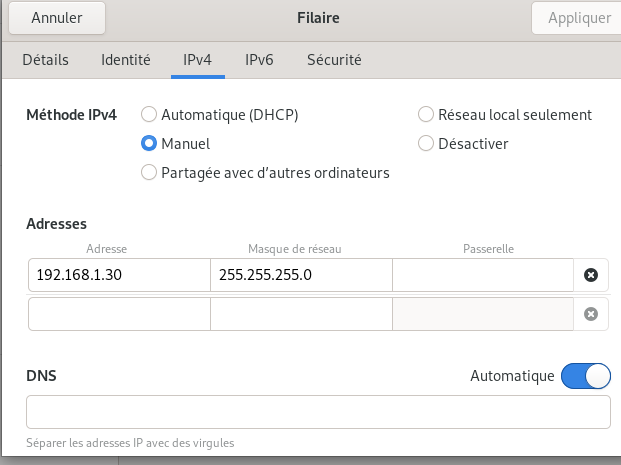
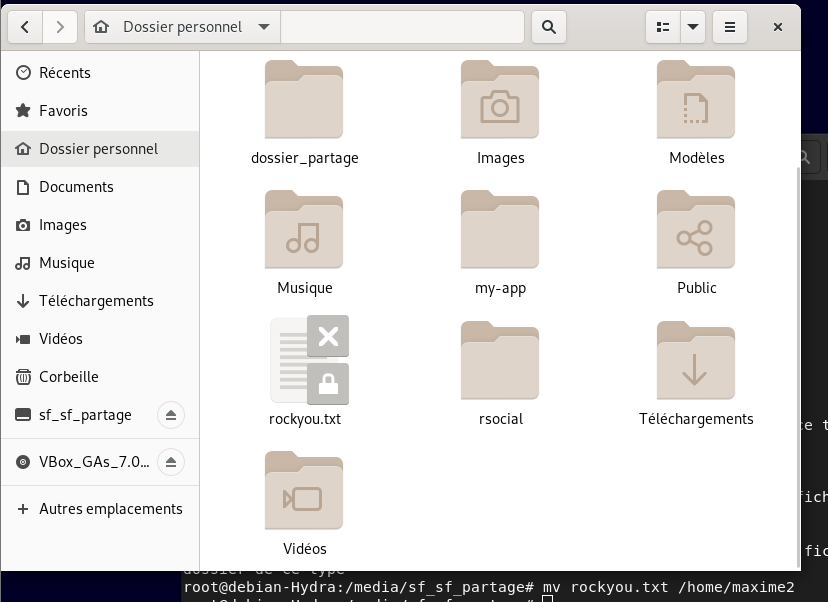
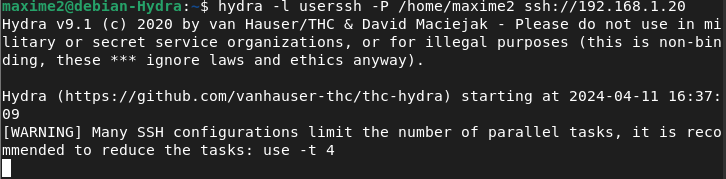
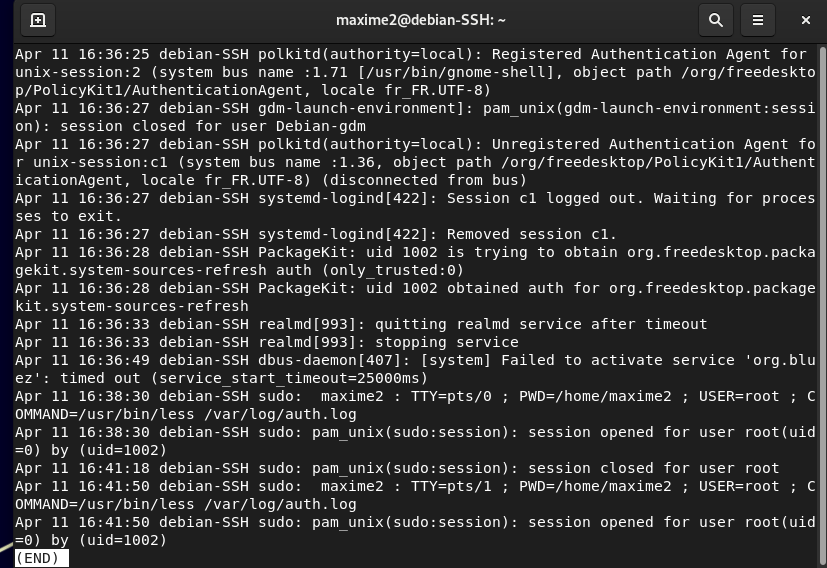
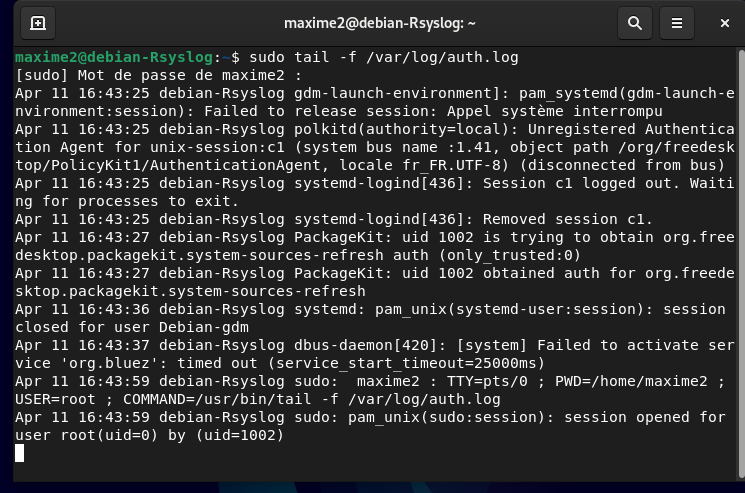
3- Machine Hydra



Je n’ai pas réussi à régler le problème rencontré en cours, j’ai vérifié que toutes les machines avaient bien le port 22 ouvert mais la debian attaquante s’arrête toujours pendant l’attaque et je ne vois pas l’attaque dans les logs centralisés. Toutes les machines ont bien l’ip adéquate, les ports ouverts, sont sur le réseau interne, devant travailler le week-end et le bts blanc à réviser, je n’ai pas eu plus de temps pour recommencer tout le tp.

5 – Conclusion

Il est important de centraliser les logs pour mieux détecter les attaques et les analyser. On peut plus facilement voir les informations sur les attaques que si on devait parcourir tous les logs pour voir ceux qui concernent les attaques.

On doit protéger le SSH des attaques brute force en implantant des mots de passe forts, en verrouillant les comptes si il y a trop de tentatives de connexions infructueuses, on peut aussi utiliser une double authentification.