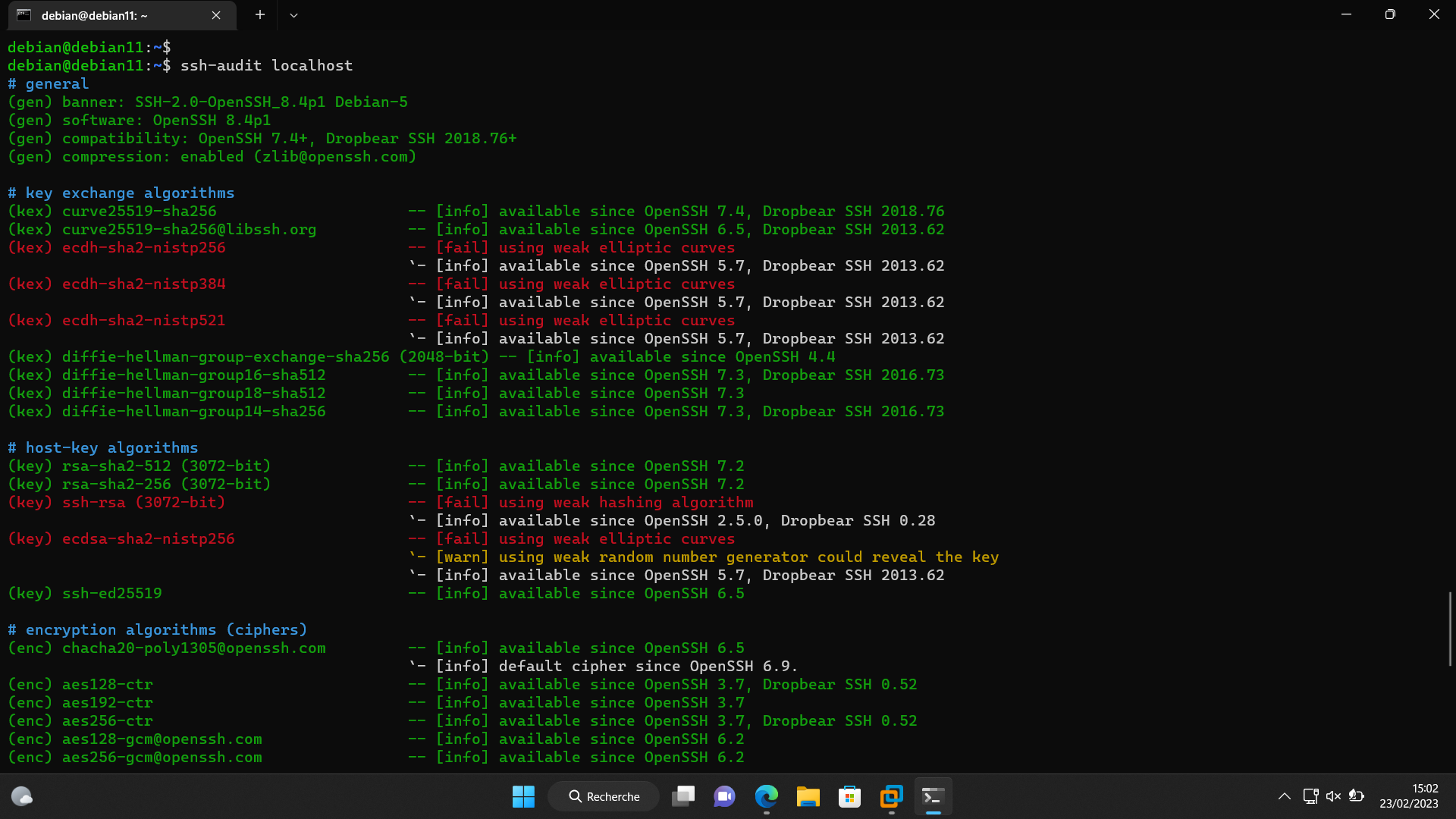
AUDITEZ UN SYSTÈME LINUX

SSH, ou *Secure Shell*, est un protocole utilisé pour se connecter en toute sécurité à des systèmes distants. C’est le moyen le plus courant d’accéder à des serveurs Linux distants. Dans cette partie nous vous présenterons comment un auditer le service SSH , Transférer les logs d’une machine à une autre.

DEMMARRONS L’AUDIT DU SERVICE SSH

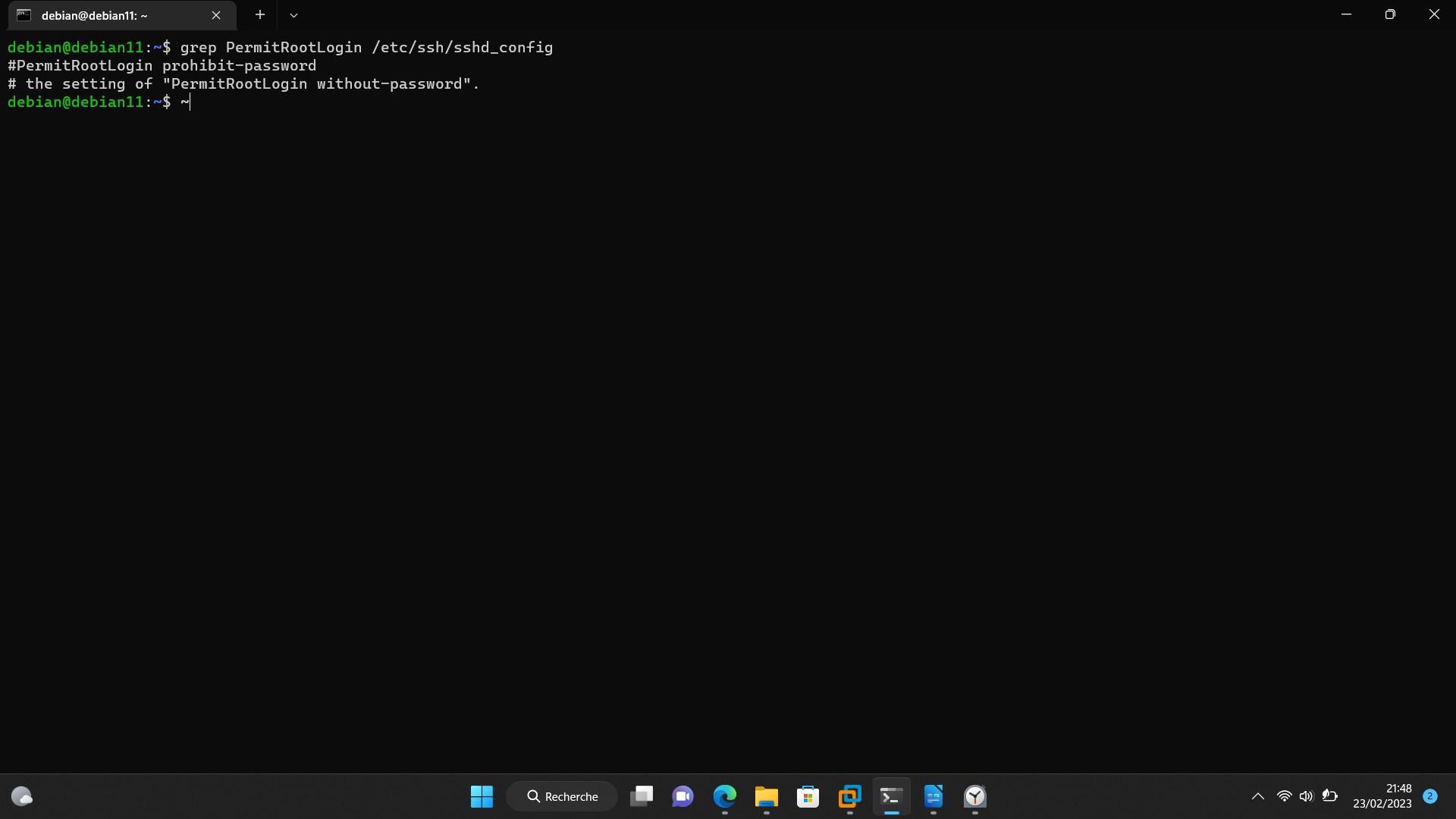
Récupérons les informations concernant le service SSH



Parmi les lignes affichées, nous avons comme informations que la version du protocole SSH est la version 2. La version 2 amène plus de fonctionnalités, et la version 1 du protocole est aujourd'hui obsolète

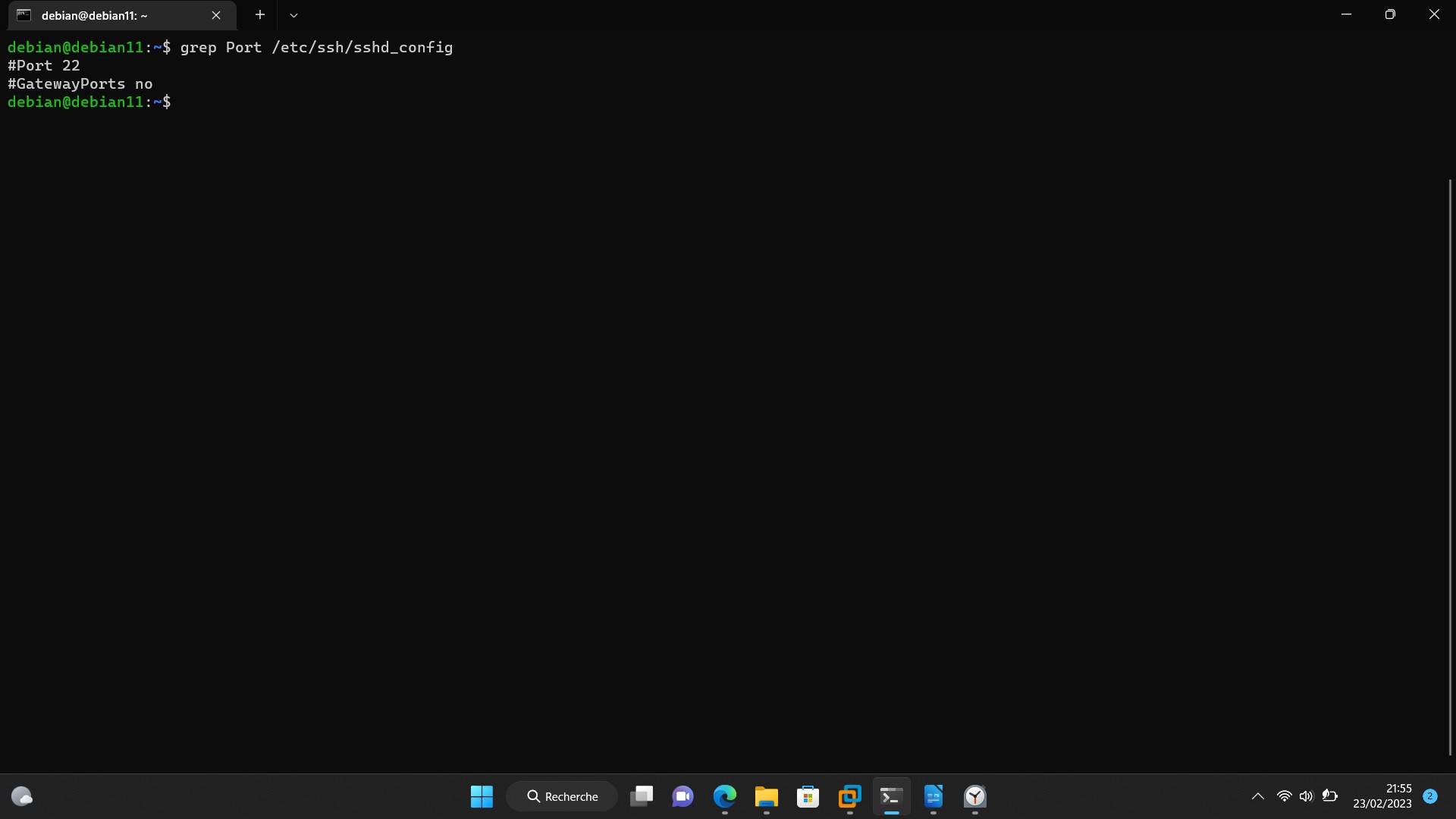
S'il y a une chose qu'il faut absolument bannir en ce qui concerne le service SSH, c'est la possibilité de se connecter directement avec le compte root. Ce réglage est indiqué dans le fichier de configuration avec la

directive PermitRootLogin :



Examinez la directive PermitRootLogin du service SSH celle ci doit avoir comme valeur indiquer PermitRootLogin no

Nous allons encore rechercher dans notre fichier /etc/ssh/sshd\_config avec la commande :



Nous constatons que le port d’écoute est le 22 ceci est le port par défaut du protocole SSH une mesure importante serait de modifier le port d’écoute par un autre numéro de port.

CONSULTEZ LES FICHIERS LOGS DES CONNEXIONS AUX SERVICES SSH

