L’ objectif de ce TP est de sécurisé un server apache qui se trouve sur une vm rocky linux.

Pour ce faire j’ ai utilisé des outils comme nmap ou nikto

* Avec nmap lorsqu’ on tape la commande : sudo nmap ADRESSE\_IP\_ROCKY\_LINUX -O -sV -p1-65535 ont peut connaitre le système d exploitation de la machine ainsi que les ports qui sont ouverts.

Pour éviter que des potentiels attaquant connaissant trop de détails sur notre machine nous pouvons mettre en place un firewall. Ici j’ ai installé iptables voici la configuration de base :

Une image contenant texte, capture d’écran, noir, Police

Description générée automatiquement

Maintenant si je relance un scan nmap n est plus sur de mon système d’exploitation mais connais toujours la version de oppenssh.

Pour que nmap ne soit plus sur des ports ouvert je peux lui dire de drop au lieu de reject pour qu’ il n y ai pas de message d’erreur cela donne moins d’ info. Ou alors je peux faire du port knocking ( devoir demander d’accéder à plusieurs port dans un certain ordre afin d’accéder au port que je veux réellement.

Pour résistez au attaques brute force par exemple sur des connections ssh je peux utiliser fai2ban. Un exemple de comment faire un attaque bruteforce : Hydra -l bruteforce -P /usr/share/wordlist/rockyou.

Pour configurer fail2ban :

dnf -y install epel-release

puis on peut installer fail2ban

on tape cette commande : cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local