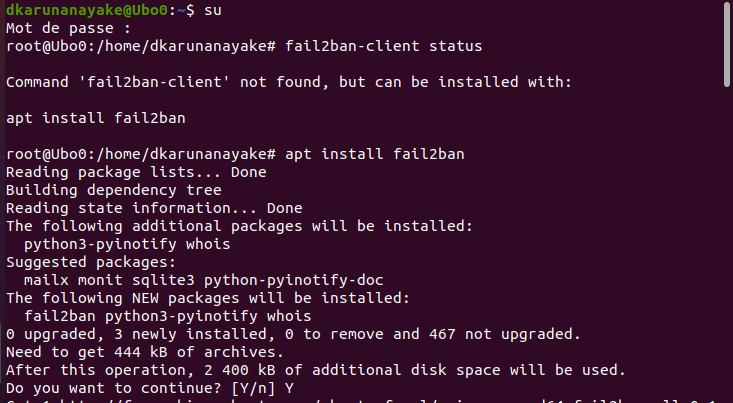
**Simulation attaque/Bannissement adresseIP** Dinura Karunanayake

**1 / Installation de Fail2ban sous Ubuntu**

1. Fail2ban est un log dont l’objectif premier est de détecter des tentatives d’intrusion ou de connexions infructueuses sur un service et de bannir les adresses IP à l’origine de ces tentatives d’intrusion.

Il est donc primordial de l’avoir avec nous pour éviter tout type d’attaques.

Tout d’abord, nous devons bénéficier des droits administrateurs :



1. Après avoir eu accès aux droits administrateurs, lançons l’installation de Fail2ban avec la commande suivante et de le confirmer :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

1. Voilà, Fail2ban est implémenté dans votre terminal. Maintenant, nous allons le mettre en place en commençant par lancer le service :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Puis de créer le démarrage automatique :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Et enfin de contrôler sa bonne installation :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

PS : si vous voyez le « active (running) » en vert, cela veut dire que votre fail2ban à bien été mis en place et prêt à bloquer des adresses.

On peut ainsi observer si les prisons ont bien été lancées correctement avec la commande suivante :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

**2 / Installation de Open SSH sous Ubuntu**

1. On aura besoin d’open ssh installé dans les 2 machines différentes afin de pouvoir simuler l’attaque et le bannissement. Pour cela, il vous suffit de faire la commande suivante :



Vous pourrez aussi vérifier si le serveur ssh a bien été mis en place avec cette commande :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

**3 / Installation de Patator sous Ubuntu**

1. Depuis une autre VM Ubuntu, nous allons attaquer la machine contenant le fail2ban et l’open ssh.

Pour cela, nous allons installer Patator, qui est un service d’attaque par force brut.

Pour l’installer, il faut faire la commande suivante :



**4 / Commencement de l’attaque**

1. Après installation, il faut se placer dans notre bureau et créer un fichier qui contiendra tous les mots de passe que vous voulez faire tester au fail2ban pour vérifier si c’est le bon mot de passe ou non :

La commande « cd » permettant de faire le déplacement et la commande « touch » permettant de créer le fichier.

Une image contenant texte, Police, capture d’écran

Description générée automatiquement

Si vous ne possédez les droits d’écritures, vous pouvez modifier les droits du fichier grâce à la commande « chmod » :



1. Après avoir rempli votre fichier avec le nombre de mots de passe que vous souhaitez tester, nous allons passer au vif du sujet : l’attaque.

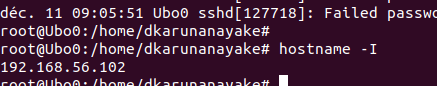
Depuis la VM où nous avons installer patator, effectuer cette commande suivante pour attaquer la VM où on retrouve fail2ban :

Une image contenant texte, capture d’écran, menu

Description générée automatiquement

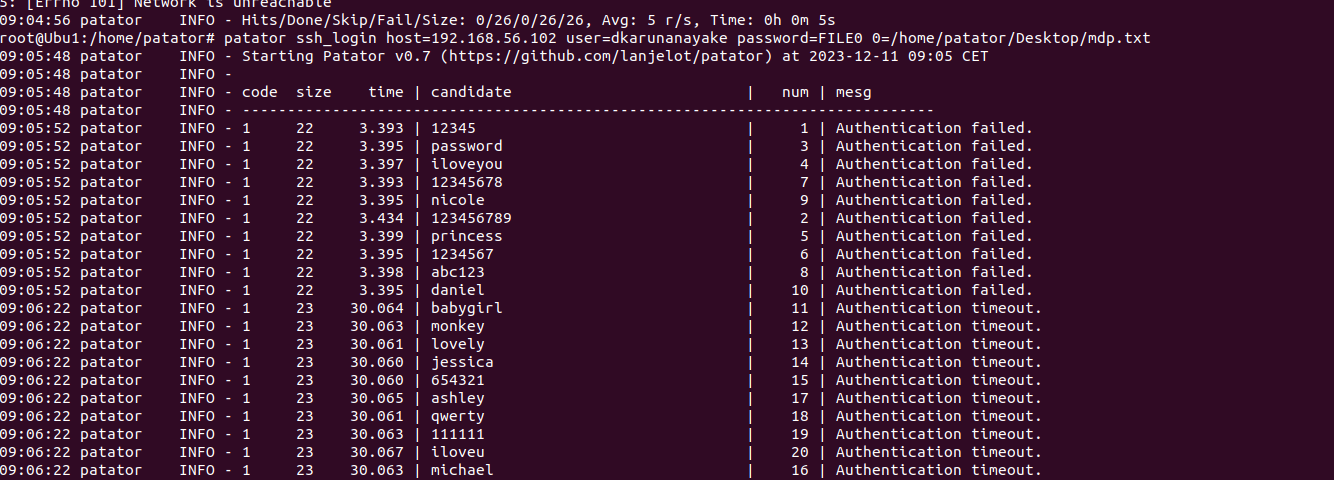
Où le host doit être celui de la machine contenant fail2ban.

Pour connaître l’adresse IP d’une machine, vous pouvez utiliser la commande suivante :



Le user doit être le nom de la machine contenant fail2ban et le password doit contenir le chemin dans lequel se trouve le fichier mdp.txt que vous avez créer.

Après avoir exécuter cette commande, le terminal devrait vous afficher ceci :



Lorsqu’on retrouve le message « Authentification failed », cela signifie que l’adresse IP de l’attaquant à été banni dans la prison du fail2ban.

Cela peut être vérifié depuis la VM où l’on retrouve fail2ban grâce à la commande suivante :

