Attaque par Force Brute

AVEC LES OUTILS CUPP ET MEDUSA SOUS KALI LINUX

Réalisé par Khadim MARONE
(étudiant en Licence 3 en Génie Informatique)

Sous la directive de M. DIOUF
(Ingénieur en informatique)

maronekhadim66@gmail.com

Plan

- Force Brute
- CUPP
- Medusa
- TP

maronekhadim66@gmail.com

Attaque par Force Brute

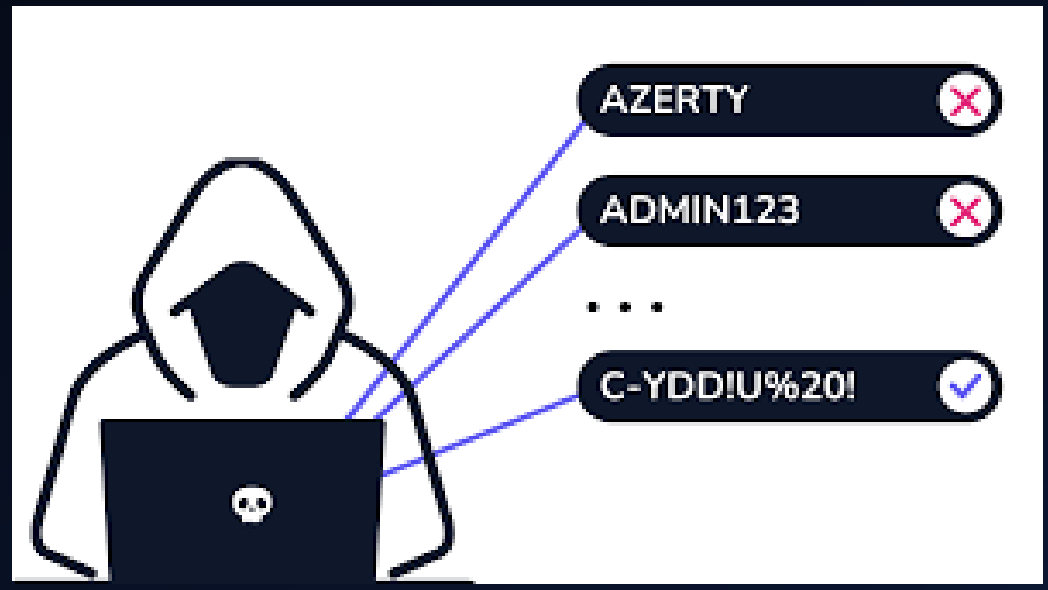
C’EST QUOI ATTAQUE PAR FORCE BRUTE ?

maronekhadim66@gmail.com

DÉFINITION

Une attaque par force brute (*bruteforce attack*) consiste à tester, l'une après l'autre, chaque combinaison possible d'un mot de passe ou d'une clé pour un identifiant donné afin se connecter au service ciblé.

Il s'agit d'une méthode ancienne et répandue chez les pirates. Le temps nécessaire à celle-ci dépend du nombre de possibilités, de la vitesse que met l'attaquant pour tester chaque combinaison et des défenses qui lui sont opposées.



maronekhadim66@gmail.com

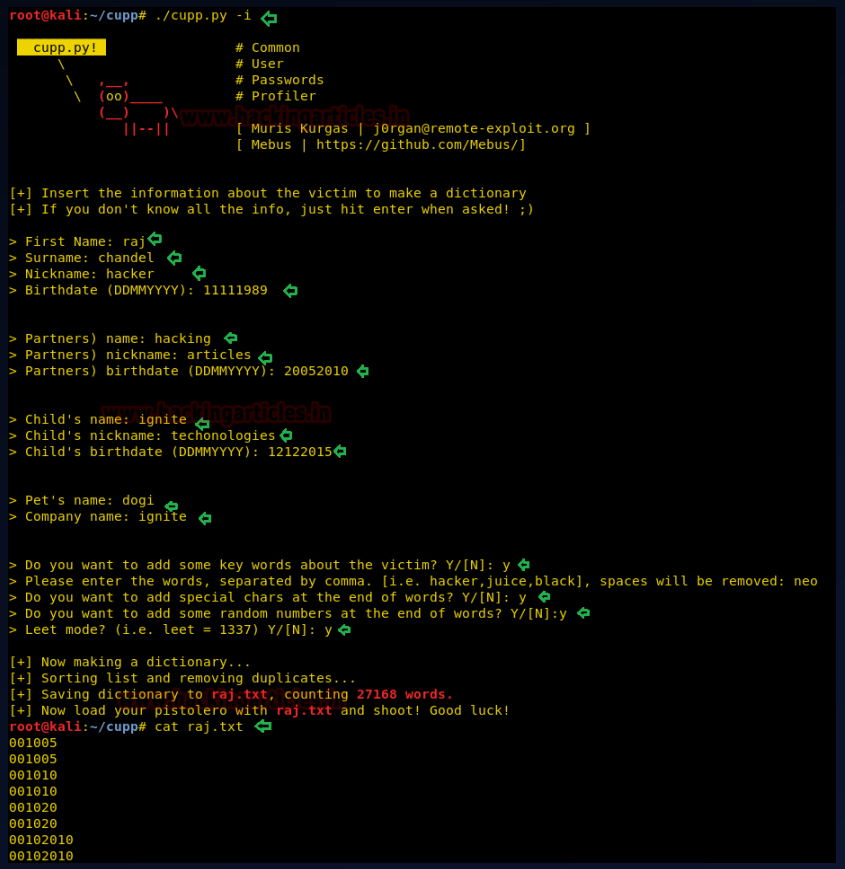
Cupp

C’EST QUOI CUPP ?

maronekhadim66@gmail.com

DÉFINITION

CUPP (Common User Passwords Profiler) est un générateur de liste de mots à partir d'informations telles qu'une date de naissance, un pseudonyme, une adresse, le nom d'un animal de compagnie ou un mot courant comme dieu, aimer, argent ou mot de passe.



maronekhadim66@gmail.com

Medusa

C’EST QUOI MEDUSA ?

maronekhadim66@gmail.com

DÉFINITION

Medusa est destiné à être un outil de force brute de connexion rapide, massivement parallèle et modulaire. L'objectif est de prendre en charge autant de services que possible qui permettent l'authentification à distance.

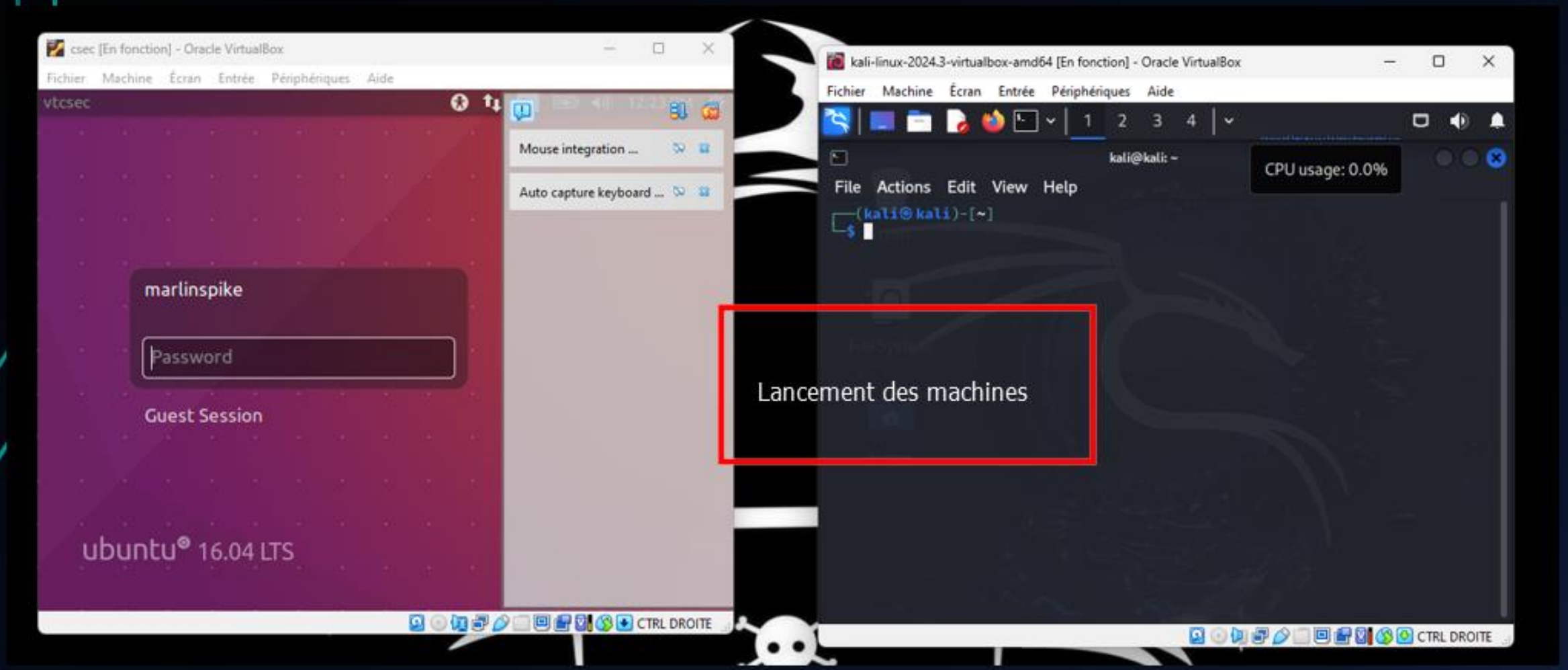
maronekhadim66@gmail.com

TP: Attaque par Force Brute avec l’utilisation des outils Cupp et Medusa

Ce TP consiste à trouver le mot de passe d’une machine vulnérable. Cette machine appartient à un certain MarleySprite. Notons que nous avons que deux informations à savoir la vulnérabilité de la machine et son propriétaire. Nous nous basons sur ses deux informations pour savoir si nous parviendrons à obtenir le mot de passe de la machine. Nous allons utiliser au cours de notre travail les outils cupp et medusu.

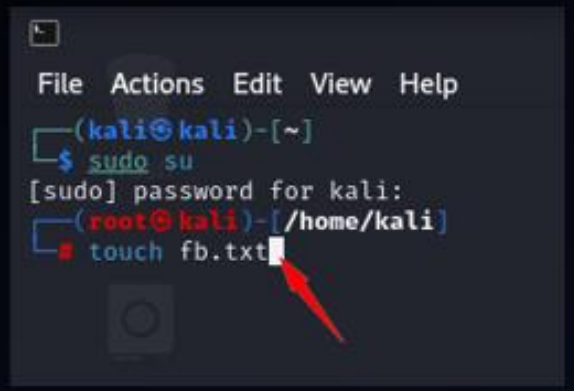
maronekhadim66@gmail.com

TP: Attaque par Force Brute avec l'utilisation des outils Cupp et Medusa



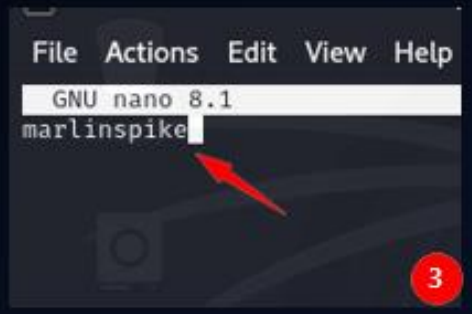
maronekhadim66@gmail.com

TP: Attaque par Force Brute avec l'utilisation des outils Cupp et Medusa

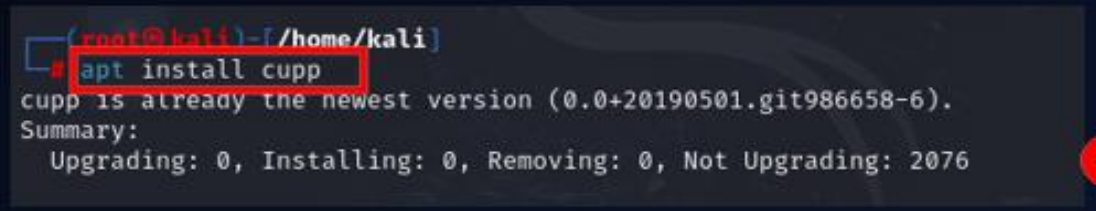


1 Création de fichier fb.txt

2 Editer le fichier crée



3 Rensigner le nom d'utilisateur



4 Installer cupp

maronekhadim66@gmail.com

TP: Attaque par Force Brute avec l'utilisation des outils Cupp et Medusa

Ortions:
w-: compte le nombre de mots
&&: une assertion
mv: deplace un fichier ou un dosier.

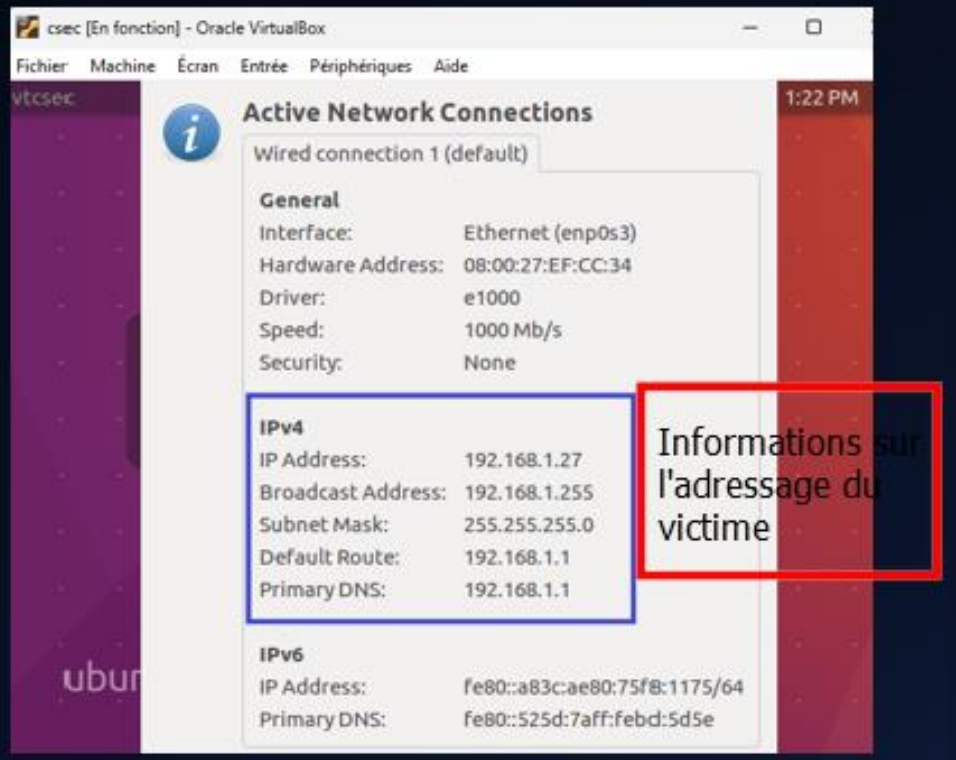
42 mots de passe trouvés

maronekhadim66@gmail.com

TP: Attaque par Force Brute avec l'utilisation des outils Cupp et Medusa

Informations sur l'adressqge de l'attaquant

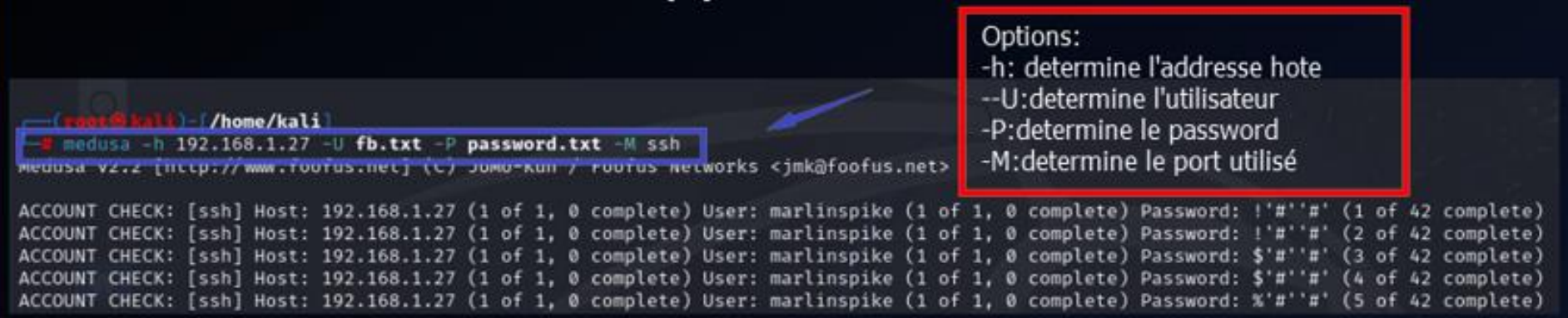
```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.25  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a83c:ae80:75f8:1175  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ad:25:87  txqueuelen 1000  (Ethernet)
        RX packets 2233  bytes 154255 (150.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 5132 (5.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

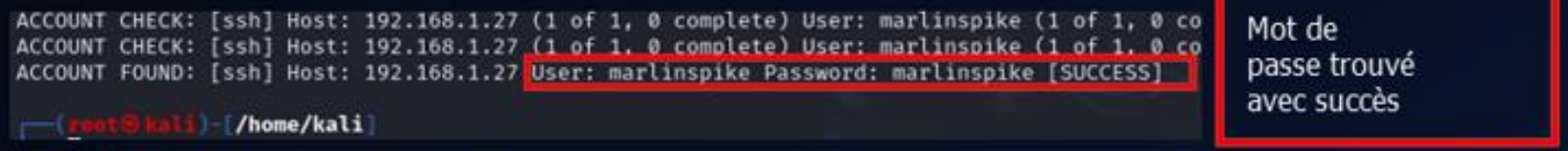


Informations sur l'adressage du victime

maronekhadim66@gmail.com

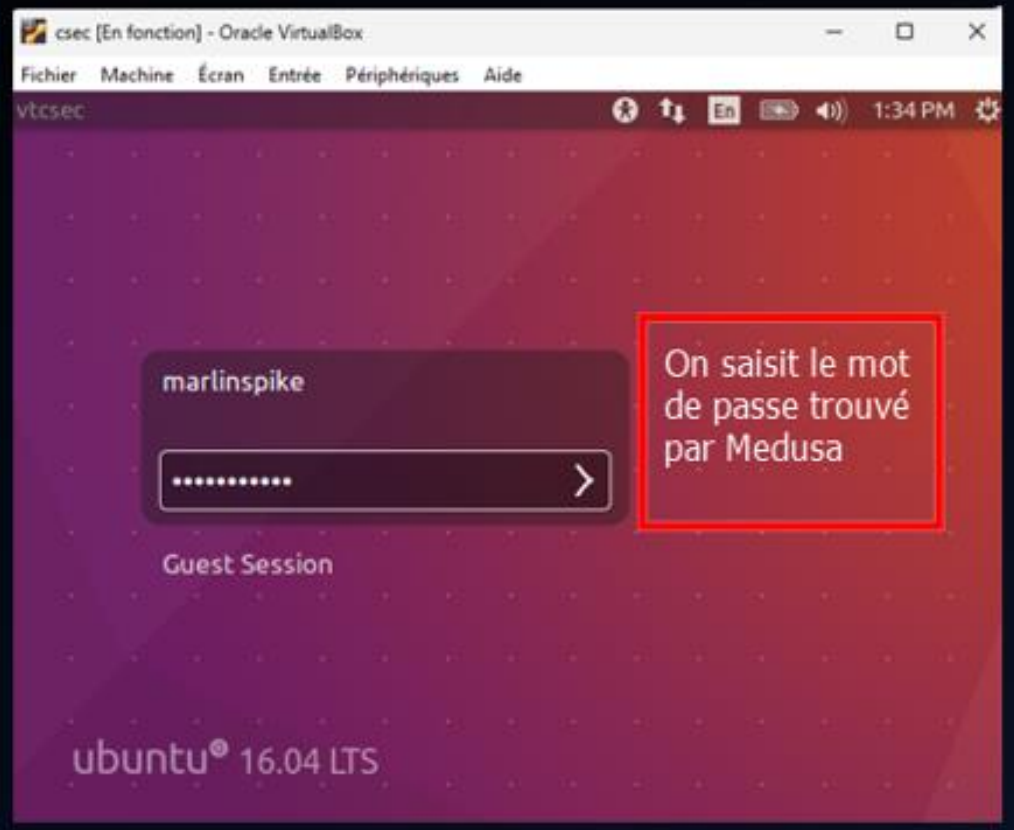
TP: Attaque par Force Brute avec l'utilisation des outils Cupp et Medusa

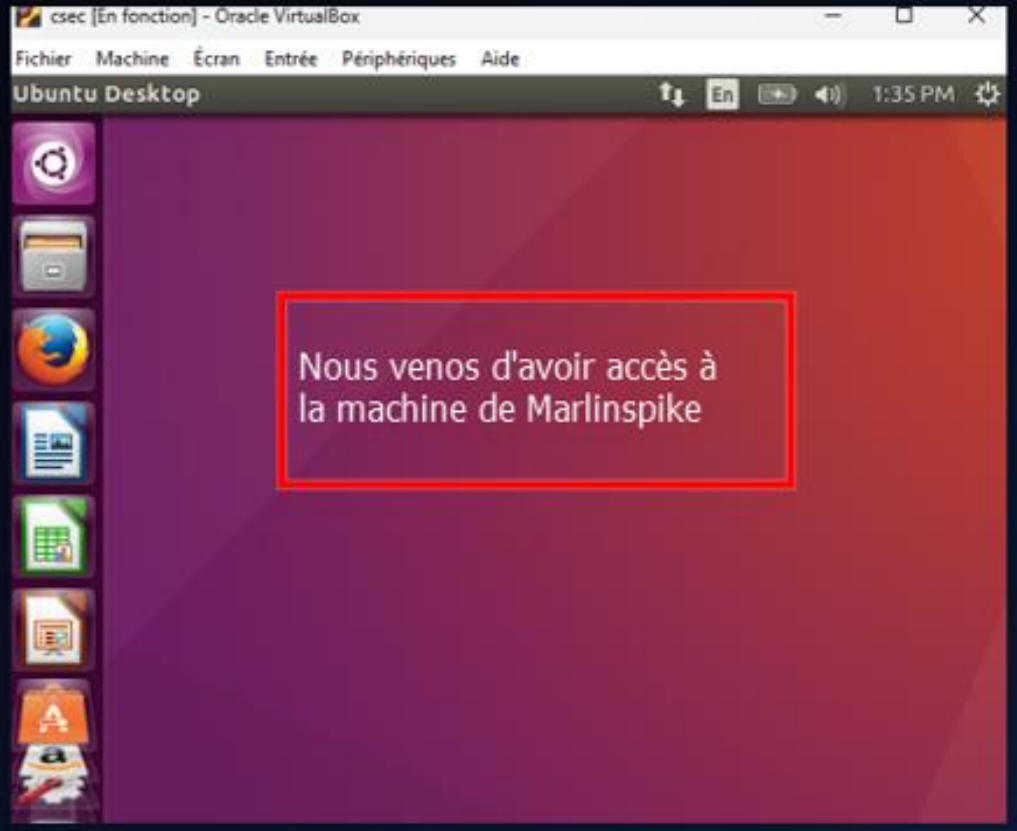




maronekhadim66@gmail.com

TP: Attaque par Force Brute avec l’utilisation des





maronekhadim66@gmail.com

FIN

maronekhadim66@gmail.com