Mon Projet personnel :
Capture the flag (VULNHUB - bulldog)

🎯 CTF : Boulldog 1

Auteur : Nick Frichette
Date de sortie : 28 août 2017
Niveau : Débutant / Intermédiaire
Objectif : Obtenir un accès root et lire le message de félicitations dans le répertoire `/root`

🕹️ Contexte

Le site web de **Bulldog Industries** a été piraté par la **German Shepherd Hack Team**. À nous de découvrir s'il reste des vulnérabilités exploitables !

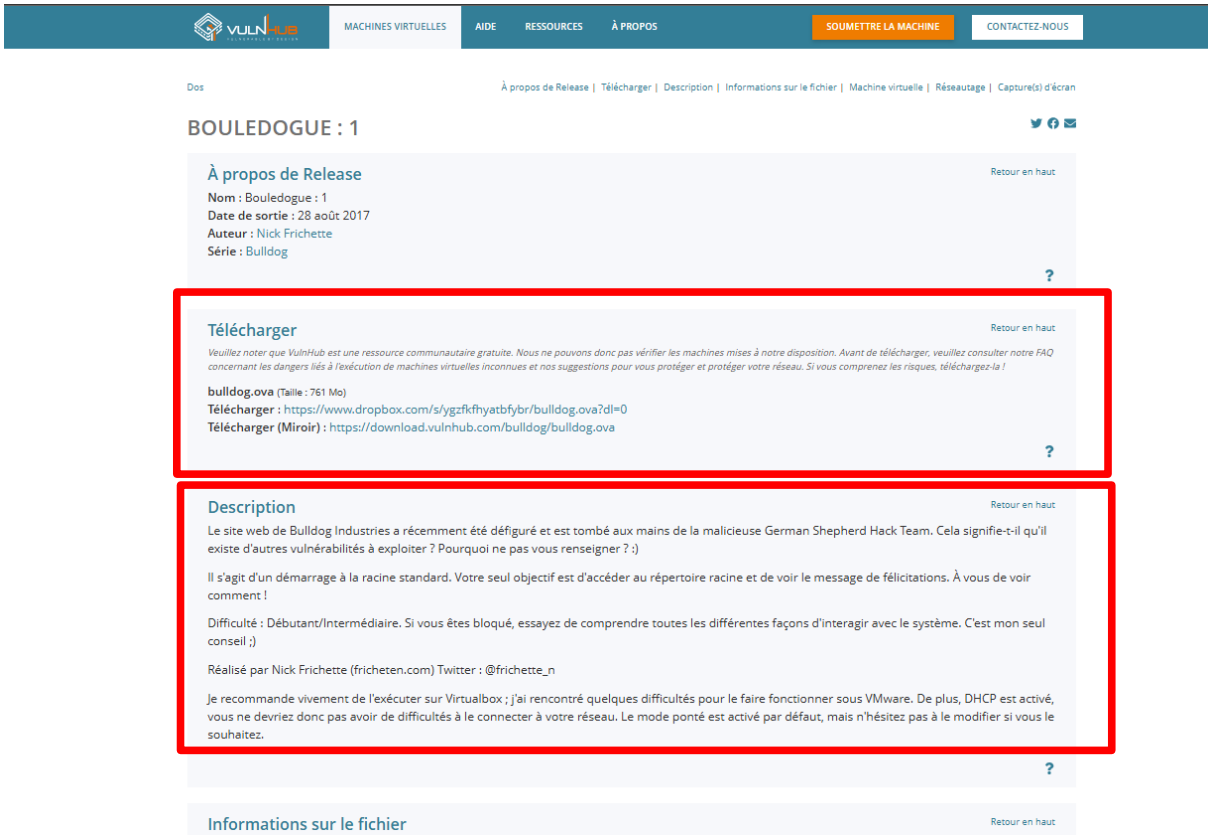
🧰 Infos techniques

- **Format** : Fichier `.ova` (VirtualBox)
- **OS** : Linux
- **Taille** : 761 Mo
- **DHCP** : Activé automatiquement
- **Réseau** : Mode ponté par défaut
- **MD5** : `7073036C6A749714FDEFB47E0E2BF9AA`
- **SHA1** : `CC4C750C1BB547A35F21EF1D66EB51B0ED9B83AE`

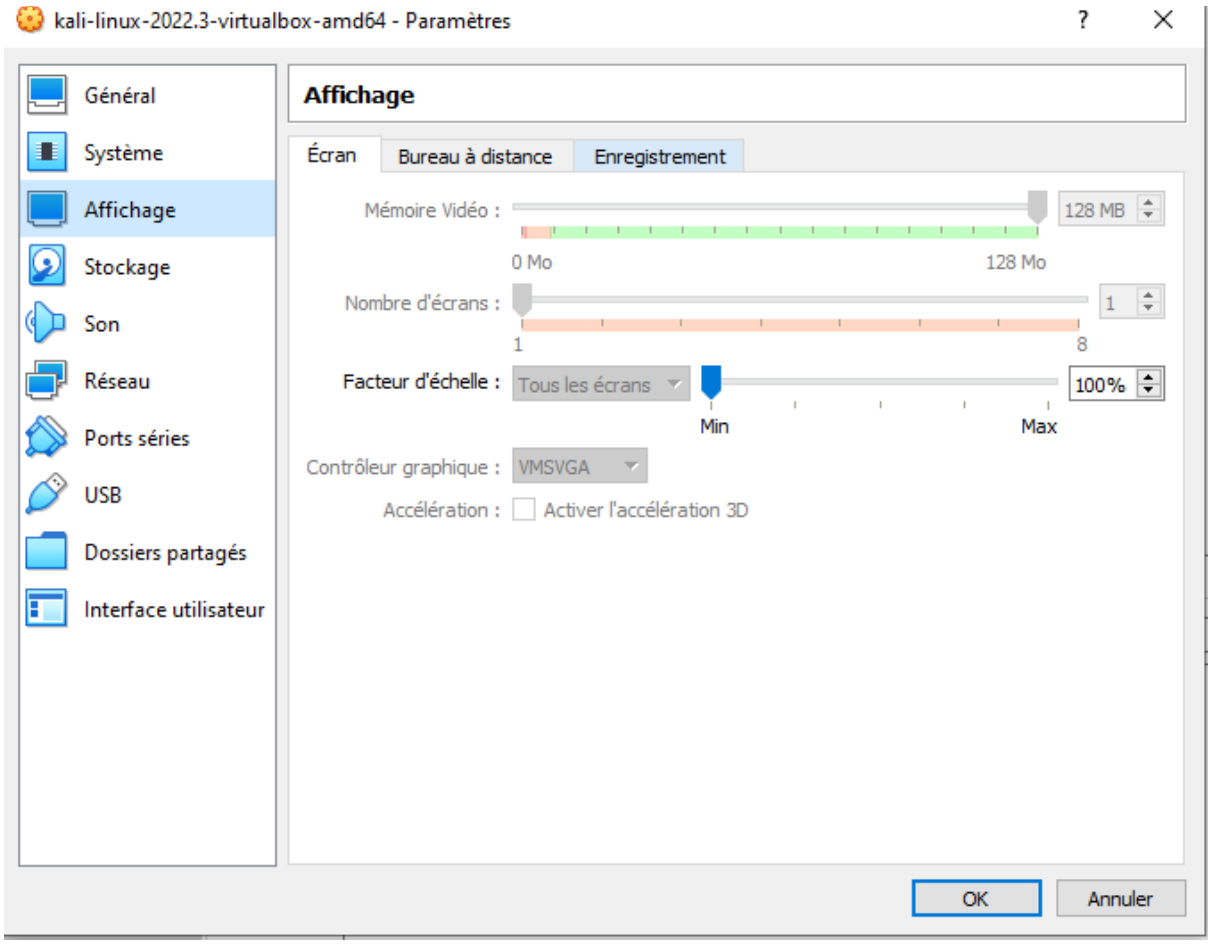
Pour télécharger un CTF sur VulnHub, il faut d’abord se rendre sur le site officiel et éventuellement créer un compte. Ensuite, on parcourt les différentes machines disponibles jusqu’à trouver un défi qui nous intéresse. Une fois sur la page du CTF choisi, on clique sur le lien de téléchargement fourni. Le fichier téléchargé est généralement une image de machine virtuelle, au format OVA ou VMDK. Il ne reste plus qu’à l’importer dans un hyperviseur comme VirtualBox pour commencer à jouer.

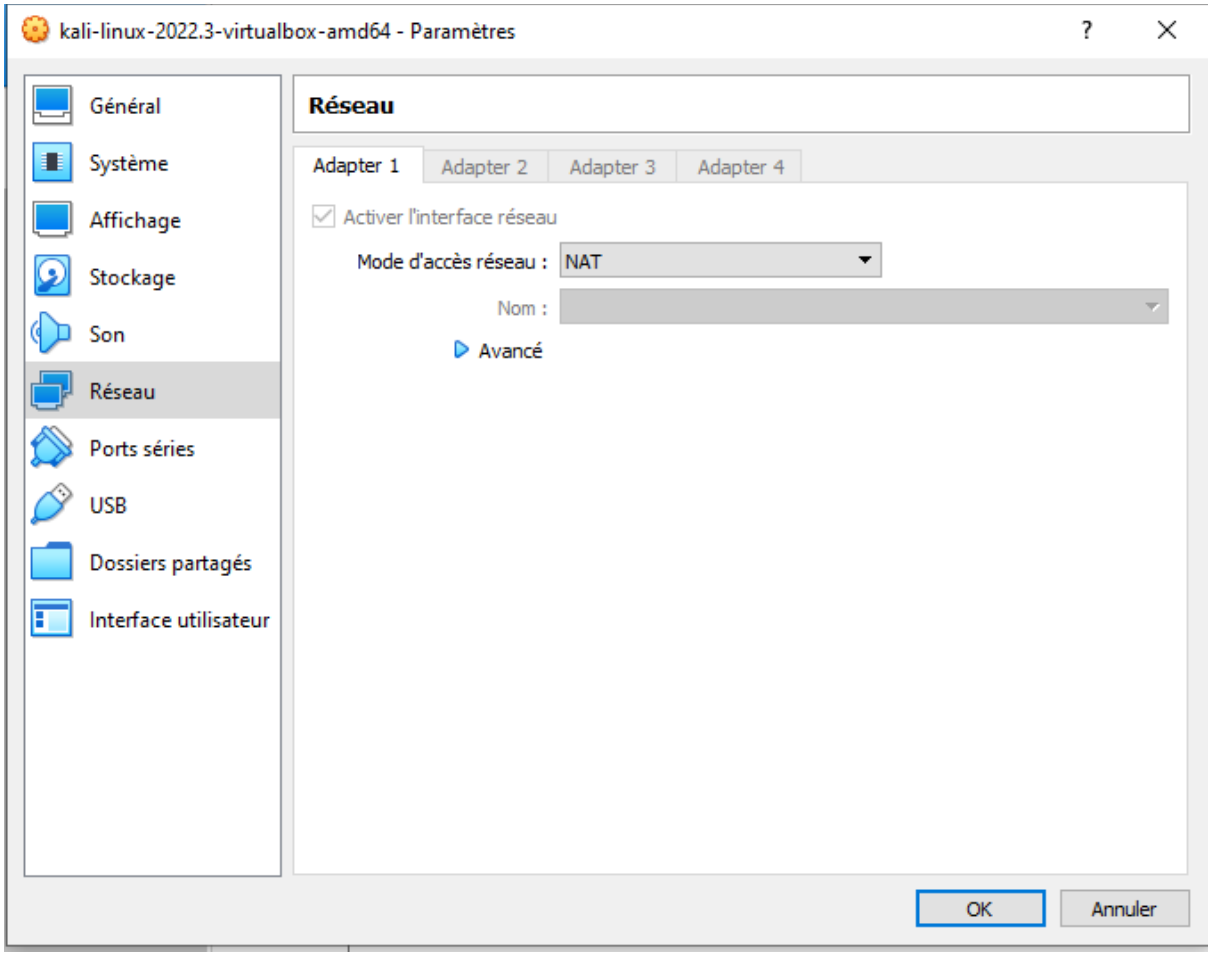
Sur VulnHub, chaque machine virtuelle (VM) proposée pour un CTF est accompagnée d’une description détaillée. Cette description présente généralement le niveau de difficulté, les objectifs du défi, et parfois des indices pour commencer. On y trouve aussi des informations techniques comme le type de fichier, la compatibilité avec les hyperviseurs, et l’adresse IP à configurer.

Après avoir choisi une VM, il suffit de télécharger l'image depuis le lien fourni. Une fois importée dans un hyperviseur, on peut commencer à interagir avec la machine pour résoudre le CTF.

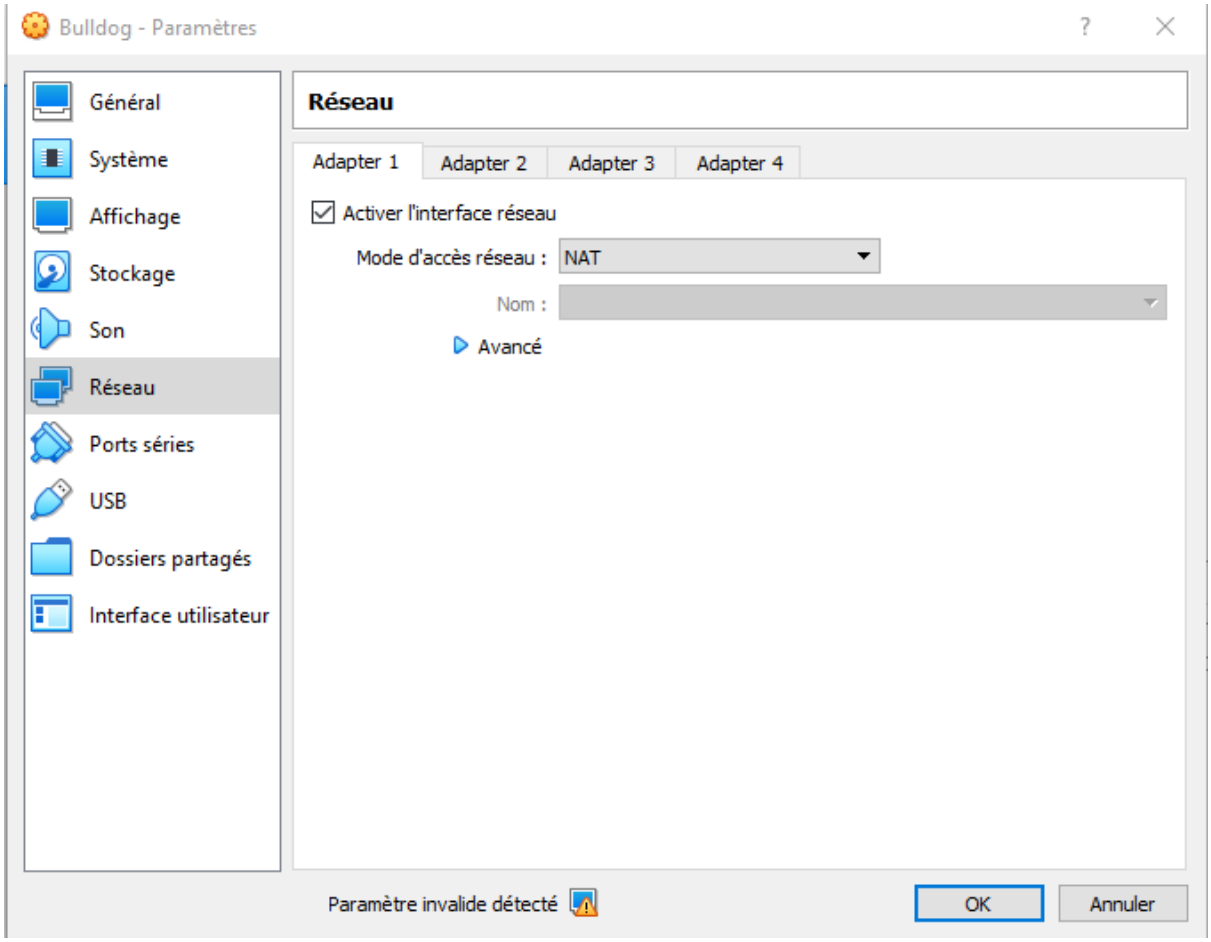


Pour ma machine attaquante, j'utilise Kali Linux 2022 avec une mémoire vidéo de 128 MB, ainsi qu'un accès réseau configuré en NAT, que j'ai exceptionnellement modifié en mode Accès par pont.

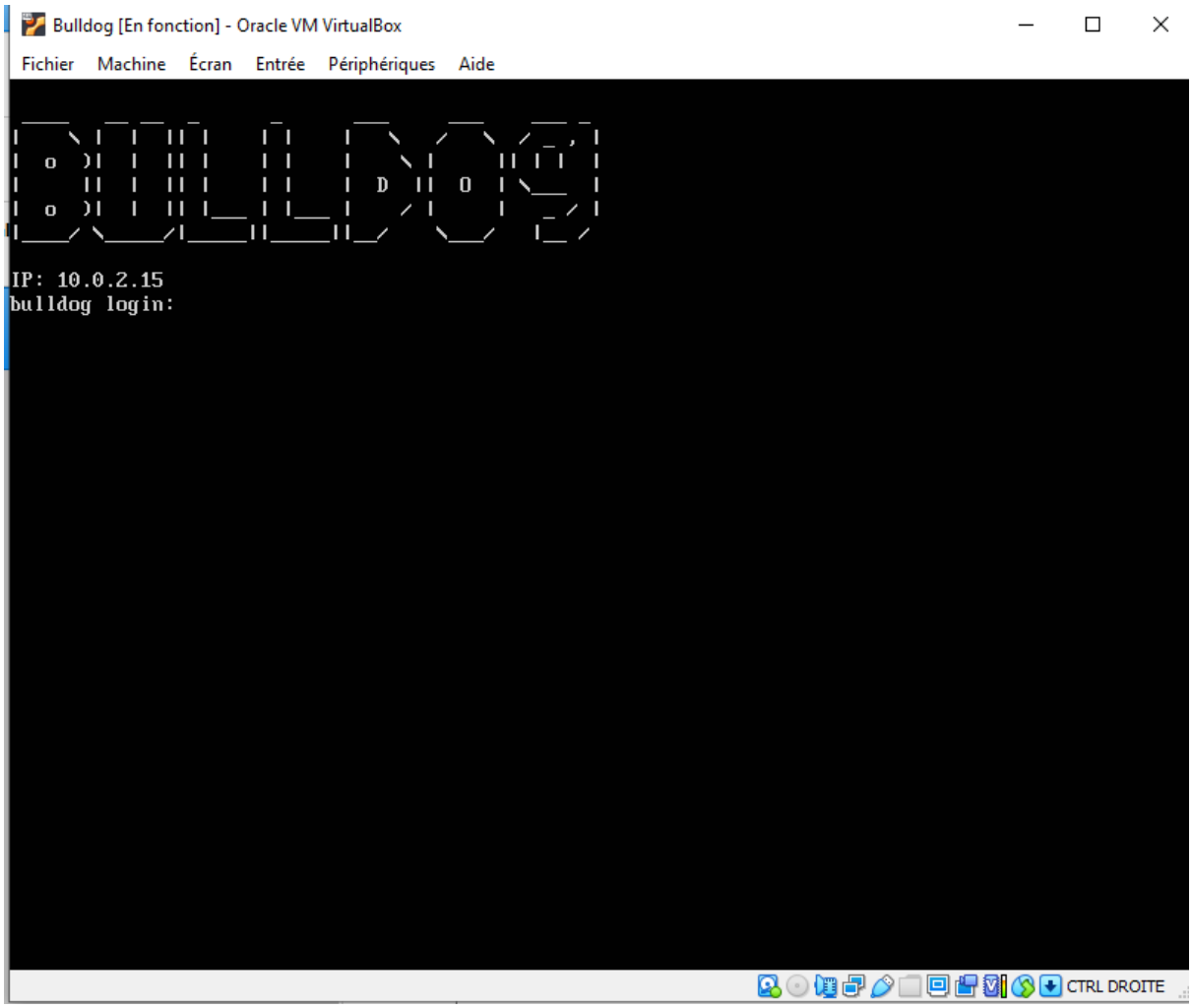

kali-linux-2022.3-virtualbox-amd64 - Paramètres
Général
Système
Affichage
Stockage
Son
Réseau
Ports séries
USB
Dossiers partagés
Interface utilisateur
Affichage
Écran
Bureau à distance
Enregistrement
Mémoire Vidéo :
128 MB
0 Mo
128 Mo
Nombre d'écrans :
1
1
8
Facteur d'échelle :
Tous les écrans
100%
Min
Max
Contrôleur graphique :
VMSVGA
Accélération :
Activer l'accélération 3D
OK
Annuler



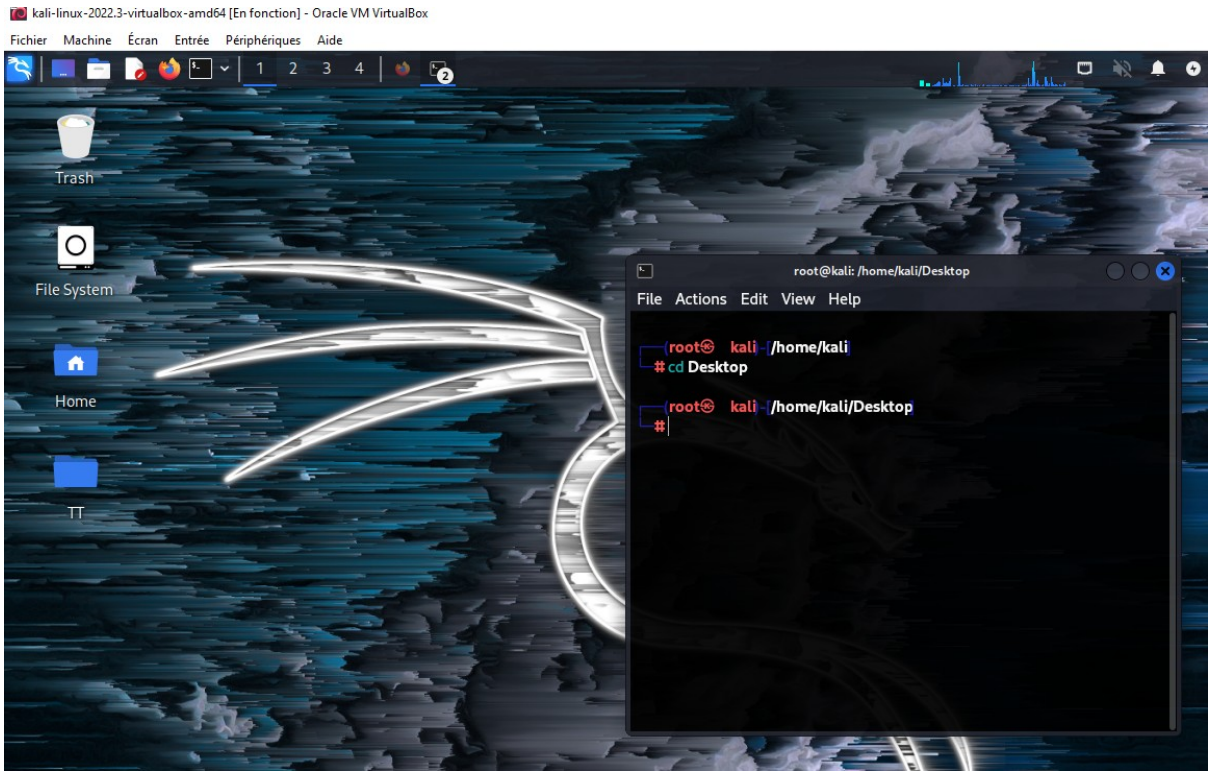
Egalement pour ma machine cible : BULLDOG :


Bulldog - Paramètres
Général
Système
Affichage
Stockage
Son
Réseau
Ports séries
USB
Dossiers partagés
Interface utilisateur
Réseau
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Activer l'interface réseau
Mode d'accès réseau :
NAT
Nom :
Avancé
Paramètre invalide détecté
OK
Annuler

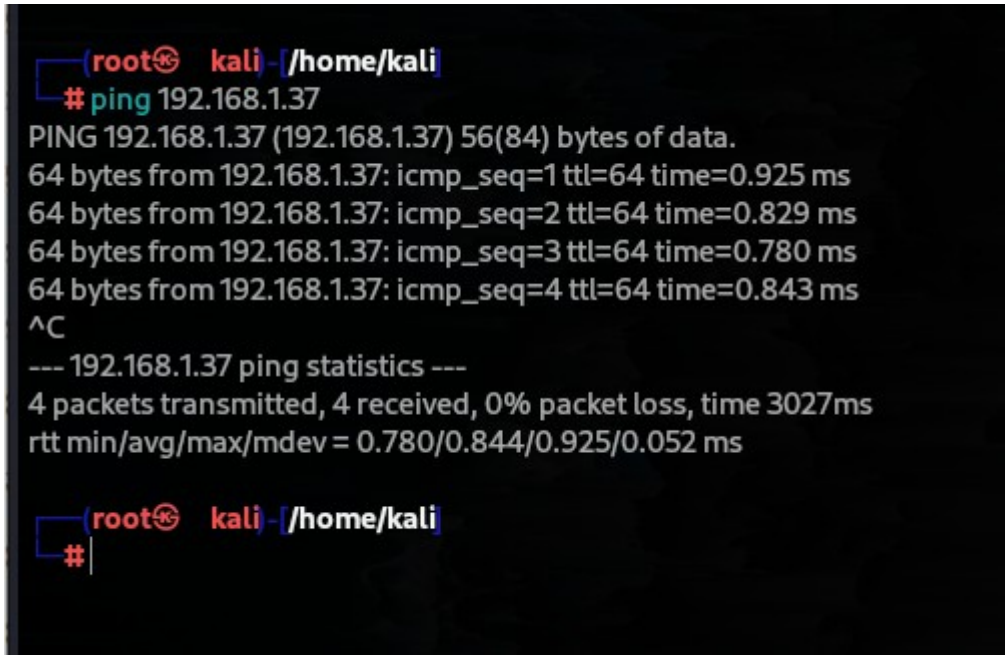
La page d'accueil de la machine cible se présente ainsi, une adresse IP fourni via une réception DHCP et un login dont nous connaissons aucune information.



Voici ma machine KALI LINUX :



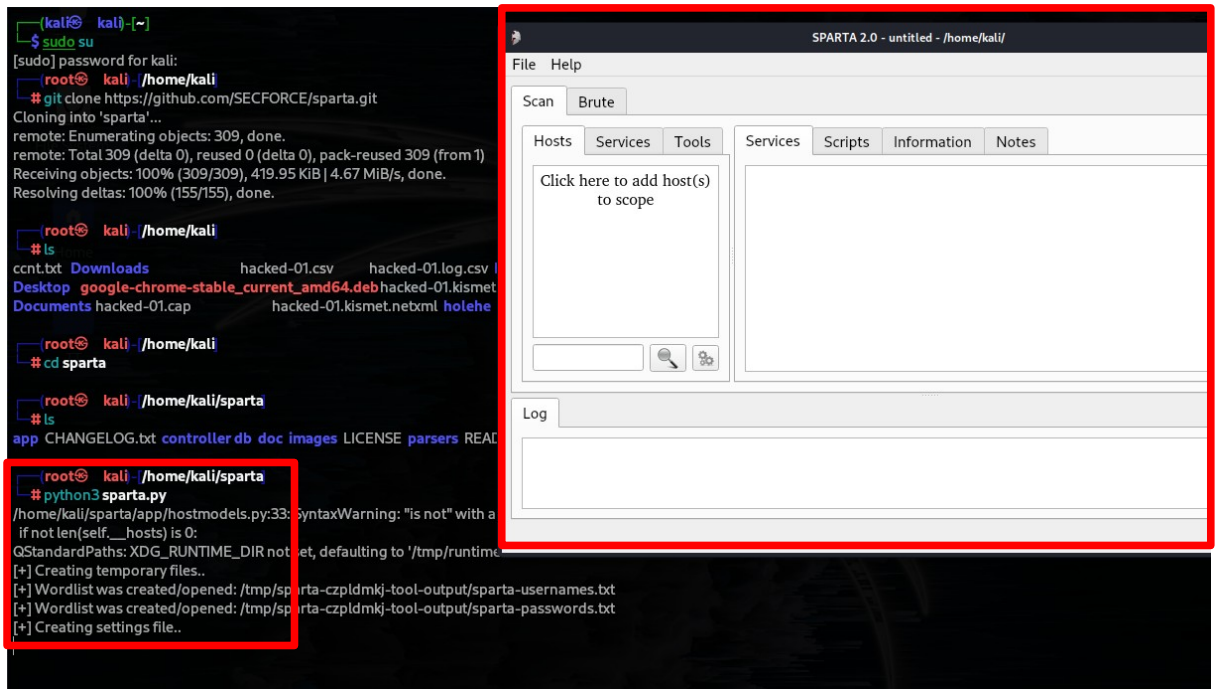
Suite à la modification du mode réseau en "Accès par pont", une nouvelle adresse IP m'a été attribuée. J'ai dû effectuer un ping pour confirmer l'interconnexion et vérifier la communication entre les différentes machines.



Plusieurs outils sont déjà pré installé sur mon kali linux et nous allons utiliser plusieurs d'entre eux afin d'arriver à la fin de ce CTF :


1
2
3
4
Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
42 - Kali & OffSec Links
• Network & Port Scanners
• OSINT Analysis
• Route Analysis
• SMB Analysis
• SMTP Analysis
• SNMP Analysis
• SSL Analysis
amass
dmitry
ike-scan
legion (root)
maltego (installer)
netdiscover
nmap
recon-ng
spiderfoot

Dans ce cas, nous allons utiliser SPARTA, un outil d'analyse doté d'une interface graphique, qui intègre également d'autres services comme Nikto ou Nmap. J'ai dû l'installer via GitHub, car la version que je possédais auparavant n'incluait pas Nikto parmi les utilitaires d'analyse.

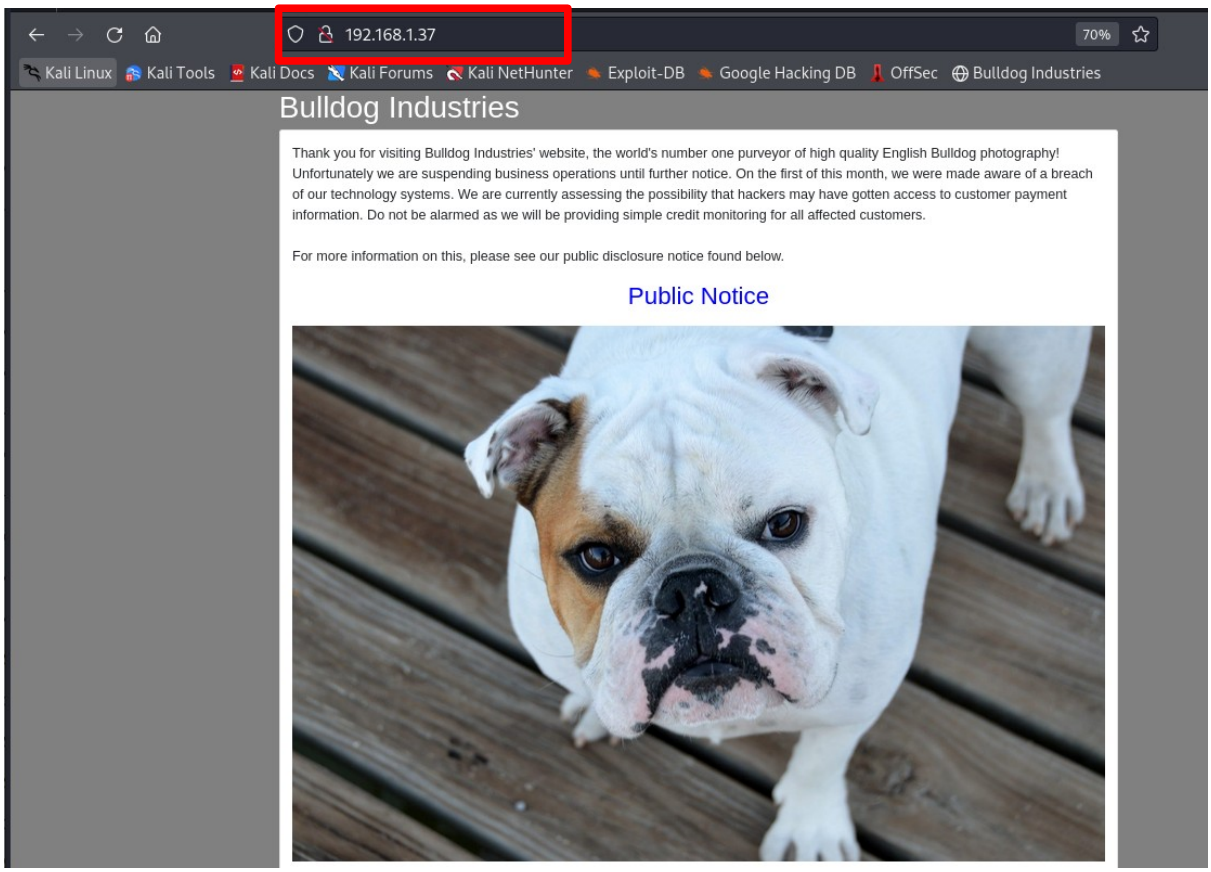


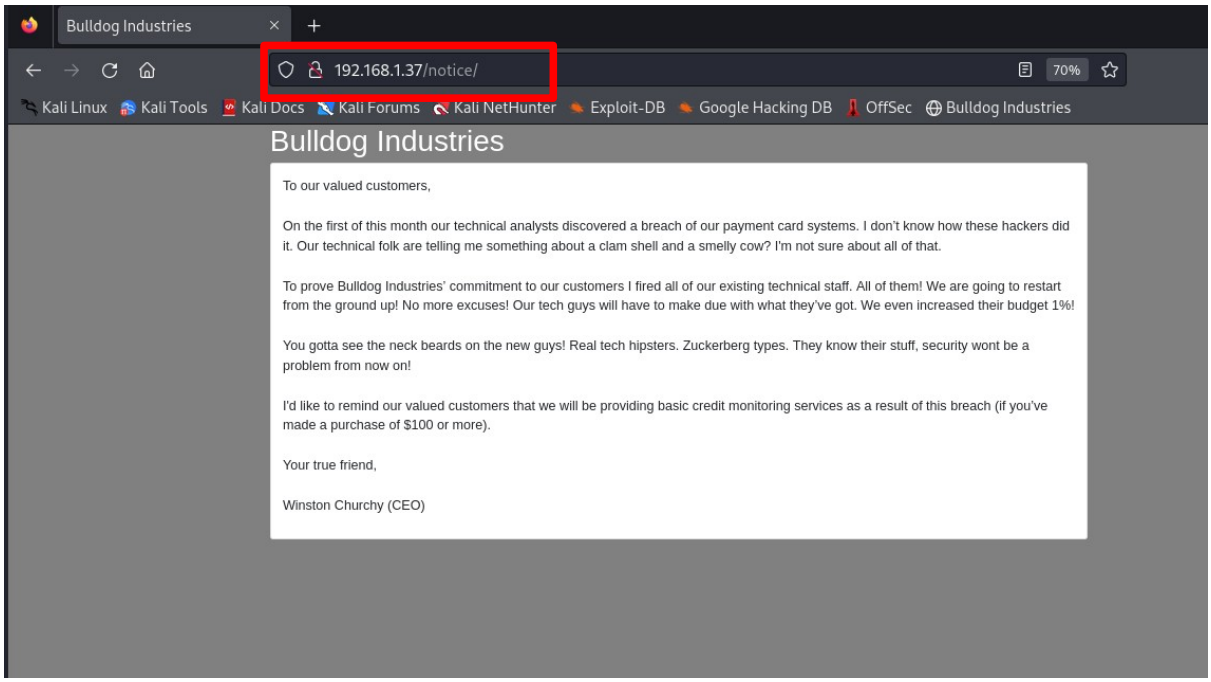
J'ai référencé l'IP à attaquer, et un scan complet a déjà révélé plusieurs informations importantes, notamment la présence des ports 80 et 8080 ouverts, ce qui indique qu'un service web est actif sur la machine.

Log

Progress	Tool	Host	Start time	End time	
	nmap (stage 5)	192.168.1.37	05 Apr 2025 13:46:47	05 Apr 2025 13:46:53	Finished
	nikto (8080/tcp)	192.168.1.37	05 Apr 2025 13:46:42	05 Apr 2025 13:47:47	Finished
	nmap (stage 4)	192.168.1.37	05 Apr 2025 13:46:42	05 Apr 2025 13:46:47	Finished
	nmap (stage 3)	192.168.1.37	05 Apr 2025 13:46:33	05 Apr 2025 13:46:42	Finished
	nikto (80/tcp)	192.168.1.37	05 Apr 2025 13:46:28	05 Apr 2025 13:47:33	Finished

Je me suis dirigé vers la page web de la machine via son adresse IP. Cette page décrit le type de société et mentionne que le site a été victime d'une cyberattaque.





Il est fortement recommandé de toujours examiner le code source

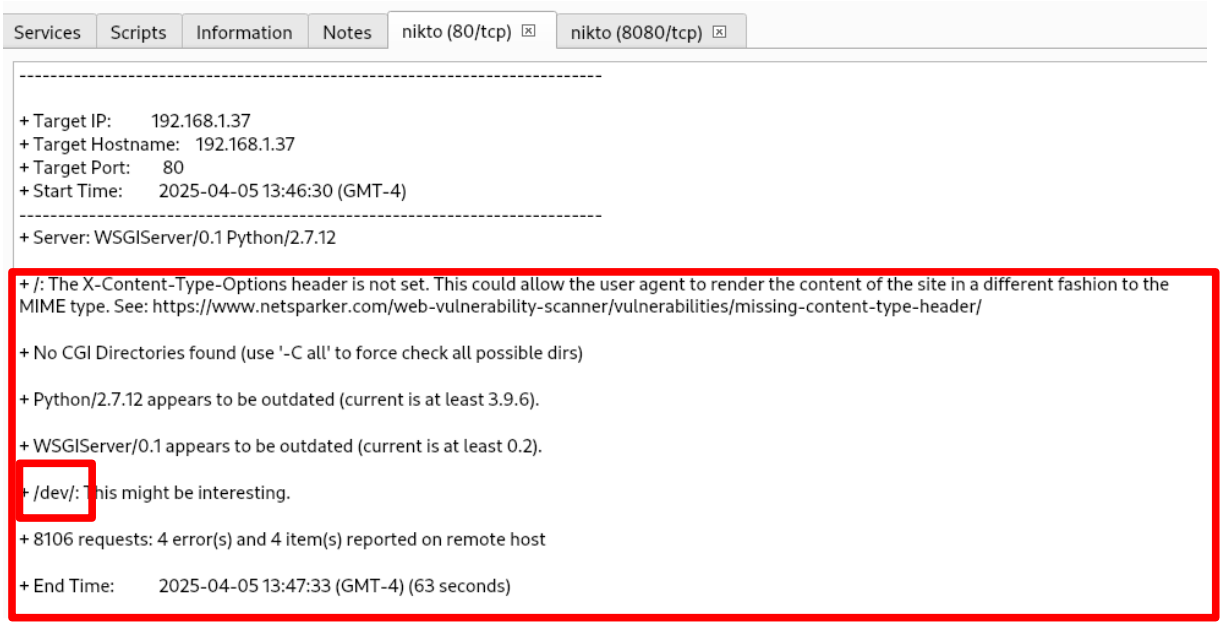
des pages web lors d'un CTF pour collecter certaines informations "cachées". Cependant, aucune information n’a été relevée dans ce cas.

```
1
2  <!DOCTYPE html>
3  <html lang="en">
4  <head>
5    <title>Bulldog Industries</title>
6    <meta charset="utf-8">
7    <meta name="viewport" content="width=device-width, initial-scale=1">
8    <link rel="stylesheet" href="/static/css/bootstrap.css">
9    <script src="/static/js/jquery.min.js"></script>
10   <script src="/static/js/bootstrap.js"></script>
11 </head>
12 <body style="background-color:grey">
13
14 <div class="container">
15   <h1><a href="/" style="color:white" >Bulldog Industries</a></h1>
16   <div class="card panel-default" style="padding:1em">
17     <div class="card-block">
18         <p><font size="4em">Thank you for visiting Bulldog Industries' website, the world's number
19     one purveyor of high quality English Bulldog photography! Unfortunately we are
20     suspending business operations until further notice. On the first of this month,
21     we were made aware of a breach of our technology systems. We are currently
22     assessing the possibility that hackers may have gotten access to customer
23     payment information. Do not be alarmed as we will be providing simple credit
24     monitoring for all affected customers.<br><br>For more information on this, please
25     see our public disclosure notice found below.</font></p>
26
27     <p><font size="6em"><center><a href="/notice" style="color:blue">Public Notice</a></center></font></p>
28
29     <center><img style="max-width:100%" src="/static/bulldog.jpg"/></center>
30     </div>
31   </div>
32 </div>
33
34 </body>
35 </html>
36
37
```

```
<!DOCTYPE html>
<html lang="en">
<head>
  <title>Bulldog Industries</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="/static/css/bootstrap.css">
  <script src="/static/js/jquery.min.js"></script>
  <script src="/static/js/bootstrap.js"></script>
</head>
<body style="background-color:grey">

<div class="container">
  <h1><a href="/" style="color:white" >Bulldog Industries</a></h1>
  <div class="card panel-default" style="padding:1em">
    <div class="card-block">
        <p><font size="4em">To our valued customers,<br><br>On the first of this month our
    technical analysts discovered a breach of our payment card systems. I don't know
    how these hackers did it. Our technical folk are telling me something about a clam
    shell and a smelly cow? I'm not sure about all of that.<br><br>
    To prove Bulldog Industries' commitment to our customers I fired all of our existing
    technical staff. All of them! We are going to restart from the ground up! No more
    excuses! Our tech guys will have to make due with what they've got. We even
    increased their budget 1%! <br><br>You gotta see the neck beards on the new guys!
    Real tech hipsters. Zuckerberg types. They know their stuff, security wont be a
    problem from now on!<br><br>
    I'd like to remind our valued customers that we will be providing basic credit
    monitoring services as a result of this breach (if you've made a purchase of $100
    or more).<br><br>
    Your true friend,<br><br>Winston Churchy (CEO)</font></p>
    </div>
  </div>
</div>

</body>
</html>


```

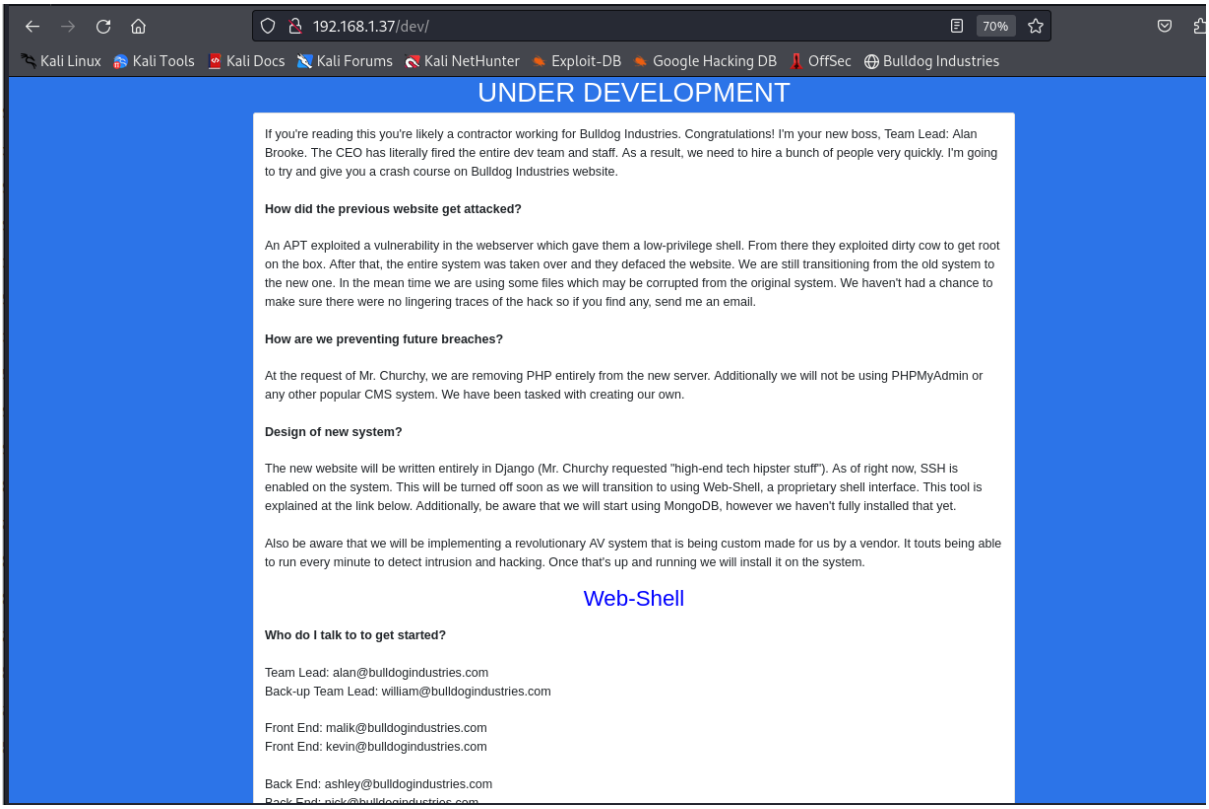
L'analyse de Nikto nous a fourni de nombreuses informations

pertinentes pour la suite de mon Capture The Flag, notamment les failles exploitables par exemple la faille XSS (Cross-Site Scripting) permet à un attaquant d'injecter du code malveillant dans une page web, souvent pour voler des informations sensibles comme des cookies ou manipuler l'affichage de la page. sur le serveur web ainsi que des répertoires ou des pages cachées. Dans ce cas, un répertoire "/dev/" a été relevé.

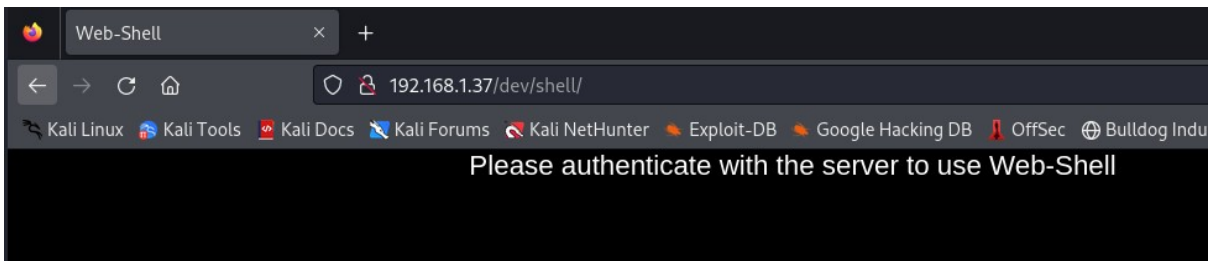


Nous pouvons constater qu’une autre page est présente, mais qui

n’est pas destinée aux utilisateurs lambda ou aux clients. Cette page explique simplement comment la cyberattaque qui les a touchés a eu lieu, ses conséquences et les mesures de prévention. On y trouve également un webshell, qui fonctionne comme une console d’administration de la machine, mais accessible via un navigateur web.



Vous vous dites sûrement que si l'on possède un webshell, nous avons forcément gagné, mais ce n'est pas le cas, car une autorisation est requise.



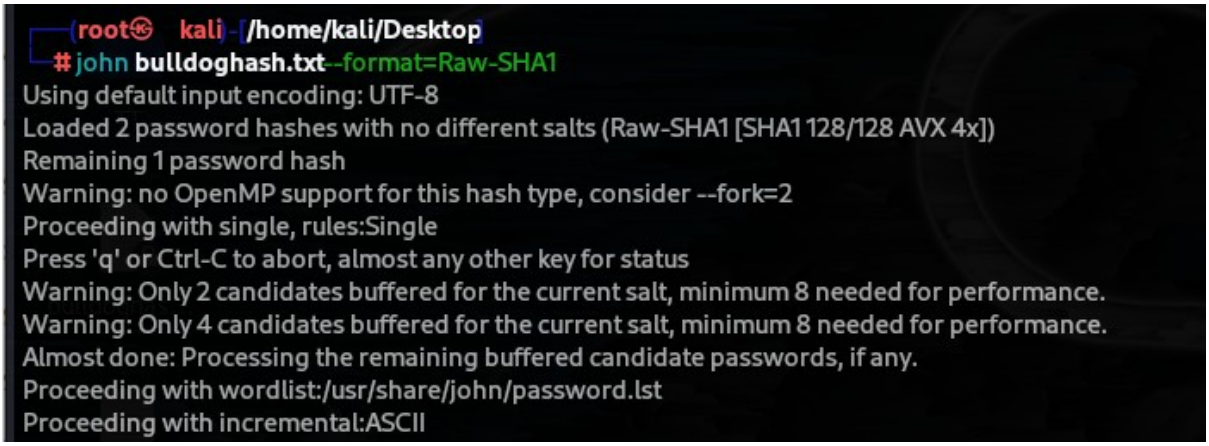
Sur la page web, il y a également des informations concernant des

adresses, c’est pourquoi j’ai exploré le code source de la page. J’y ai trouvé des mots de passe hashés. Un mot de passe hashé est un mot de passe transformé en une valeur fixe à l’aide d’un algorithme mathématique, appelé "hash". Cette valeur est unique pour chaque mot de passe, et il est pratiquement impossible de retrouver le mot de passe d’origine à partir du hash, offrant ainsi une meilleure sécurité.

```
   <b>Who do I talk to to get started?</b><br><br>

   <!--Need these password hashes for testing. Django's default is too complex-->
   <!--We'll remove these in prod. It's not like a hacker can do anything with a hash-->
   Team Lead: alan@bulldogindustries.com<br><!--6515229daf8dbdc8b89fed2e60f107433da5f2cb-->
   Back-up Team Lead: william@bulldogindustries.com<br><br><!--38882f3b81f8f2bc47d9f3119155b05f954892fb-->
   Front End: malik@bulldogindustries.com<br><!--c6f7e34d5d08ba4a40dd5627508ccb55b425e279-->
   Front End: kevin@bulldogindustries.com<br><br><!--0e6ae9fe8af1cd4192865ac97ebf6bda414218a9-->
   Back End: ashley@bulldogindustries.com<br><!--553d917a396414ab99785694afd51df3a8a8a3e0-->
   Back End: nick@bulldogindustries.com<br><br><!--ddf45997a7e18a25ad5f5cf222da64814dd060d5-->
   Database: sarah@bulldogindustries.com<br><!--d8b8dd5e7f000b8dea26ef8428caf38c04466b3e-->
   </font></p>
   </div>
  </div>
</div>

</body>
</html>
```

J'ai donc créé un fichier texte sur ma machine afin d'organiser les informations collectées et de préparer l'attaque. Cela permet de centraliser les données nécessaires pour une exploitation efficace.

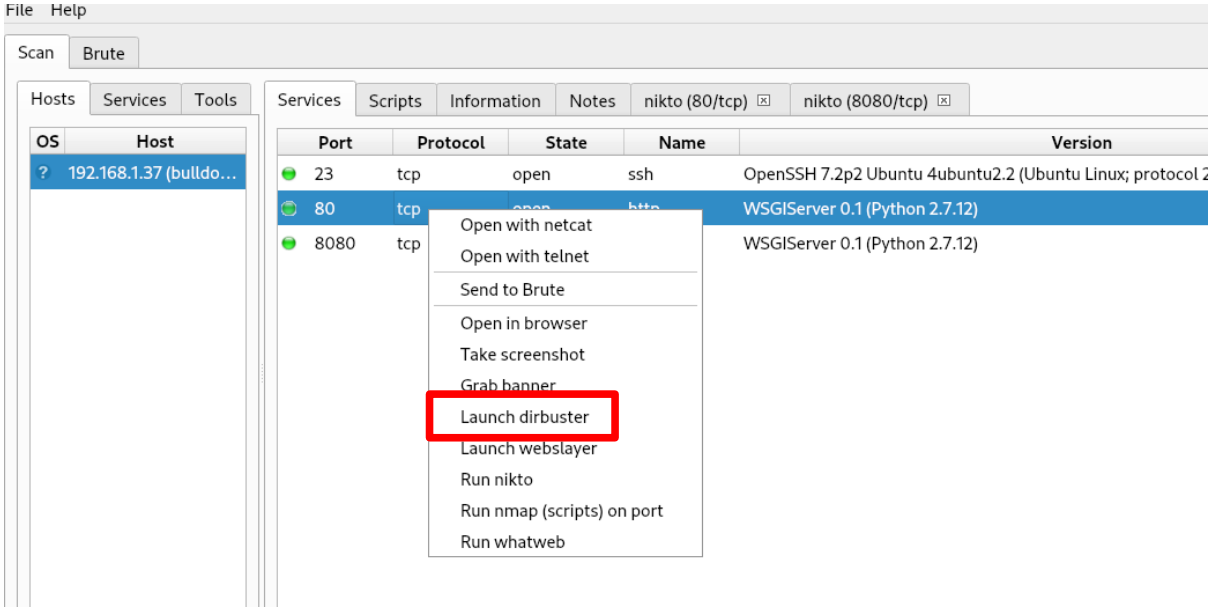
Attaque par brute force avec John the Ripper.
Pour procéder à l'attaque, j'ai utilisé l'utilitaire John the Ripper, qui est spécialement conçu pour effectuer des attaques par brute force sur des mots de passe hashés. Cet outil permet de tester différentes combinaisons de mots de passe à l'aide de wordlists. Heureusement, une wordlist était déjà fournie avec l'outil, facilitant ainsi le processus d'attaque.



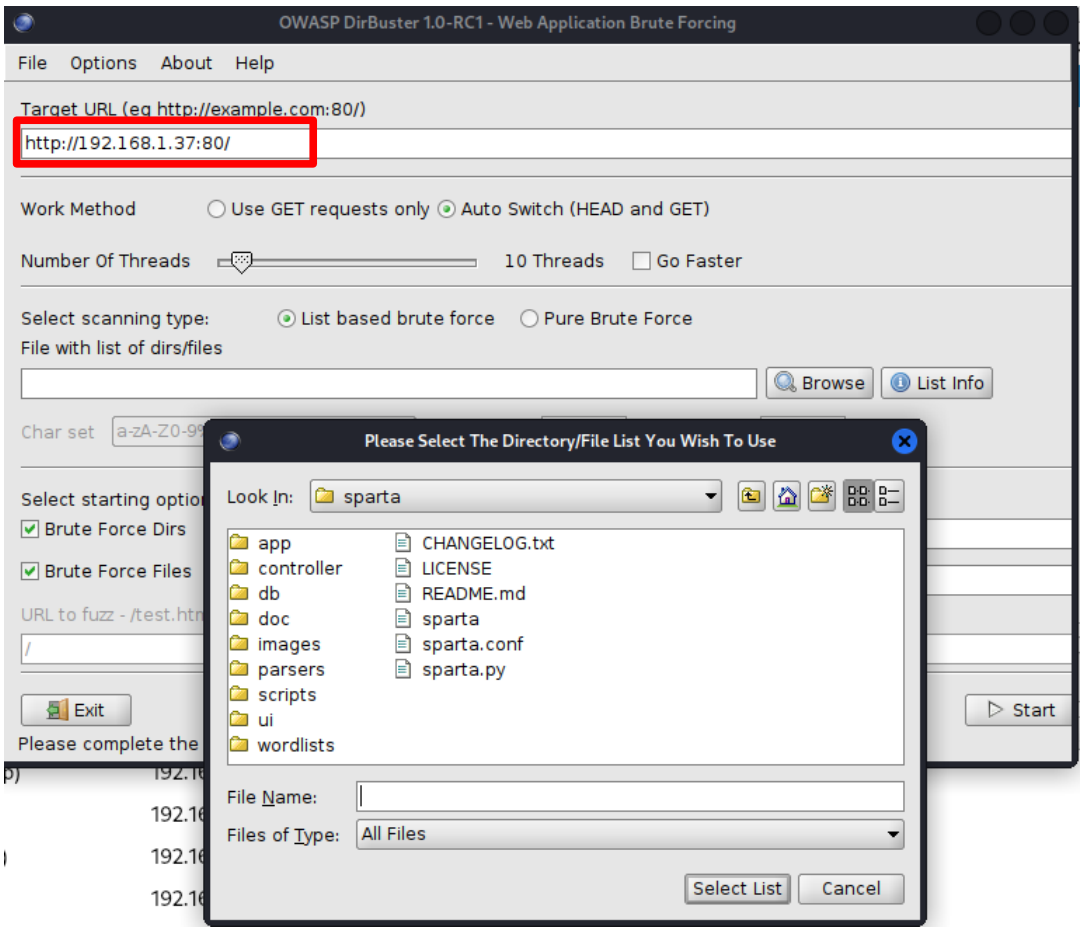
En attendant les résultats de l'attaque par brute force, nous allons procéder à un lancement de DirBuster, qui va cibler la page web en question.

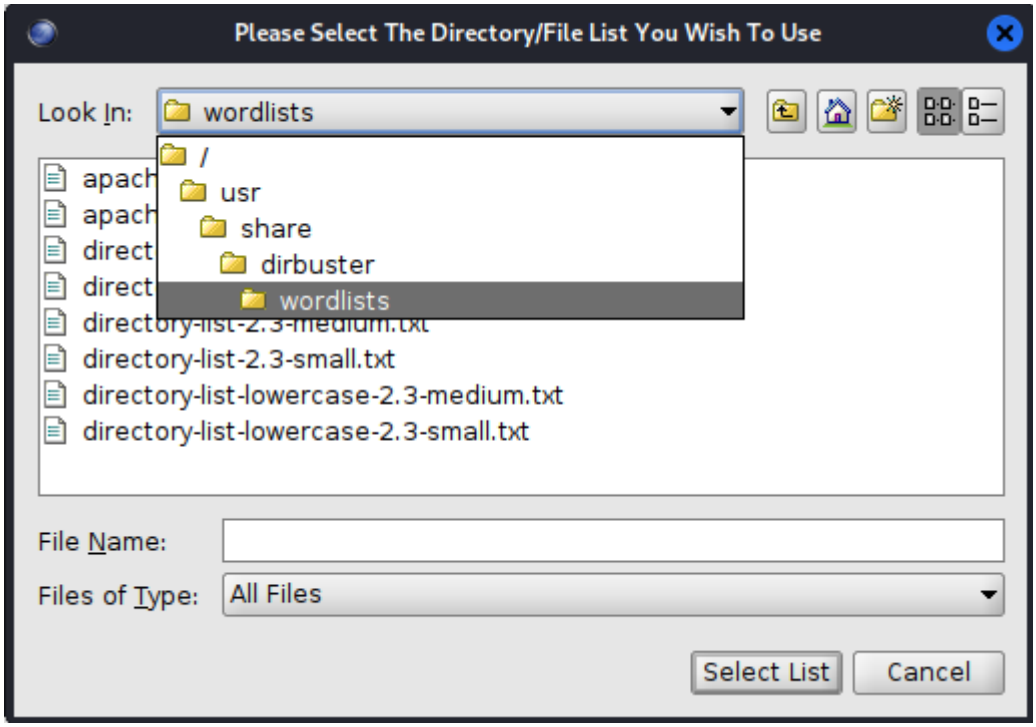
Explication de DirBuster :

DirBuster est un outil utilisé pour découvrir des répertoires ou des fichiers cachés sur un serveur web. Il fonctionne en envoyant un grand nombre de requêtes HTTP avec des mots de passe ou des chemins courants pour tester si des ressources sensibles ou non référencées sont accessibles. Cela peut aider à identifier des pages cachées ou des vulnérabilités qui ne sont pas visibles directement depuis l'interface utilisateur du site web.



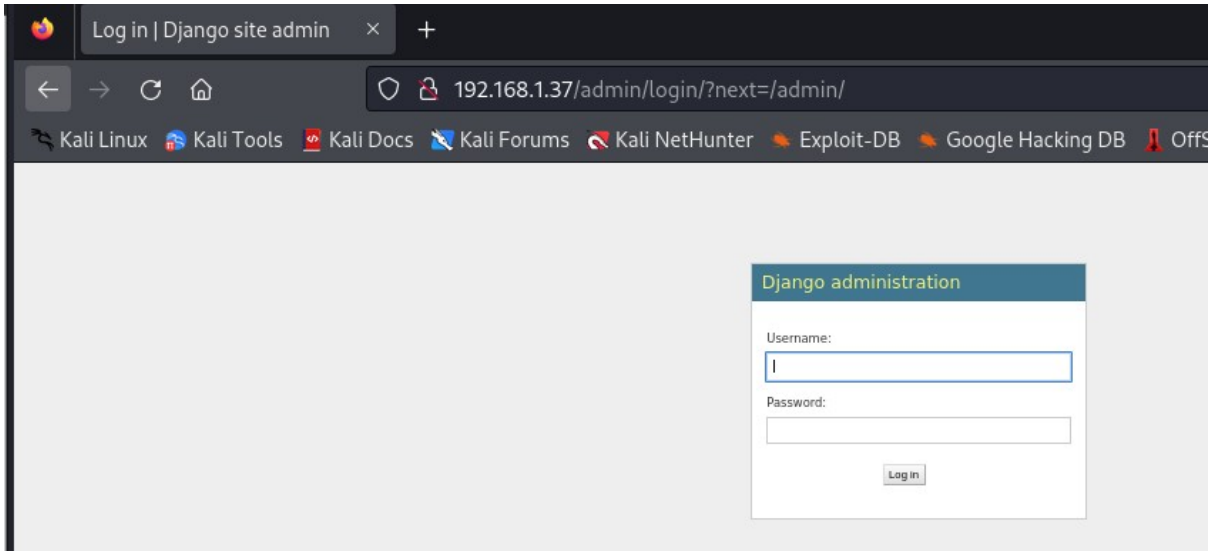
DirBuster nous fournit une wordlist déjà configurée pour tester toutes les combinaisons possibles. Cette liste se trouve dans le répertoire suivant : /usr/share/dirbuster/wordlists.



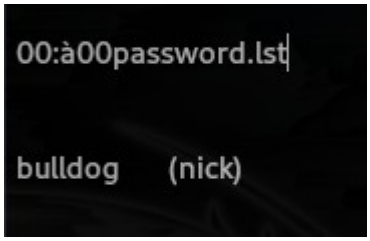


Plusieurs pages ont été révélées, dont une qui semble importante : /admin/, qui nous redirige vers une page de login. Nous allons donc utiliser les résultats obtenus via l'attaque par dictionnaire précédent pour nous authentifier.

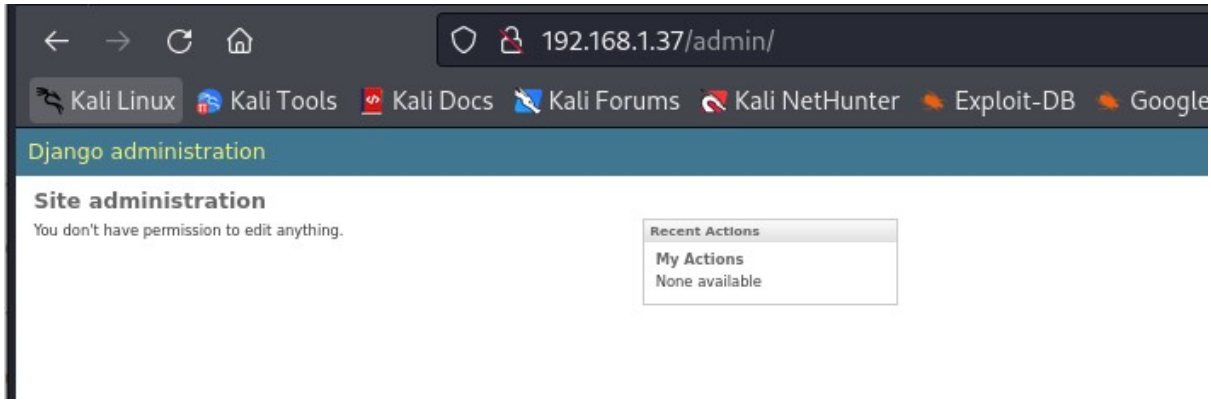
Type	Found
Dir	/
File	/notice
File	/static/js/jquery.min.js
File	/static/js/bootstrap.js
Dir	/admin/
Dir	/admin/auth/
Dir	/admin/auth/group/
Dir	/admin/login/



J’ai trouvé un seul mot de passe, ce qui indique probablement que je suis sur la bonne voie. Les autres comptes ont peut-être un chiffrement ou des mots de passe plus complexes.

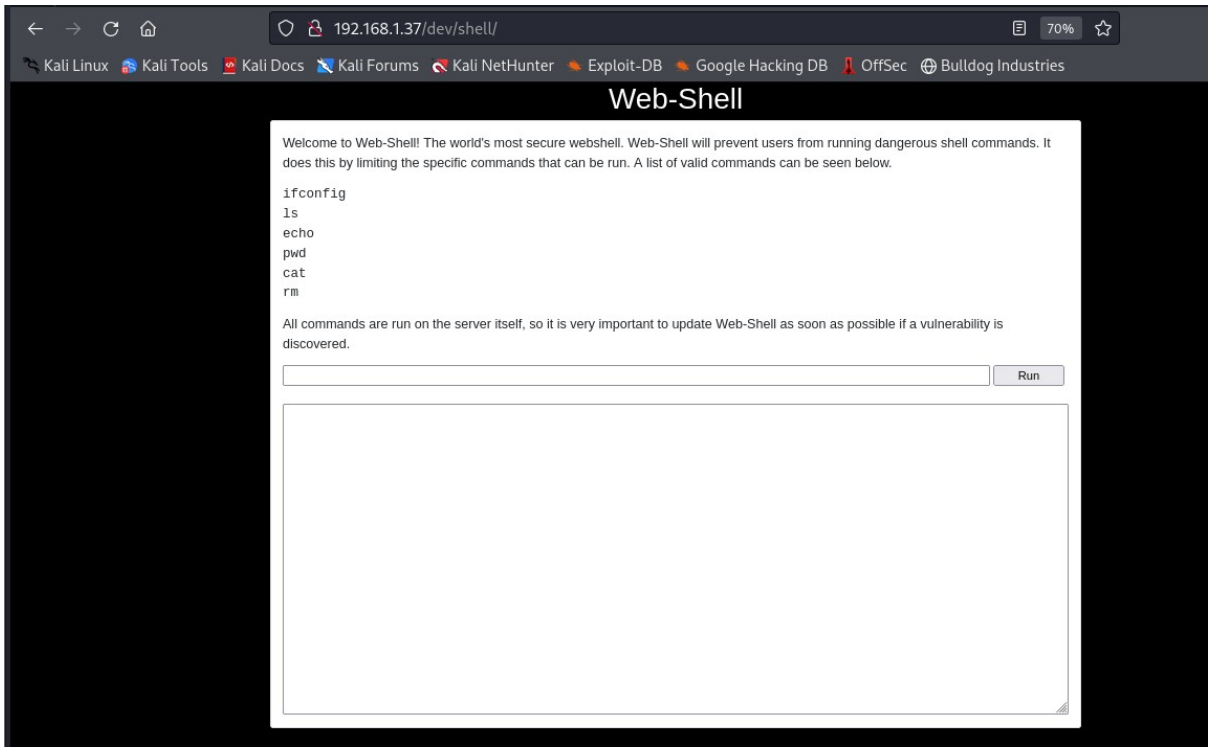


L’authentification a bien fonctionné avec le nom d'utilisateur "nick" et le mot de passe "bulldog".



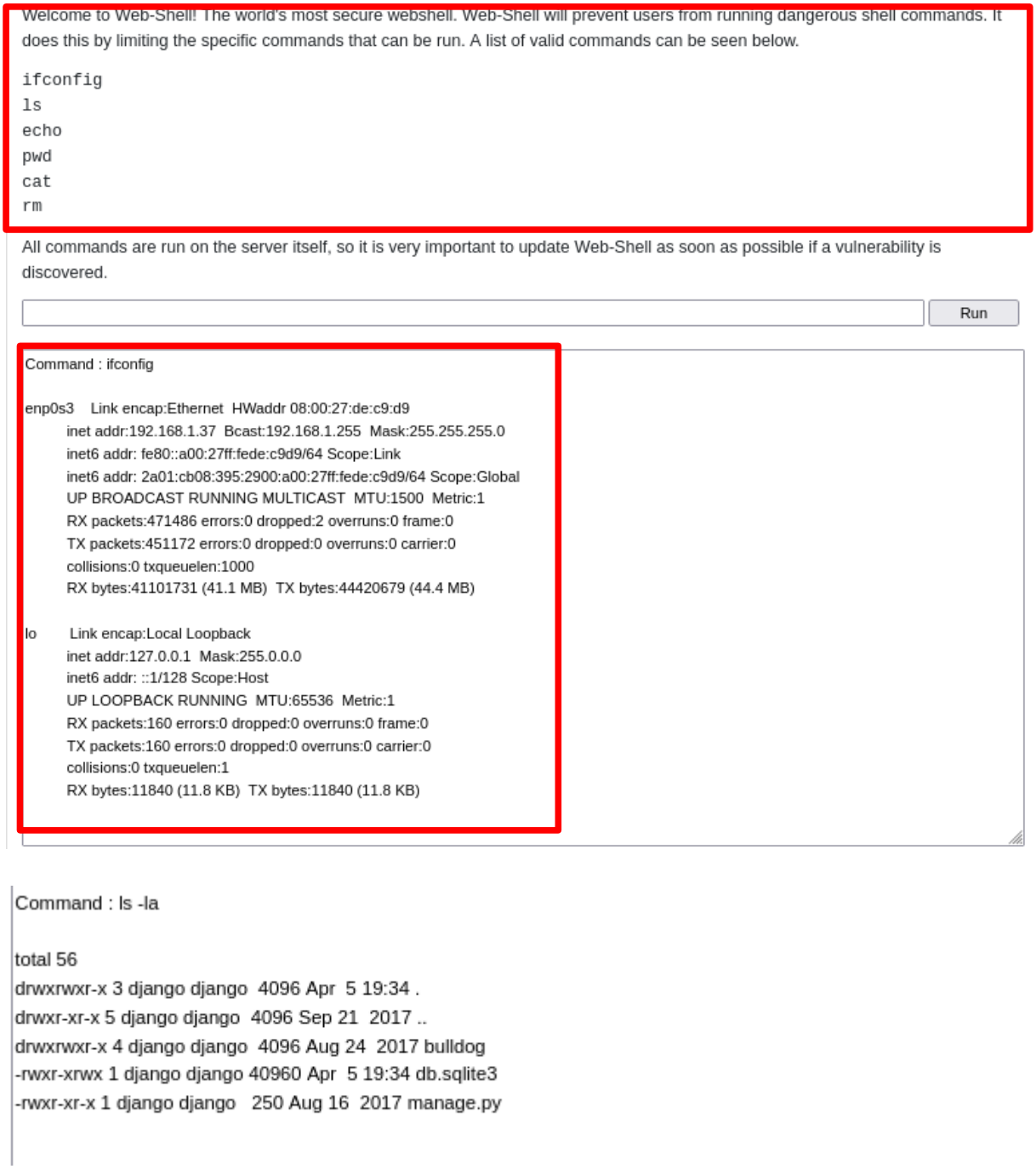
Je me suis rappelé que le webshell requiert une authentification

pour y accéder. Je suis donc retourné et le résultat a été différent : j'ai maintenant un accès complet à la machine, grâce à l'authentification obtenue précédemment.



Je remarque que le webshell fourni offre des fonctionnalités limitées

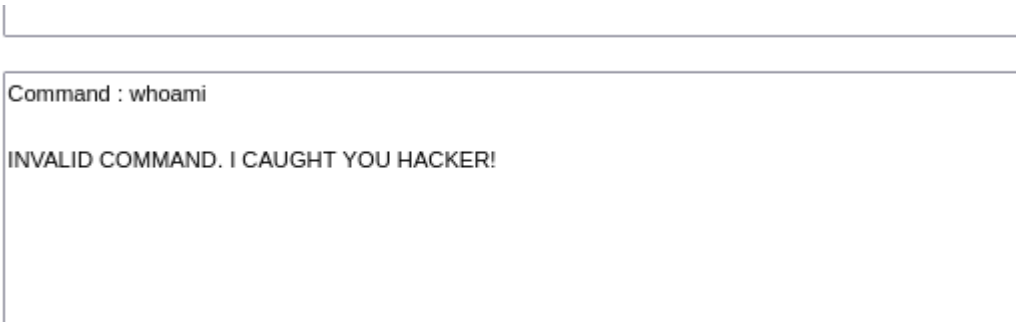
pour l'utilisation des commandes. Par exemple, je peux utiliser "ifconfig" pour obtenir plusieurs informations, comme l'adresse IP de la machine, ou encore les commandes "cat" et "rm" pour créer ou supprimer des fichiers. Cela a considérablement compliqué la tâche...



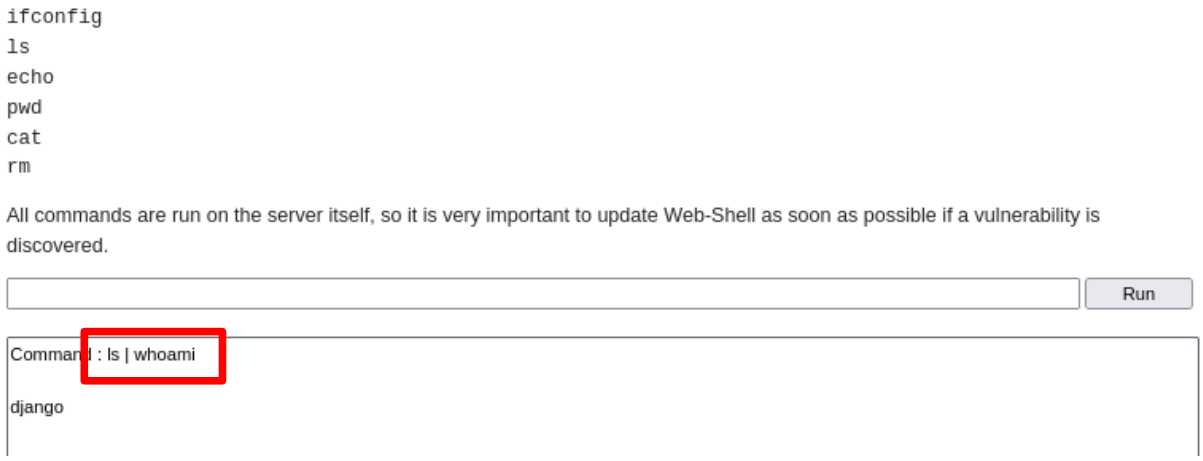
Je suis allé vérifier le fichier passwd dans le répertoire /etc pour

consulter les logins. Avant, il était possible d'attaquer directement via ce fichier, car les mots de passe n'étaient pas remplacés par des "X", mais cela date de très longtemps.

Lorsque j'essaie d'utiliser une commande non permise, un message d'erreur s'affiche : "Je t'ai attrapé HACKER".

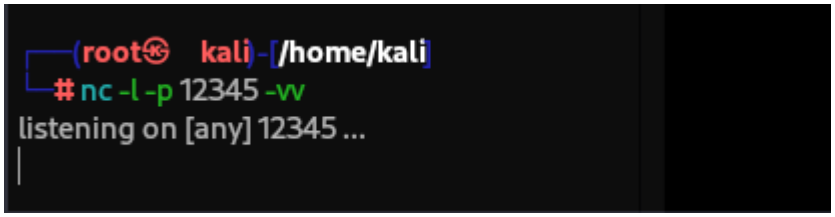


J’ai effectivement trouvé une méthode pour utiliser n’importe quelle commande en utilisant pip pour enchaîner plusieurs commandes. Nous pouvons confirmer que cela fonctionne, car j’ai utilisé la même commande qui génère le message d’erreur, et cela a fonctionné.



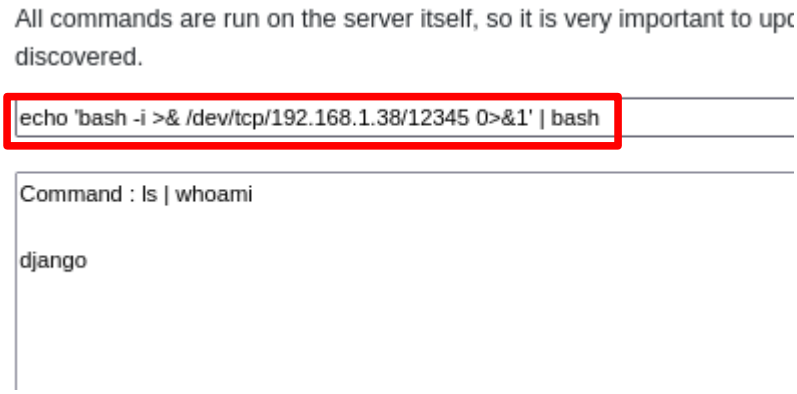
Ce site m'a énormément aidé, car il m'a fourni une méthode pour tenter un reverse shell, Un reverse shell consiste à établir une connexion où le serveur (ou la machine compromise) se connecte à l'attaquant, permettant ainsi à ce dernier de contrôler la machine cible comme s'il y était physiquement présent.depuis le serveur webshell, afin que le serveur écoute les commandes que je lui demande d'exécuter. C'est comme si nous prenions le contrôle de sa console shell à distance.

La commande **nc -l -p 12345 -vv** utilise **Netcat** pour écouter sur le port **12345**. L'option **-l** met Netcat en mode écoute, attendant une connexion entrante. L'option **-p 12345** spécifie le port à utiliser, ici **12345**. Les options **-vv** activent un mode verbeux, affichant des informations détaillées sur la connexion. Cela permet de recevoir des connexions entrantes, comme dans le cas d'un reverse shell.



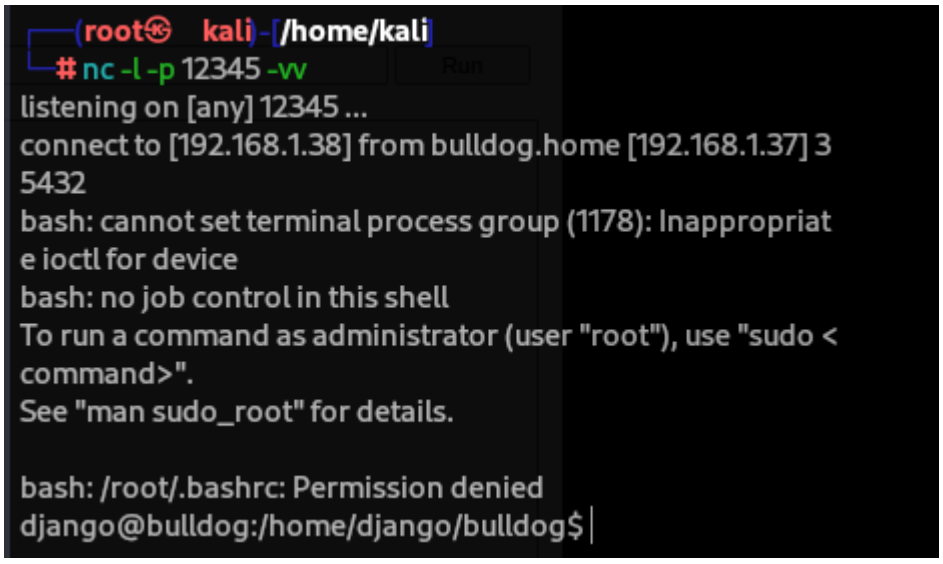
nous allons donc utiliser la commande en spécifiant l'ip de

l’attaquant et le port à l’écoute :

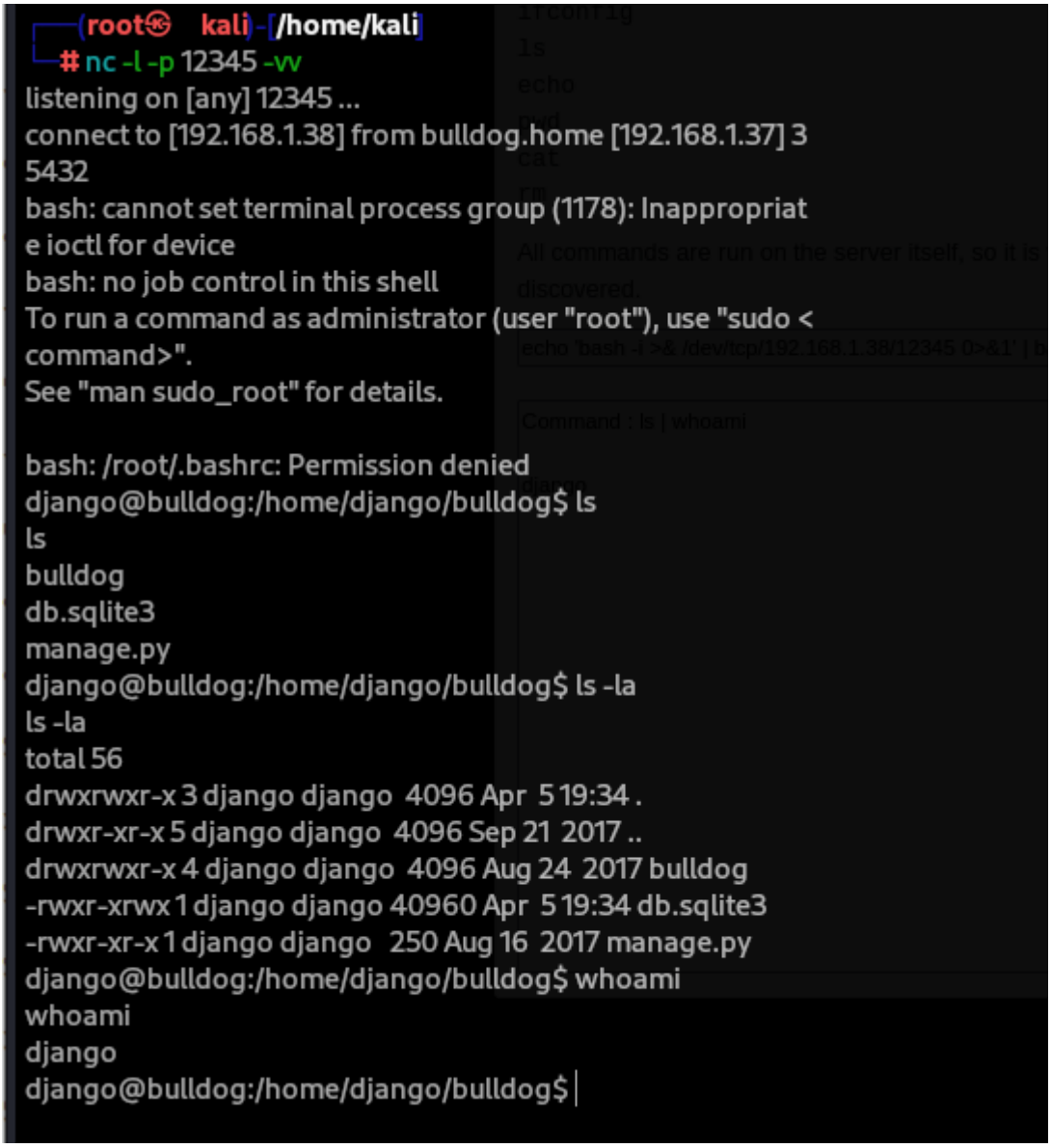


Mon attaque en reverse shell a fonctionné et un prompt est apparu.

Un prompt est une invite de commande qui indique que le système est prêt à recevoir des instructions de l'utilisateur. Dans le contexte d'un reverse shell, cela signifie que l'attaquant a réussi à établir une connexion avec la machine cible et peut maintenant exécuter des commandes sur celle-ci à travers ce prompt. C'est comme un terminal distant permettant de contrôler la machine compromise.



Nous pouvons donc utiliser n’importe quelle commande sans limite et sans détour :



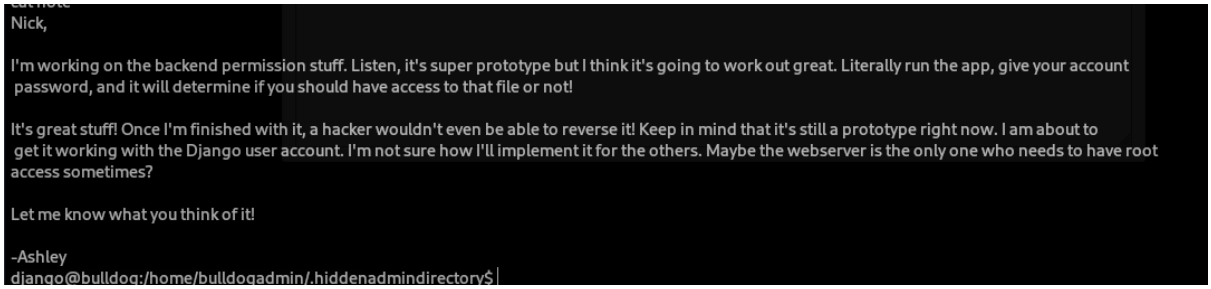
Ici nous remarquons le que répertoir root est bloqué suite à un manque de permission :

```
django@bulldog:/home$ ls
ls
bulldogadmin
django
django@bulldog:/home$ cd
cd
bash: cd: /root: Permission denied
django@bulldog:/home$
```

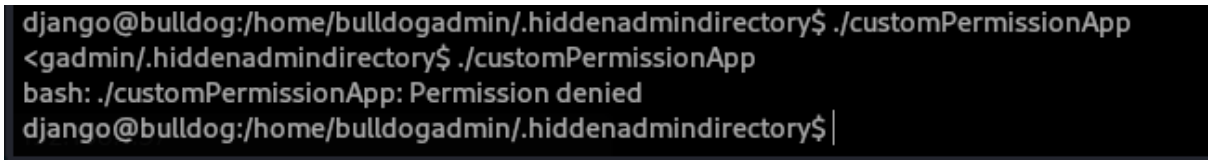
Un dossier m'a interrompu, c'était le "bulldogadmin". J'y suis donc allé et j'ai examiné les fichiers intéressants. J'ai eu du mal pendant 30 minutes, car je n'utilisais pas la commande ls -la pour afficher toutes les informations et les fichiers, notamment les fichiers cachés. Il y avait beaucoup de résultats, mais j'ai passé beaucoup de temps sur le dossier .hiddenadmindirectory, qui me semblait plus important. Dans ce dossier, j'ai trouvé une application en .exe et une note qui expliquait une chose peu intéressante.

```
django@bulldog:/home/bulldogadmin$ ls -la
ls -la
total 40
drwxr-xr-x 5 bulldogadmin bulldogadmin 4096 Sep 21 2017 .
drwxr-xr-x 4 root      root      4096 Aug 24 2017 ..
-rw-r--r-- 1 bulldogadmin bulldogadmin  220 Aug 24 2017 .bash_logout
-rw-r--r-- 1 bulldogadmin bulldogadmin 3771 Aug 24 2017 .bashrc
drwx------ 2 bulldogadmin bulldogadmin 4096 Aug 24 2017 .cache
drwxrwxr-x 2 bulldogadmin bulldogadmin 4096 Sep 21 2017 .hiddenadmindirectory
drwxrwxr-x 2 bulldogadmin bulldogadmin 4096 Aug 25 2017 .nano
-rw-r--r-- 1 bulldogadmin bulldogadmin  655 Aug 24 2017 .profile
-rw-rw-r-- 1 bulldogadmin bulldogadmin   66 Aug 25 2017 .selected_editor
-rw-r--r-- 1 bulldogadmin bulldogadmin    0 Aug 24 2017 .sudo_as_admin_successful
-rw-rw-r-- 1 bulldogadmin bulldogadmin  217 Aug 24 2017 .wget-hsts
django@bulldog:/home/bulldogadmin$
```

```
django@bulldog:/home/bulldogadmin/.hiddenadmindirectory$ ls
ls
customPermissionApp
note
django@bulldog:/home/bulldogadmin/.hiddenadmindirectory$
```



Je ne peux pas exécuter le fichier, donc j'ai utilisé la commande cat afin d'afficher son contenu.



Comme le fichier est en .exe, il fournit de nombreuses informations illisibles. J'ai donc utilisé la commande strings pour extraire toutes les chaînes de caractères du fichier en question.

Après une longue recherche difficile et pleine de casse-tête, j'ai

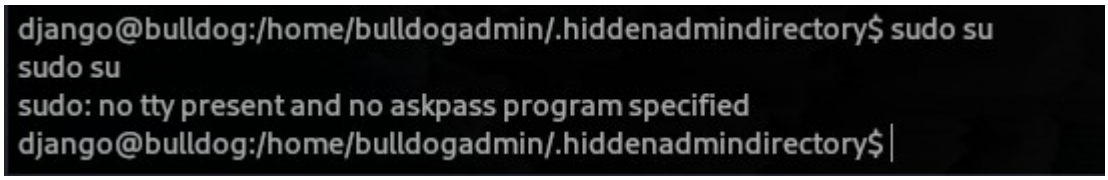
enfin trouvé un répertoire qui était sous mes yeux depuis tout ce temps.

J’ai recopier les caractère et cela ma donné un mot de passe (attention il y’a des choses en plus à supprimer telle que les certaine lettre qui n’ont rien à faire la)

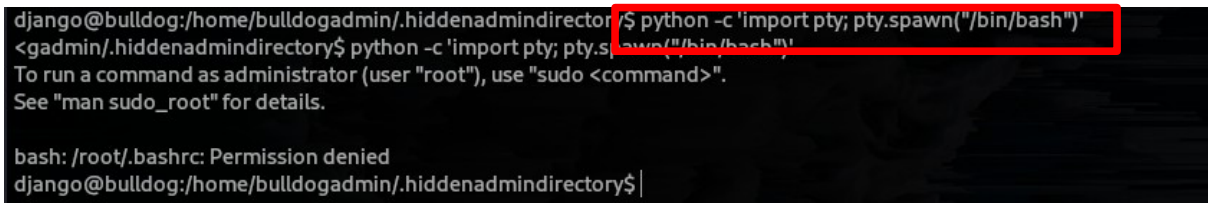
```
SUPERultHimatePASHSWORDyouHCANTget
```

J'ai essayé une commande pour changer d'utilisateur et me

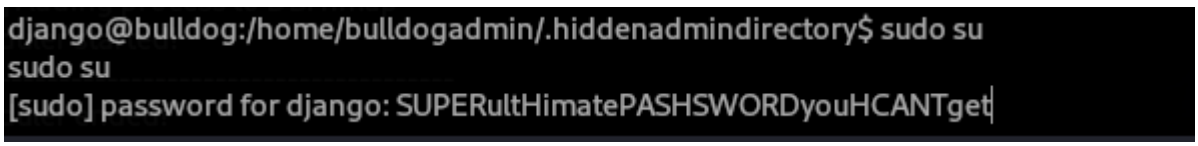
connecter en tant que root, mais il me manquait un TTY. Un **TTY** (teletypewriter) est un terminal virtuel qui permet à un utilisateur d'interagir avec le système. Il est nécessaire pour exécuter certaines commandes qui nécessitent une interface terminal active, comme celles qui changent d'utilisateur ou demandent une authentification.

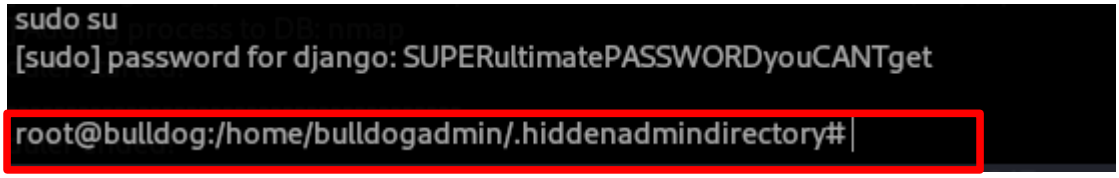


Pour avoir un tty j'ai donc utilisé la commande `python -c 'import pty; pty.spawn("/bin/bash")'` pour ouvrir un pseudo-terminal interactif. Le module `pty` permet de manipuler des terminaux virtuels, et la fonction `spawn` lance un shell `/bin/bash` dans ce terminal. Cela permet d'obtenir un shell interactif complet, utile notamment dans les reverse shells ou les environnements limités. Cette méthode améliore l'expérience d'interaction avec le système compromis.



Je peux enfin m'identifier avec django le root et via le mot de passe que l'on a retrouvé :





Je suis officiellement super utilisateur et j'ai un accès complet à la

machine. Je peux donc accéder au répertoire /root et afficher le message de félicitations. Mon CTF s'achève ici.