First basic CTF

Author: Raya Klein 2024

> CTF is in tryhackme rooms. username: `PTpaint`

High level process:

1. nmap the IP - found port 3000 & 22
2. Open in browser - http://192.168.100.223:3000/. There is a simple NodeJS app.
3. Find hint link hidden in developer tools
4. Login as admin using SQL injection
5. Upload any file - it will lead to a button that will show the file content
6. There is a File Inclusion Vulnerability - Can read the /etc/passwd file - see there is a user `james`
7. Search for `id_rsa` private key for james - found in his home directory
8. Login as `james` to ssh.
9. Check this user privileges - he can use `head` as sudo.
10. Use GTFobins to find a way to PrivEsc that. We can read /etc/shadow file - and therefore many other interesting files we did not have access to before.
11. We are able to read /etc/shadow and get the root hash
12. Crack the hash offline using hashcat and rockyou.txt list.
13. read /root/flag.txt file - we got the flag!

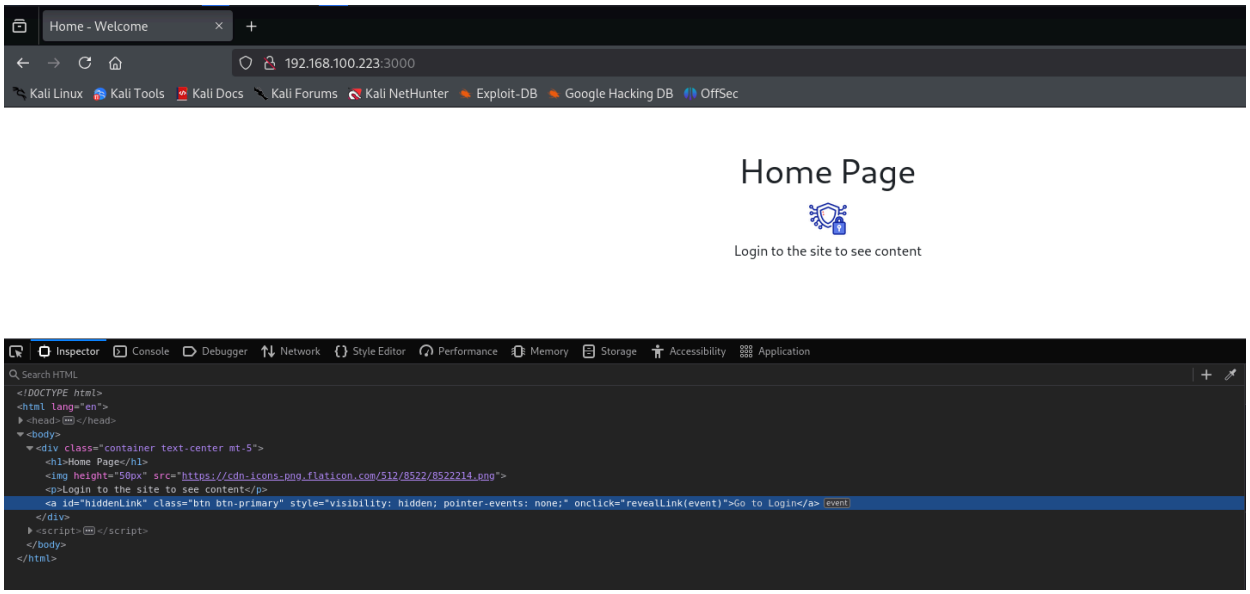
Walkthrough

1. Nmap: port 22 for ssh and port 3000 for web server are open.

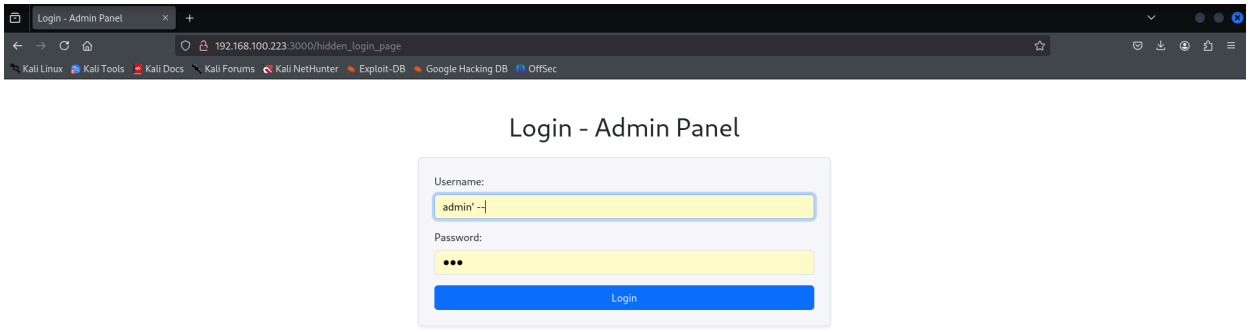
```
┌──(raya㉿kali)-[~/CTFs]
└─$ nmap 192.168.100.223 -sC -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-12 04:35 EST
Nmap scan report for 192.168.100.223
Host is up (0.0014s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 33:bd:1b:3e:d2:a2:19:fb:98:2b:89:be:90:f8:ee:ec (ECDSA)
|_  256 23:13:aa:e6:ef:51:ef:2f:85:8a:8d:67:80:8a:24:73 (ED25519)
3000/tcp open  http    Node.js (Express middleware)
|_http-title: Home - Welcome
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 21.21 seconds
```

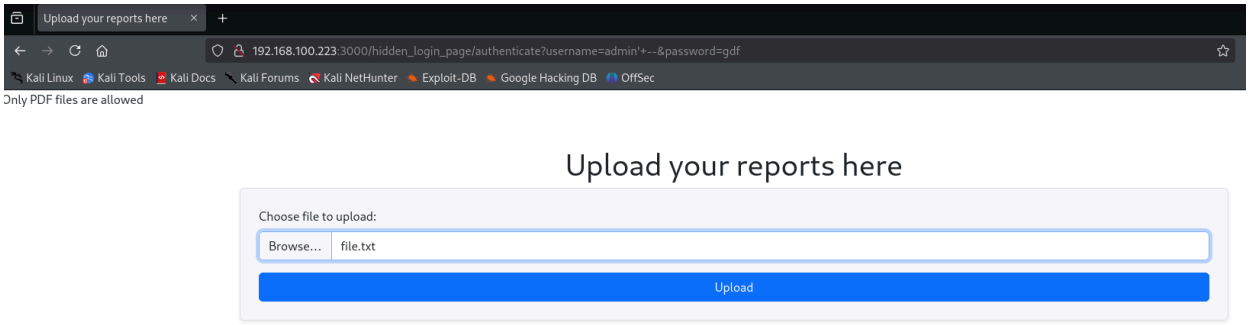
2. start with web - In dev tools - remove the style from `<a></a>` tag and we get the button. Click the button - will show in developer tools the route for login.



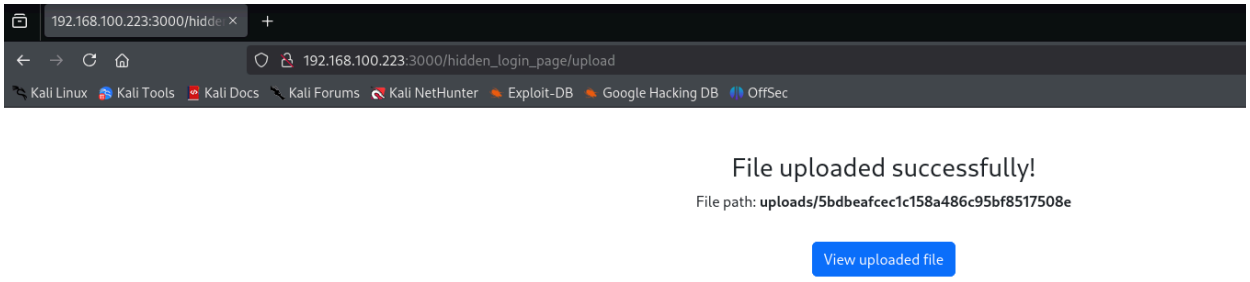
3. SQL inject the username to login as admin:



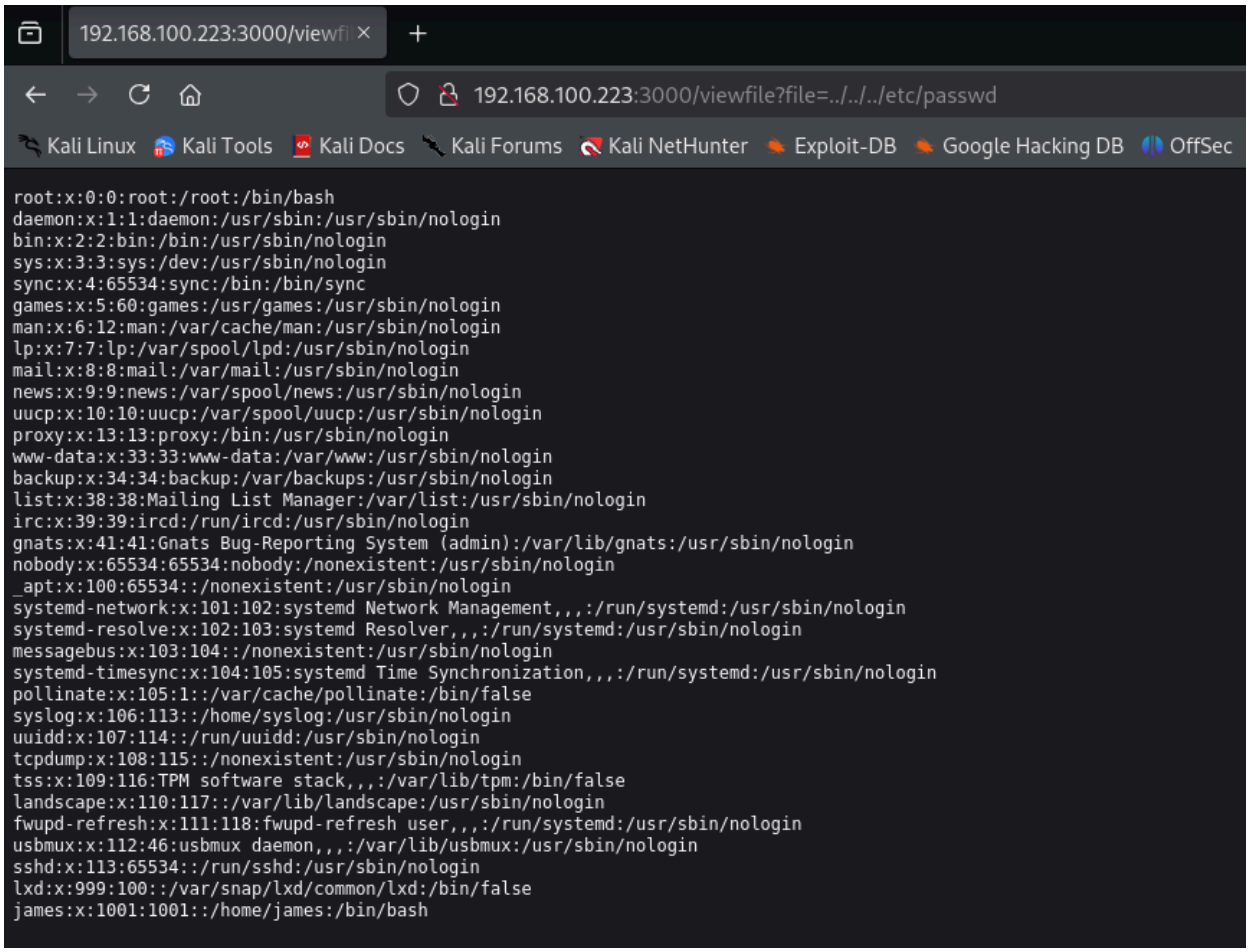
4. Now we can upload a file - any file..



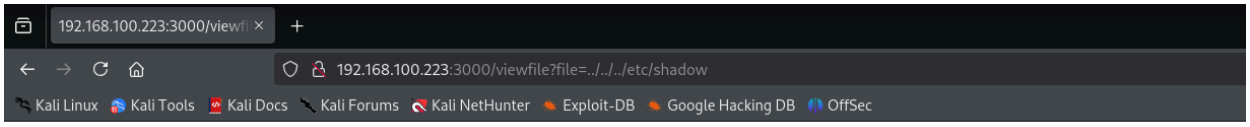
5. Follow the link to view uploaded file



6. There is a File Inclusion Vulnerability - Can read the /etc/passwd file - see there is a user `james`

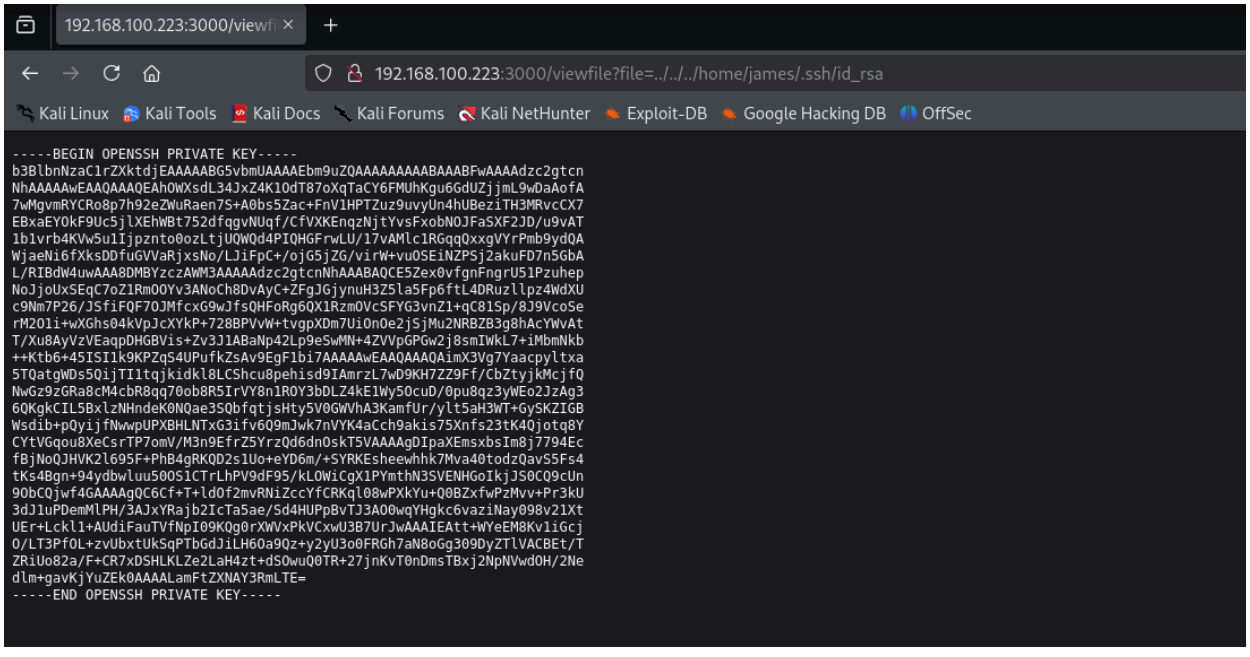


7. Trying to read /etc/shadow for example - gives an error



Access to /etc/shadow is forbidden.

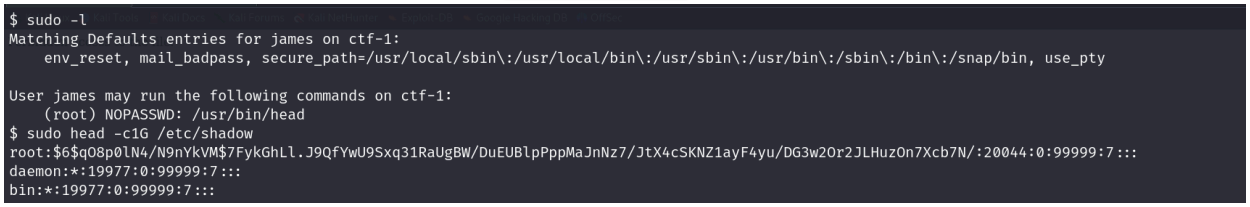
8. Read the `id_rsa` of `james`



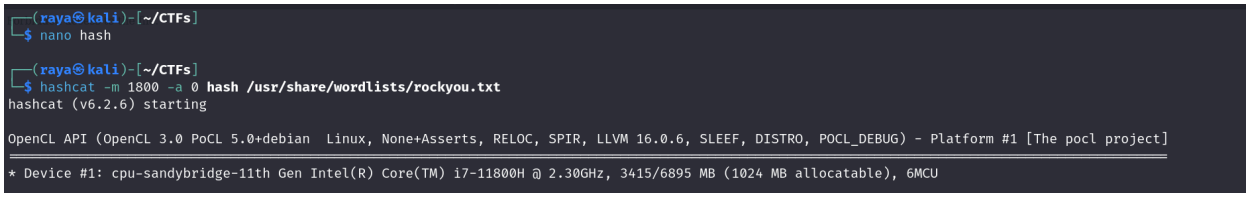
9. Save to a file and connect as james

```
nano id_rsa_james
...copy content
chmod 600 id_rsa_james
ssh -i id_rsa_james james@192.168.100.223
```

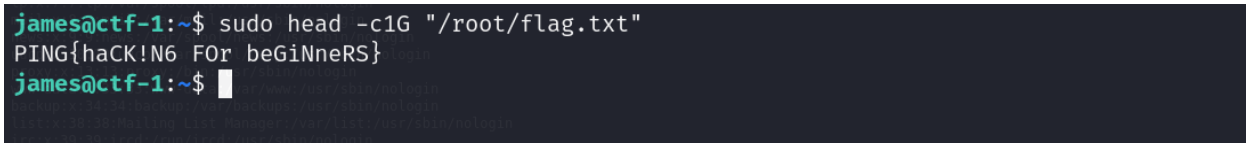
11. Search for special privileges the user has: he can run the command `head` as root - that allows us to read the important file `/etc/shadow` and get the hash for the root user



12. Crack the hash offline using hashcat and the rockyou.txt wordlist, and then login with the root password.



13. Read the flag.txt file in the root folder - can read it with james's privilege or as root -



Goodluck!!!