Day 18 - The Bits of Christmas

Scenario

(DOTNET Microsoft., 2020)

Day 18: The Bits of Christmas - Story:

"Silly Santa...Forgetting his password yet again!" complains Elf McEager. However, it is in fact Elf McEager who is silly for not creating a way to reset Santa's password for the TBFC dashboard.

Santa needs to get back into the dashboard for Christmas! Can you help Elf McEager reverse engineer TBFC's application to retrieve the password for Santa?!

18.3. Challenge:

Deploy the instance attached to this task and log in using the Remote Desktop Protocol (RDP). Open the application "TBFC_APP.exe" on the Desktop and enter the correct password!

You can use "Remmina" on the TryHackMe AttackBox to connect to the instance with the following credentials, or any RDP client such as Microsofts if you wish to connect to the TryHackMe VPN:

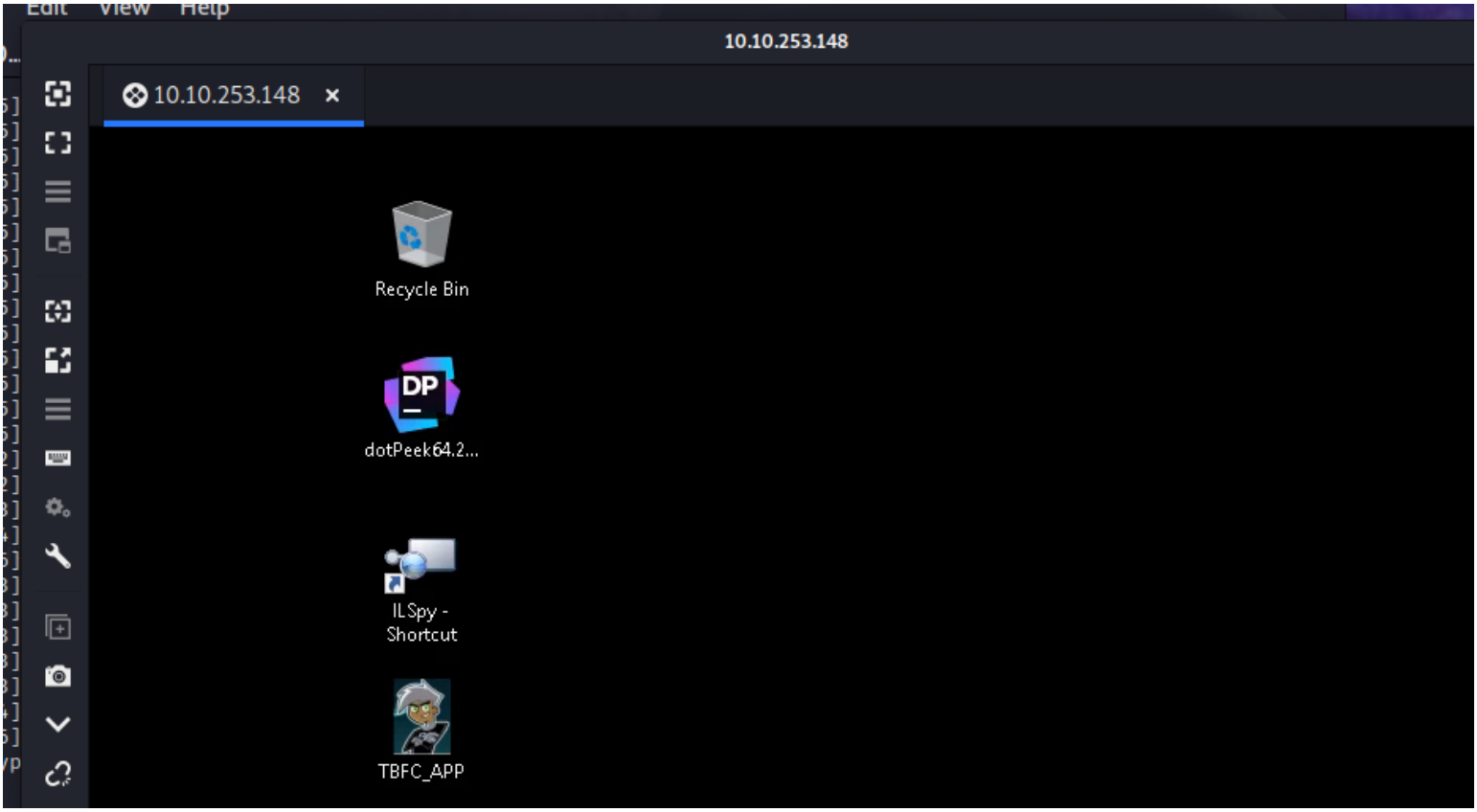
IP Address: `10.10.253.148`

Username: cmnatic

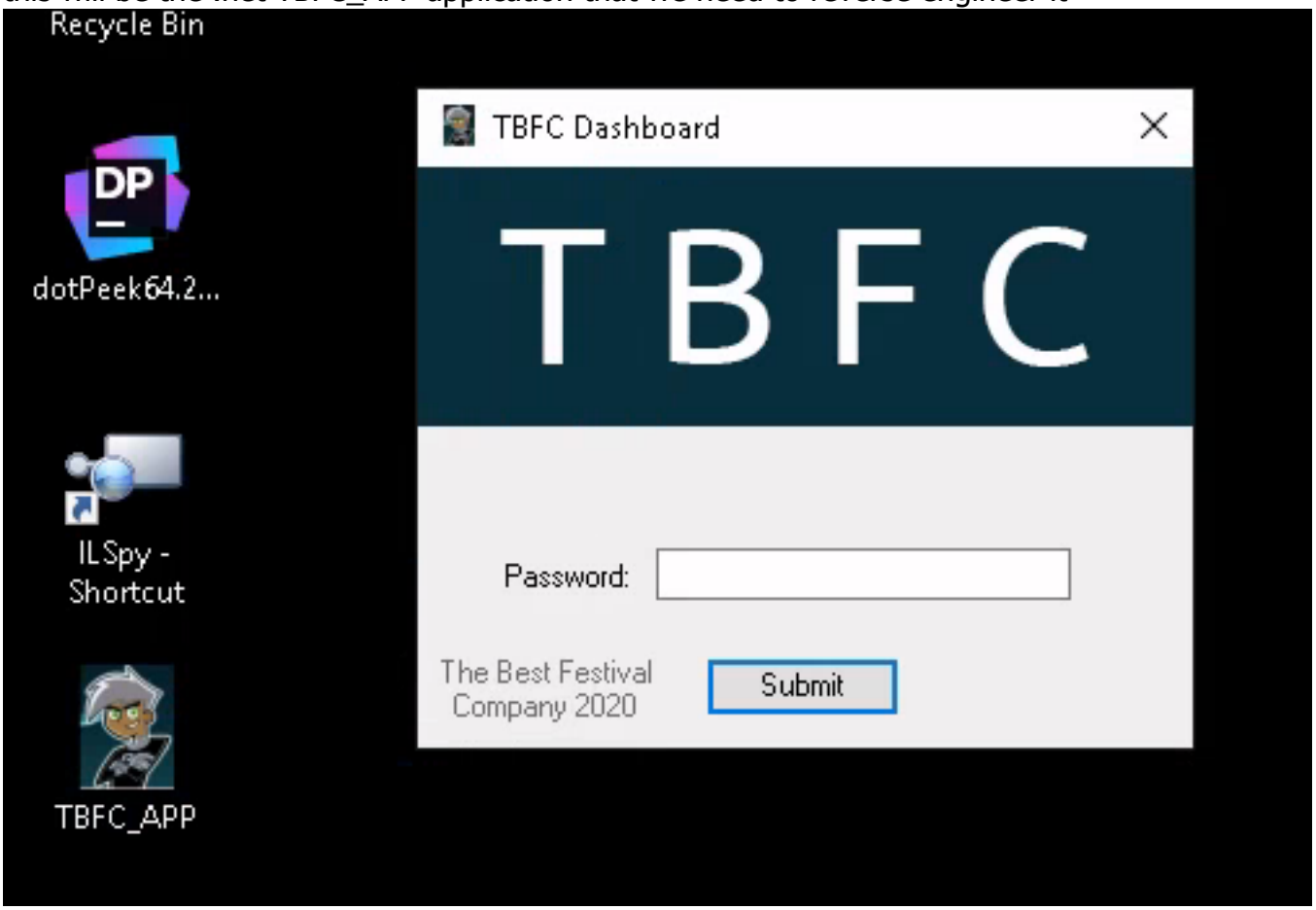
Password: Adventofcyber!

so today's challenge will be reversing .net program

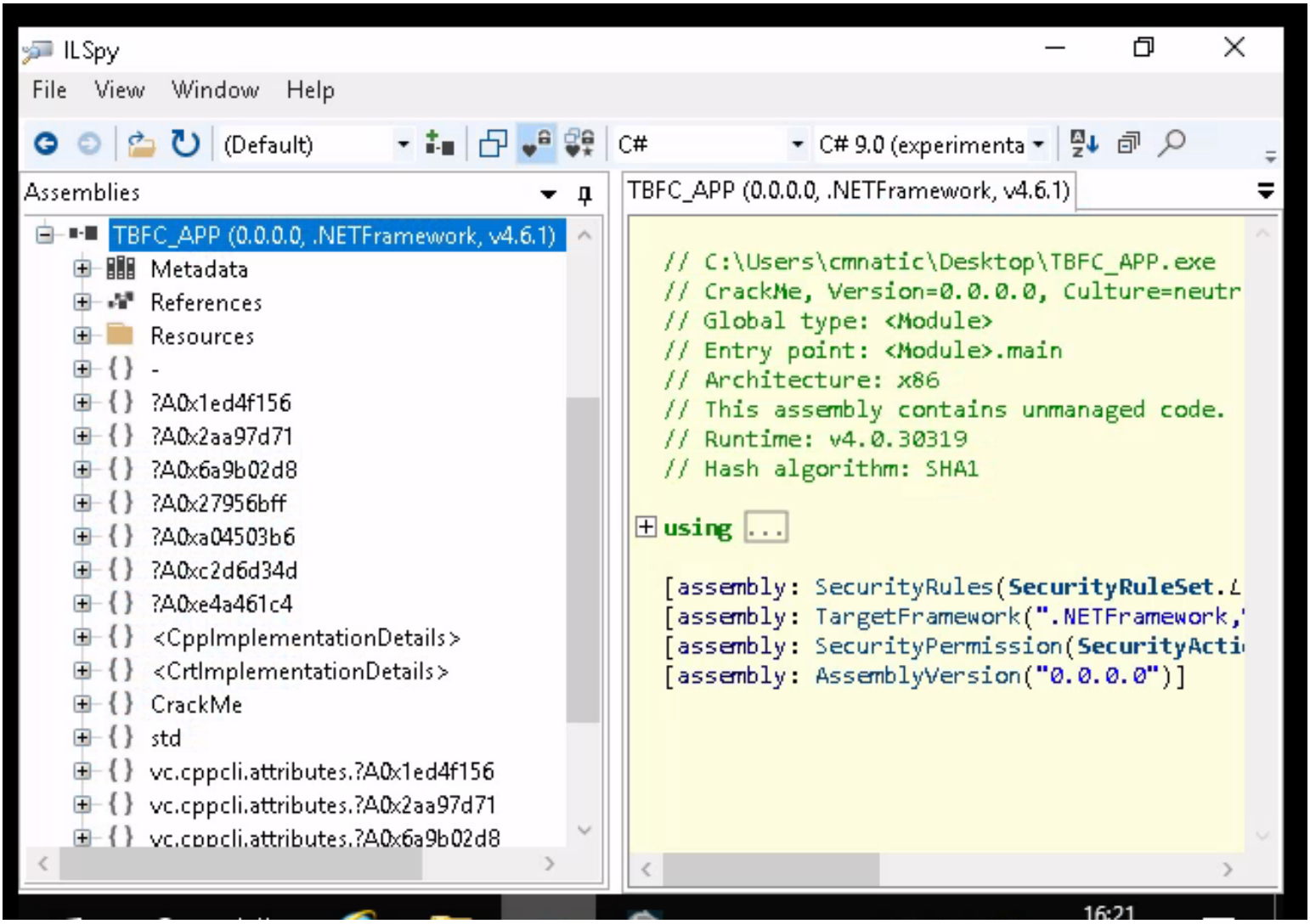
let's logon into the RDP using the credential provided using remmina



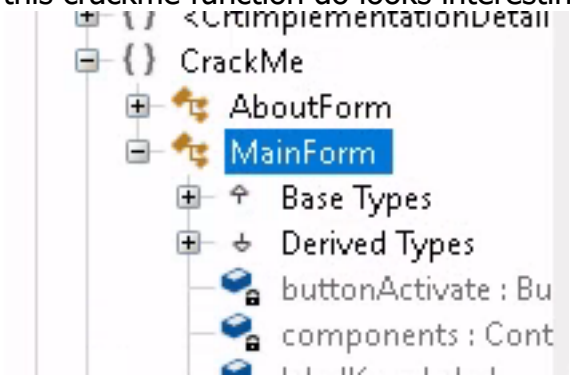
this will be the .net TBFC_APP application that we need to reverse engineer it



use ILSpy to decompile the application



this crackme function do looks interesting here



this buttonActivate_click seems to be the function to the Submit button

```
private unsafe void buttonActivate_Click(obje
{
    IntPtr value = Marshal.StringToHGlobalAns
    sbyte* ptr = (sbyte*)System.Runtime.Compi
    void* ptr2 = (void*)value;
    byte b = *(byte*)ptr2;
    byte b2 = 115;
    if ((uint)b >= 115u)
    {
        while ((uint)b <= (uint)b2)
        {
            if (b != 0)
            {
                ptr2 = (byte*)ptr2 + 1;
                ptr++;
                b = *(byte*)ptr2;
                b2 = (byte)(*ptr);
                if ((uint)b < (uint)b2)
                {
```

if we check this ptr sbyte pointer we'll notice there's a ref for it

```
sbyte* ptr = (sbyte*
```

reference is "santapassword321"? seems like the password for santa here

```
.Unsafe.AsPointer(ref <Module>.??_C@_0BB@IKKDFEPG@santapassword321@);
```

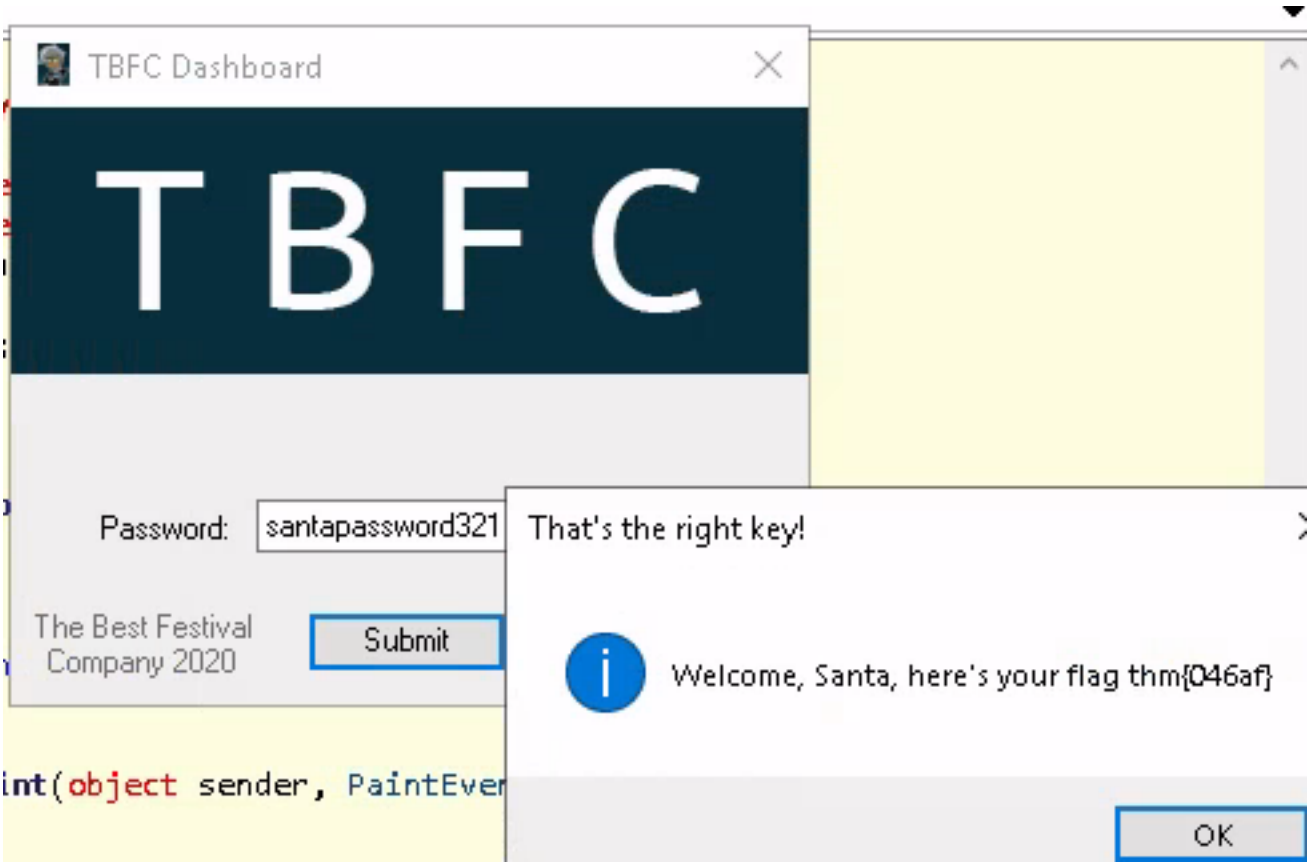
if the password is correct we'll retrieve the message box prompt the flag

```
    continue;
}
MessageBox.Show("Welcome, Santa, here's your flag thm{046af}", "That's the right
return;
```

or else we'll get the message we're not santa!

```
Box.Show("Uh Oh! That's the wrong key", "You're not Santa!", Message
```

let's try out the password that we found see is that the real password for it? & yes it's the correct password & we retrieved our flag!


TBFC Dashboard
TBFC
Password:
santapassword321
The Best Festival Company 2020
Submit
That's the right key!
Welcome, Santa, here's your flag thm{046af}
OK