NeverLAN CTF

Forensics : Open Backpack

Value : 100 pts

Difficulty : Unknown

Description : We've forgotten the password to our payroll machine. Can you extract it ?

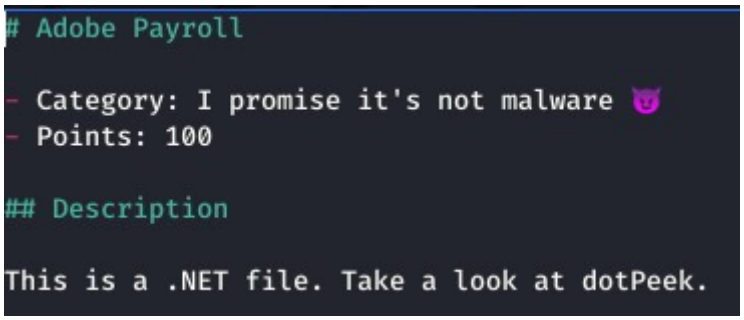
Your flag will be in the normal flag{flagGoesHere} syntax.

Attachment : Adobe_Payroll.7z

Solution :

First let's download the attachment file «Adobe_Payroll.7z» and extract his content.

Once extracted we got a file called «description.md» and our challenge «Adobe_Employee_Payroll.exe». The description file give us a hint.

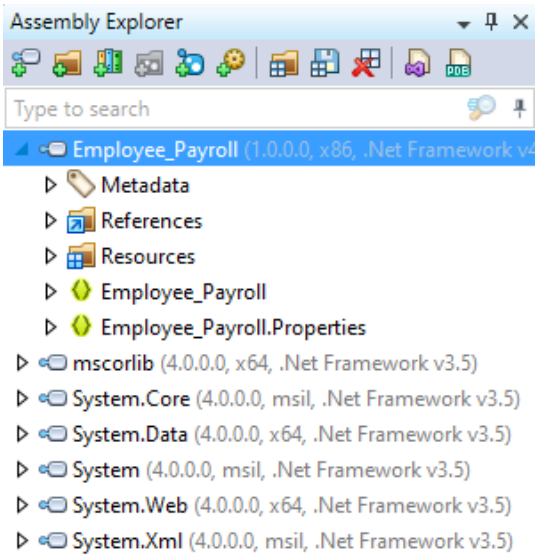


Let's go inside a Windows OS and download the tool «dotPeek».

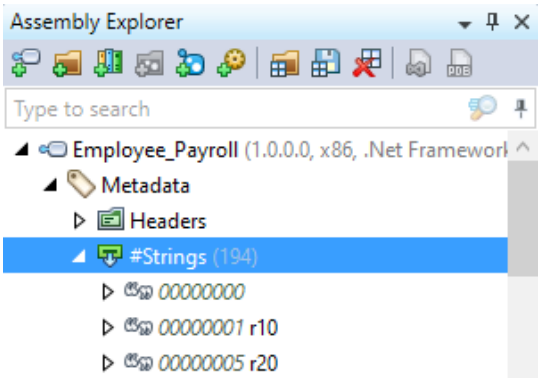
Source : https://www.jetbrains.com/decompiler/download/download-thanks.html?platform=windowsWeb

Once the tool downloaded and installed open it and load our «Adobe_Employee_Payroll.exe» file in it. «File > Open > Adobe_Employee_Payroll.exe»

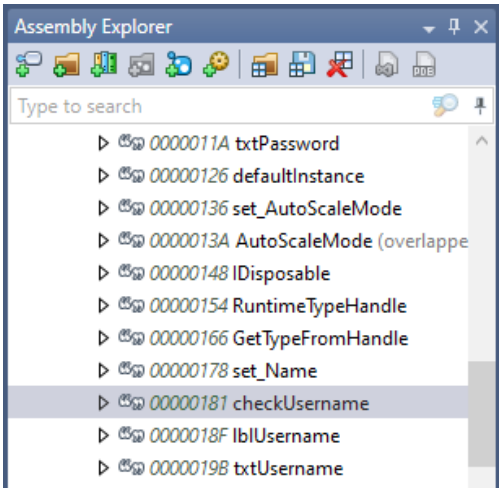
Then we can see into the «Assembly Explorer» our «exe» decompiled.



Browsing inside «Metadata», we can see the category «Strings» it seem interesting.



Browsing inside the «Strings» content, and we see a function called «checkUsername».

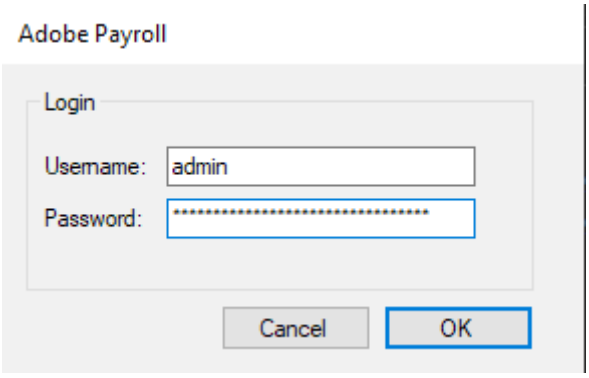


Double click on it for open the data. Then at the right of the Assembly Explorer we can see the script containing our function where we can see the username and the password !

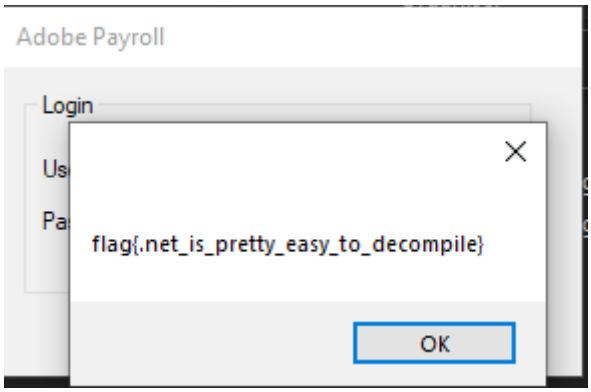
```
private bool checkUsername()
{
  return this.txtUsername.Text == "admin";
}

private bool checkPassword()
{
  return this.txtPassword.Text == "bmV2ZXJfZ29ubmFfZ2l2ZV95b3VfdXAh";
}
```

Username : admin
Password : bmV2ZXJfZ29ubmFfZ2l2ZV95b3VfdXAh

As we now get the credentials, open the executable «Adobe_Employee_Payroll.exe» and enter the credentials.



Then press «OK» and we get the flag.



Flag : flag{.net_is_pretty_easy_to_decompile}