.NET Application Hacking

/LennyPenny/.nethacking

Gliederung

Was?

Motivation

Vorgehen

Tools

Demos!

Was?

1. Quellcode einsehen
2. verstehen
3. verändern

Warum?

Risk management

Neugier

Spaß

Wie?

Dekompilation

programm.exe/dll → IL asm → (fast) C# Quellcode

```
IL_0000: nop
IL_0001: ldarg.0
IL_0002: callvirt instance class [System.Windows.Forms]Sys
IL_0007: callvirt instance string [System.Windows.Forms]Sy
IL_000c: ldarg.0
IL_000d: ldarg.0
IL_000e: callvirt instance class [System.Windows.Forms]Sys
IL_0013: callvirt instance string [System.Windows.Forms]Sy
IL_0018: ldstr "wtMd3x6ucb16w9P9BBPj5qoHKPCq0MIy"
IL_001d: call instance string CrackMe.Form1::enc(string, s
IL_0022: ldc.i4.0
```

```
private void Button1_Click(object sender, EventArgs e)
{
    bool flag = Operators.CompareString(this.TextBox2.Text, this.er
    if (flag)
    {
        Interaction.MsgBox("Yup, you did it! Go write a KeyGen!", M
    }
    else
    {
        Interaction.MsgBox("Sorry, try again!", MsgBoxStyle.OkOnly,
    }
}
```

Modifikation

besserer C# Quellcode

```
private void Button1_Click(object sender, EventArgs e)
{
    bool flag = Operators.CompareString(this.TextBox2.Text, this.
    if (true)
    {
        Interaction.MsgBox("Yup, you did it! Go write a KeyGen!",
    }
    else
    {
        Interaction.MsgBox("Sorry, try again!", MsgBoxStyle.OkOnl
    }
}
```

Demo

/LennyPenny/.nethacking