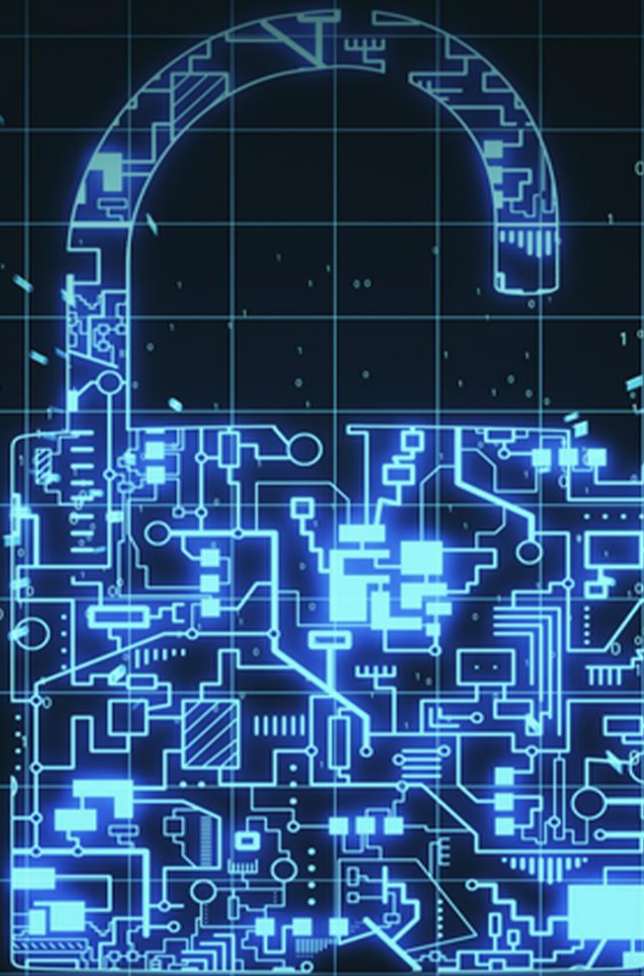


Credential Dumping



Windows Autologon

Contents

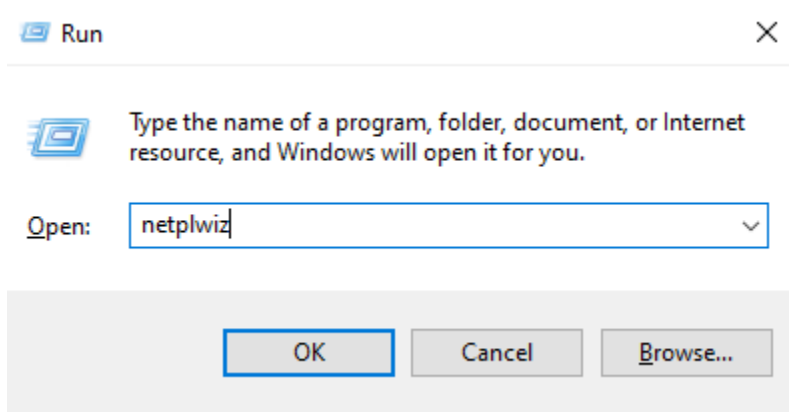
Introduction	3
Method 1: Nirsoft-Network Password Recovery	5
Method 2: DecryptAutologon.exe	6

Introduction

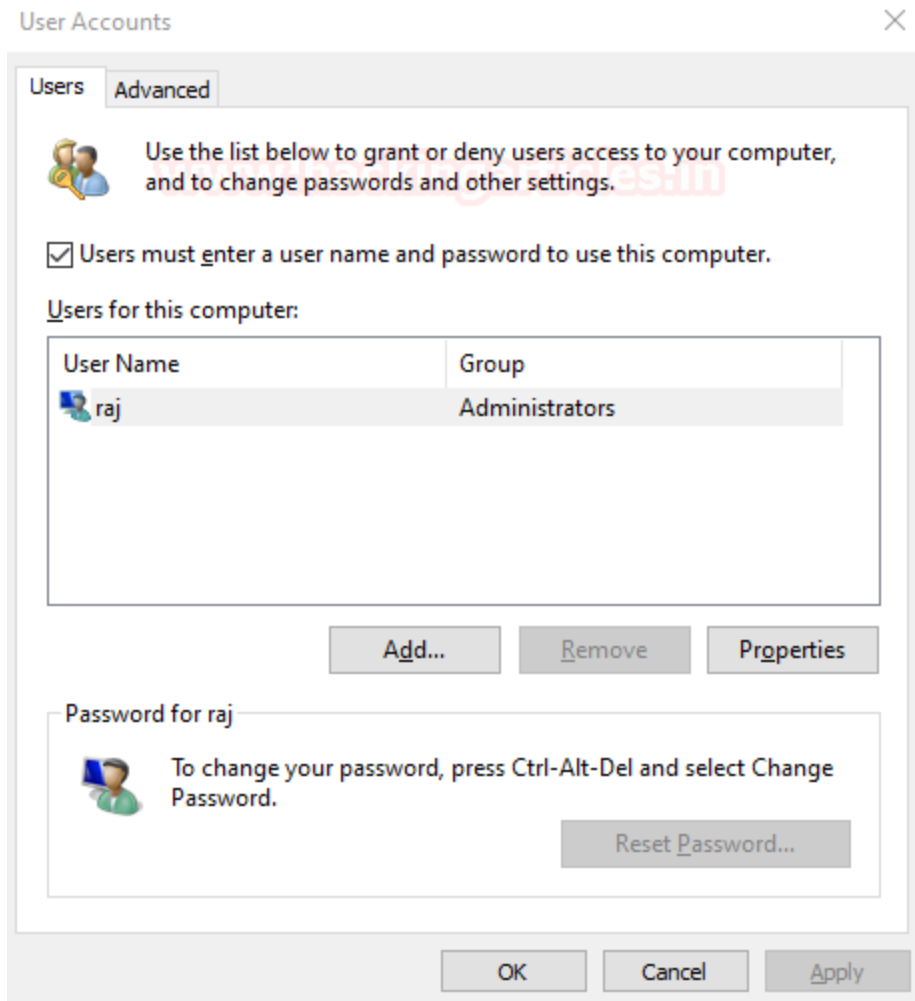
Autologon helps you to conveniently customise the built-in Autologon mechanism for Windows. Rather than waiting for a user to enter their name and password, Windows will automatically log in to the required user using the credentials you submit with Autologon, which are encrypted in the registry.

We'll try to dump the stored autologin credentials using two different tools.

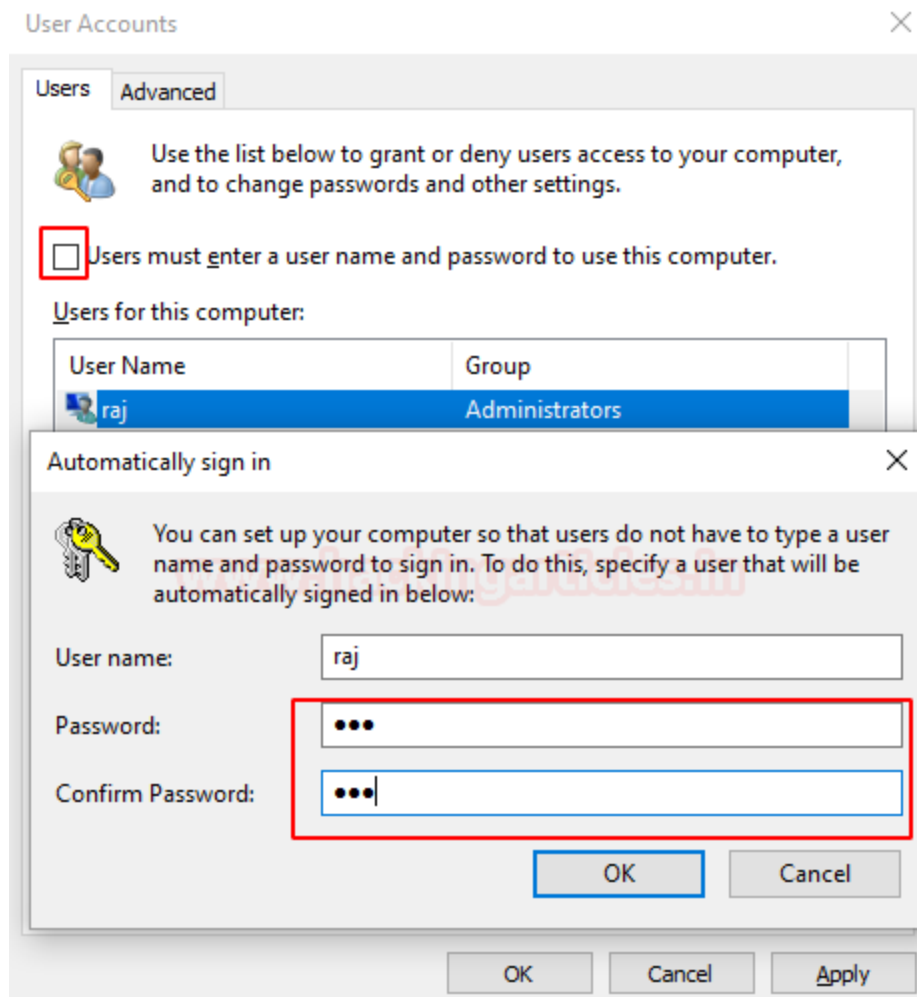
Let's see the settings for autologin. First, you need to access the User Accounts Control Panel using the **netplwiz** command inside the run prompt.



Choose the account for autologon, for example, we have selected user Raj.



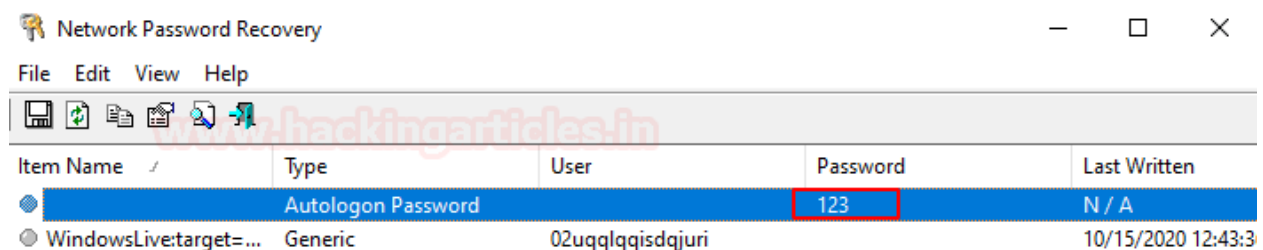
Enter your password once and then a second time to confirm it and uncheck the box Users must enter a user name and password to use this computer, **then click OK.**



Method 1: Nirsoft-Network Password Recovery

Network Password Recovery is very easy to use, install and run the tool on the local machine whose password you chose to extract. It will dump the stored credential for the autologon account.

You can download this tool from [here](#)



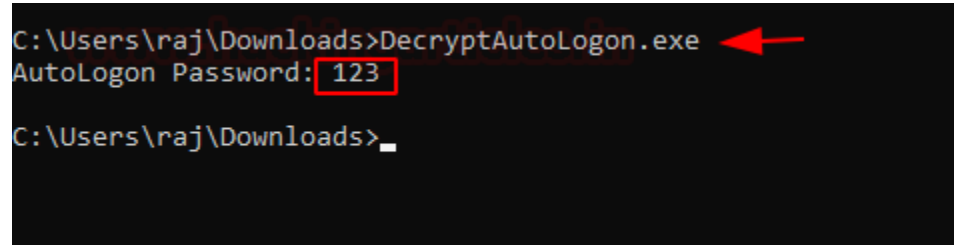
Method 2: DecryptAutoLogon.exe

This tool can extract/decrypt the password that was stored in the LSA by SysInternals AutoLogo.

You can download its Compiled Version [HERE](#)

Run the downloaded .exe as shown in the given image, it will dump the password in the Plain text.

DecryptAutoLogon.exe



```
C:\Users\raj\Downloads>DecryptAutoLogon.exe
AutoLogon Password: 123
C:\Users\raj\Downloads>
```

JOIN OUR TRAINING PROGRAMS

