

```
C:\Windows\system32\cmd.exe
cmd~pwd
'pwd' is not recognized as an internal or external command,
operable program or batch file.
cmd~dir
Volume in drive C has no label.
Volume Serial Number is 6AE1-984D

Directory of C:\Users\loiliangyang\Desktop

05/05/2023  06:44 AM    <DIR>          .
05/05/2023  06:44 AM    <DIR>          ..
05/05/2023  06:44 AM                47 hackerloi.bat
05/01/2023  06:02 AM            446,990 powershell.exe
04/15/2023  12:09 AM            11,834 Untitled1.ps1
               3 File(s)            458,871 bytes
               2 Dir(s)  16,985,686,016 bytes free

cmd~
```

```
C:\Windows\system32\cmd.exe
cmd~whoami
desktop-9972nie\loiliangyang
cmd~net user loiliangyang
User name                loiliangyang
Full Name
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          Never

Password last set        2/17/2020 5:03:45 AM
Password expires         Never
Password changeable      2/17/2020 5:03:45 AM
Password required        Yes
User may change password  Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               5/5/2023 6:25:14 AM

Logon hours allowed      All

Local Group Memberships  *Administrators      *Remote Desktop Users
Global Group memberships *None
The command completed successfully.
```

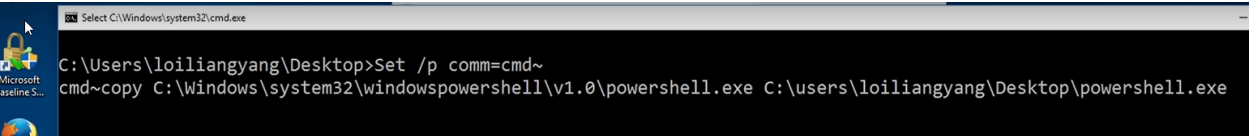
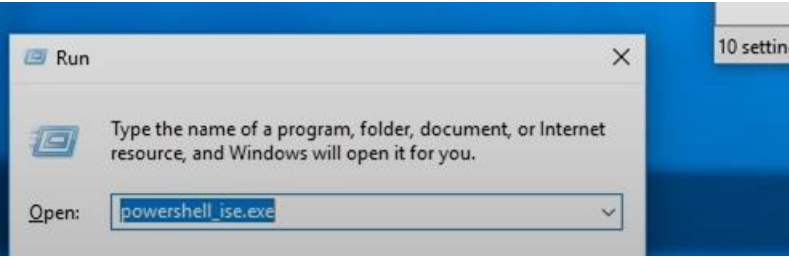
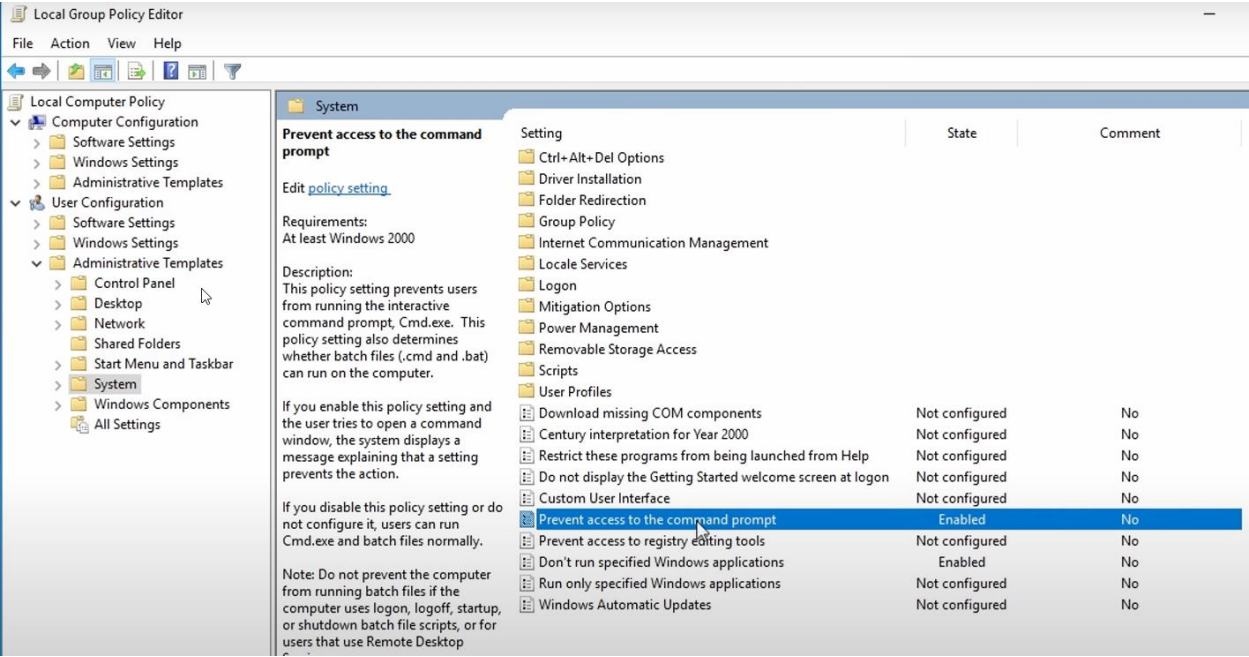
Access FTP from Start

```
C:\Windows\System32\ftp.exe
ftp> !dir_

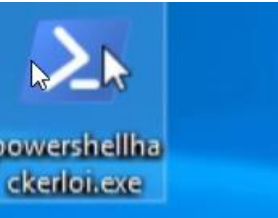
ftp> !net user

User accounts for \\DESKTOP-9972NIE

-----
Administrator          DefaultAccount        defaultuser0
Guest                   loiliangyang          scriptkiddieloi
The command completed successfully.
```



If it does not work change name of the file



Local Group Policy Editor

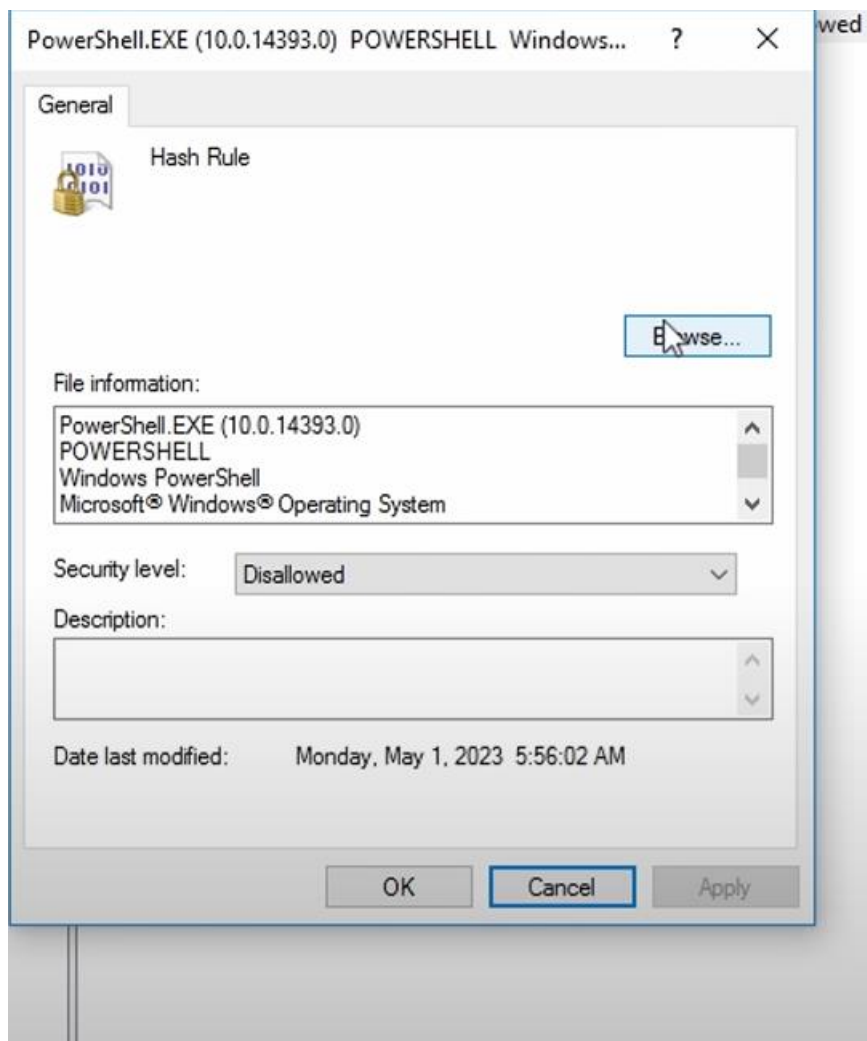
File Action View Help

Local Computer Policy

- Computer Configuration
 - Software Settings
 - Windows Settings
 - Name Resolution Policy
 - Scripts (Startup/Shutdown)
 - Deployed Printers
 - Security Settings
 - Account Policies
 - Local Policies
 - Windows Firewall with Advanced Security
 - Network List Manager Policies
 - Public Key Policies
 - Software Restriction Policies
 - Security Levels
 - Additional Rules
 - Application Control Policies
 - IP Security Policies on Local Computer
 - Advanced Audit Policy Configuration
 - Policy-based QoS
 - Administrative Templates
 - User Configuration
 - Software Settings
 - Windows Settings
 - Administrative Templates
 - Control Panel
 - Desktop
 - Network
 - Shared Folders
 - Start Menu and Taskbar
 - System
 - Windows Components
 - All Settings

Name
%HKI
%HKI
Power

Name	Type	Security Level	Description	Last Modifi
%HKEY_LOCAL_MACHINE\SOFTWARE\...	Path	Unrestricted		5/1/2023 5
%HKEY_LOCAL_MACHINE\SOFTWARE\...	Path	Unrestricted		5/1/2023 5
Powershell.EXE (10.0.14393.0) POWERSH...	Hash	Disallowed		5/1/2023 5



Browse It

You can target on following executes

```
C:\Users\loiliangyang\Desktop>Set /p comm=cmd~  
cmd~copy C:\Windows\system32\windowpowershell\v1.0\powershell.exe C:\Users\loiliangyang\Desktop\powershell.exe
```

Finally if we copy it passes

If any errors try this

```
C:\Users\loiliangyang\Desktop>Set /p comm=cmd~  
cmd~echo >>C:\Users\loiliangyang\Desktop\powershell.exe
```

And enter into BYPASS

