Application Escape and Breakout

Summary

Gaining a command shell

- **Shortcut**
    - [Window] + [R] -> cmd
    - [CTRL] + [SHIFT] + [ESC] -> Task Manager
    - [CTRL] + [ALT] + [DELETE] -> Task Manager
- **Access through file browser**: Browsing to the folder containing the binary (i.e. `C:\windows\system32\`), we can simply right click and `open` it
- **Drag-and-drop**: dragging and dropping any file onto the cmd.exe
- **Hyperlink**: `file:///c:/Windows/System32/cmd.exe`
- **Task Manager**: `File` > `New Task (Run...)` > `cmd`
- **MSPAINT.exe**
    - Open MSPaint.exe and set the canvas size to: Width=6 and Height=1 pixels
    - Zoom in to make the following tasks easier
    - Using the colour picker, set pixels values to (from left to right):
        - 1st: R: 10, G: 0, B: 0
        - 2nd: R: 13, G: 10, B: 13
        - 3rd: R: 100, G: 109, B: 99
        - 4th: R: 120, G: 101, B: 46
        - 5th: R: 0, G: 0, B: 101
        - 6th: R: 0, G: 0, B: 0
    - Save it as 24-bit Bitmap (.*bmp;*.dib)
    - Change its extension from bmp to bat and run

Sticky Keys

- Spawn the sticky keys dialog

    - Via Shell URI : `shell:::{20D04FE0-3AEA-1069-A2D8-08002B30309D}`
    - Hit 5 times [SHIFT]
- Visit "Ease of Access Center"
- You land on "Setup Sticky Keys", move up a level on "Ease of Access Center"
- Start the OSK (On-Screen-Keyboard)
- You can now use the keyboard shortcut (CTRL+N)

Dialog Boxes

Creating new files

- Batch files – Right click > New > Text File > rename to .BAT (or .CMD) > edit > open
- Shortcuts – Right click > New > Shortcut > `%WINDIR%\system32`

Open a new Windows Explorer instance

- Right click any folder > select `Open in new window`

Exploring Context Menus

- Right click any file/folder and explore context menus
- Clicking `Properties`, especially on shortcuts, can yield further access via `Open File Location`

Save as

- "Save as" / "Open as" option
- "Print" feature – selecting "print to file" option (XPS/PDF/etc)
- `\\127.0.0.1\c$\Windows\System32\` and execute `cmd.exe`

Input Boxes

Many input boxes accept file paths; try all inputs with UNC paths such as `//attacker–pc/` or `//127.0.0.1/c$` or `C:\`

Bypass file restrictions

Enter . or *.exe or similar in `File name` box

Internet Explorer

Download and Run/Open

- Text files -> opened by Notepad

Menus

- The address bar
- Search menus
- Help menus
- Print menus
- All other menus that provide dialog boxes

Accessing filesystem

Enter these paths in the address bar:

- file://C:/windows

- C:/windows/
- %HOMEDRIVE%
- \127.0.0.1\c$\Windows\System32

Unassociated Protocols

It is possible to escape a browser based kiosk with other protocols than usual `http` or `https`. If you have access to the address bar, you can use any known protocol (`irc`, `ftp`, `telnet`, `mailto`, etc.) to trigger the *open with* prompt and select a program installed on the host. The program will than be launched with the uri as a parameter, you need to select a program that will not crash when recieving it. It is possible to send multiple parameters to the program by adding spaces in your uri.

Note: This technique required that the protocol used is not already associated with a program.

Example - Launching Firefox with a custom profile:

This is a nice trick since Firefox launched with the custom profile may not be as much hardened as the default profile.

0. Firefox need to be installed.
1. Enter the following uri in the address bar: `irc://127.0.0.1 -P "Test"`
2. Press enter to navigate to the uri.
3. Select the firefox program.
4. Firefox will be launched with the profile `Test`.

In this example, it's the equivalent of running the following command:

```
firefox irc://127.0.0.1 -P "Test"
```

Shell URI Handlers

- shell:DocumentsLibrary
- shell:Librariesshell:UserProfiles
- shell:Personal
- shell:SearchHomeFolder
- shell:System shell:NetworkPlacesFolder
- shell:SendTo
- shell:Common Administrative Tools
- shell:MyComputerFolder
- shell:InternetFolder

References

- PentestPartners - Breaking out of Citrix and other restricted desktop environments
- Breaking Out! of Applications Deployed via Terminal Services, Citrix, and Kiosks - Scott Sutherland - May 22nd, 2013
- Escaping from KIOSKs - HackTricks