PowerShell Empire with Macro, Character Map, and Key-logger

This is another lab for client-side attack. We are using PowerShell Empire to generate a **`vbscript`**, hide it in a *Microsoft PowerPoint* file, and deliver it to the user. **Keep in mind that many of these instructions assume you have:**

1. **Completed** the previous two projects.
2. **Remember** how to carry out those projects' tasks – including, but not limited to:
   a. Setting up your http listener
   b. Setting up a stager
   c. Generating a payload file, at first in your **`/tmp`** directory
   d. Using **apache** to make said file accessible to your Win7 VM
3. Know how to **apply** that experience when asked to complete *similar* tasks during:
   a. This lab exercise
   b. Subsequent ones, as well

When you see the words **Take a screenshot…** in reference to some output or result, do that as well as copying the corresponding text from your CLI utility, be it *Kali* **or** *Win7*.

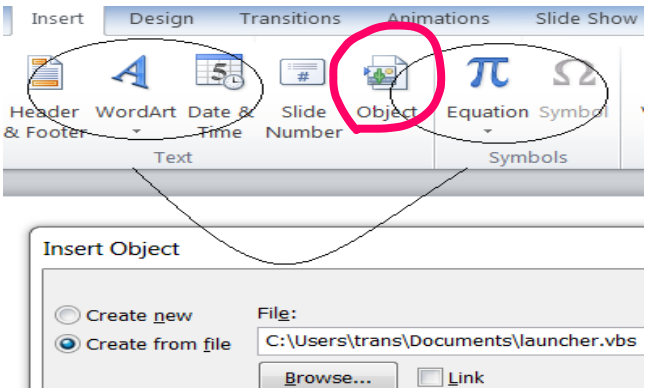
1. **Pre-requisite:**
   a. Your Kali may need an Internet connection for additional files. Make sure your VM has set the networking to **NAT**.
   b. A Win7 workstation will as a victim in the attack. This VM should be
      i. Set to **NAT**
      ii. Able to *ping* the Kali Linux.
2. *Exercise – **client-side** attack using **`vbs`** **file***
   a. On your Kali, use the same procedure you learned in the previous lab/project to set up a *listener*
   b. Type **`usestager`** and use **`windows/launcher_vbs`**
   c. Generate the **`vbs`** payload (at **`/tmp/launcher.vbs`** path) and use the **`unix2dos`** utility to convert line endings to Windows-style
   d. Copy it to your Win7 VM. Remember how we did this:
      i. Start up **apache** utility on Kali.
      ii. Copy generated file from **`/tmp`** to **`/var/www/html`** directory

iii. On Win7, navigate to **`http://YOUR_KALI_IP/launcher.vbs`** from ***IE***. It may appear as a simple webpage – in which case, choose to **Save As** text, but be sure to change the *extension*, with **`launcher.vbs`** as the file name.

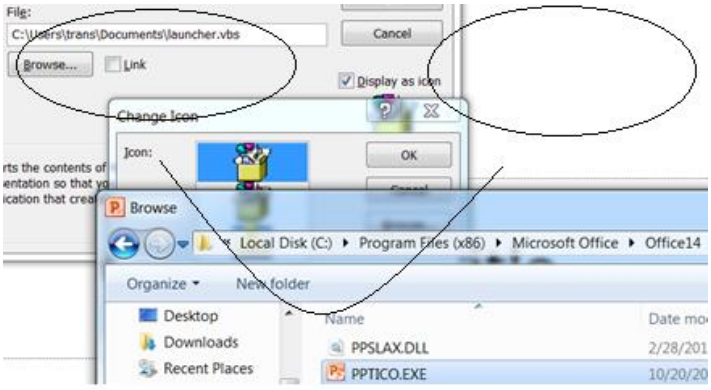
e. Using *PowerPoint* to hide the script

i. In your Win7 VM, launch *Microsoft PowerPoint*, go to Insert, and then Object.

ii. Select Create from file and browse to the **`launcher.vbs`** file



iii. Click on *Display as an icon*, and *Change icon*, and then browse to **`C:\Program Files\Microsoft Office\Office14`** folder, make sure **`.exe`** are visible, and select the **`PPTICO.exe`** file. **Take a screenshot of it**



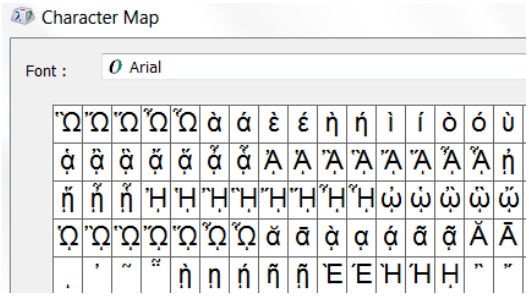
iv. **OK** to both the *Change Icon* and *Insert Object* dialogs.

v. It will look like another *PowerPoint* file on the slide. Save it for future use as an attack file....

f. Using *Character Map*, a built-in feature of your Win7 VM to change the file extension

i. From the Start menu, search for Character Map, and open the program

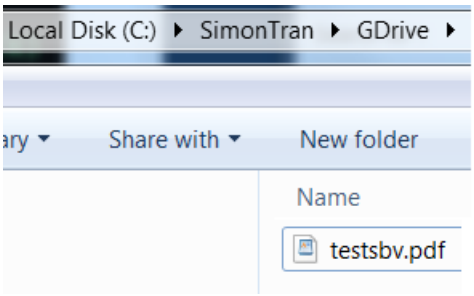
ii. You will see a dialog like the following:



iii. Open the *Advanced* view, and Go to Unicode: **202E**, which is the Right-To-Left Override

iv. Click the buttons: Select, then Copy

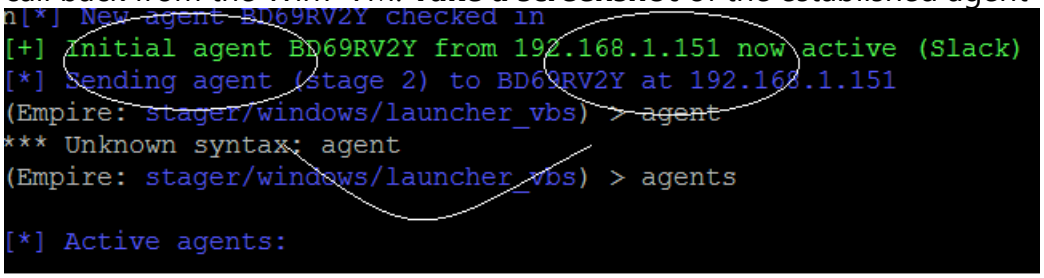
v. Go to your Windows Explorer, click on your **vbs** script to attempt to change the name. Before the dot (**.**) of the extension, type in **fdp**. Go to the beginning of the letter **f** in **fdp**, then click **Control+V**. You should see the extension changed. **Take a screenshot of the file after you change the extension** as follows:



Keeping in mind, of course, that your file name may look different...

g. Now, go back to your PowerPoint, and use it for the attack. Double click on the Object inside your PowerPoint, and when prompted, accept the warning. **Take a screenshot** for the popup that users may ignore and click Yes.

h. Go back to your Kali *PowerShell Empire listener*, and wait for the connection to call back from the Win7 VM. **Take a screenshot** of the established agent



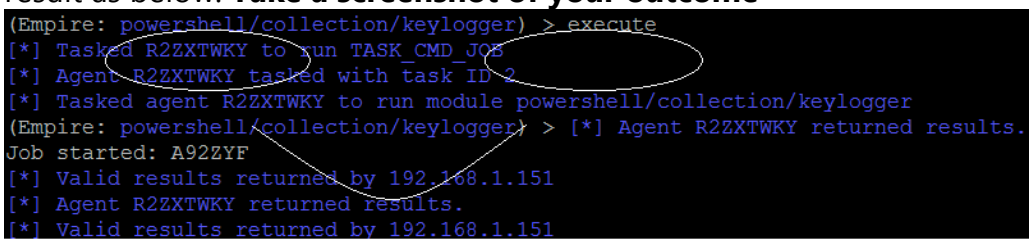
i. Interact with your new agent, using **`bypassuac http`** to gain admin privilege. **Take a screenshot of our outcome with the `*`** (the escalation point)

j. When you are inside the interactive session, type **`usemodule c`**, and then tab twice to find all available modules starting with that letter.

k. You will find a *keylogger* in the *collection* list (not the **USB** one)

l. Type **`usemodule FULL_PATH_TO_KEYLOGGER`**

m. When you finish loading the module, type **`execute`** -- and you should see the result as below. **Take a screenshot of your outcome**



n. Now, go to your Win7 VM. Open the *Notepad* program, type in something, and save it somewhere on your **`C:\`** drive

o. When you see valid results returned from your Win7, you will know that the agent works successfully.

p. Now, open another CLI session in your Kali (to avoid disconnecting your Empire). Go to the **`/opt/Empire/downloads`** directory. You should see a directory with the same name as your interactive session (i.e., the *agent* name). **Take a screenshot** of all the files you have in the directory.

q. **`cd`** to the directory, display the **`keystrokes.txt`** file, and **take the screenshot** of what your Empire could record. See the example below.