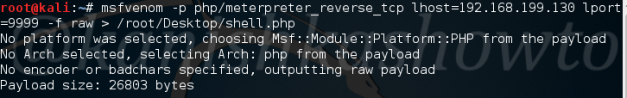
Uploading shell and hacking a website : Metasploit

Posted by  *kanishka10* on  *August 9, 2016*

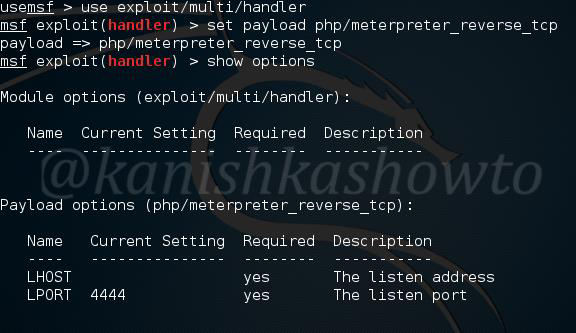
Hello aspiring hackers. In our previous howtos, we saw about different shells like the infamous c99 shell, web shells in Kali Linux and Weevely. In this howto, we will see about hacking a website by uploading shell made with Metasploit. We will be getting a meterpreter shell on the website.

One of the wonderful features of Metasploit is creating payloads as per requirement. Using msfvenom, we can create binaries for Windows, MAC and Linux. We can also create shell payloads for websites in different formats like php, asp , javascript and asp. In future howto’s we will definitely learn more about msfvenom but for this howto, we will create a php payload.

As you can see below, I have created a php payload named “shell.php” with the metasploit payload option “php/meterpreter\_reverse\_tcp”. This gives us a reverse php meterpreter shell. The “lhost” option is our attacker system’s IP address and “lport” the port on which we want php meterpreter shell back.



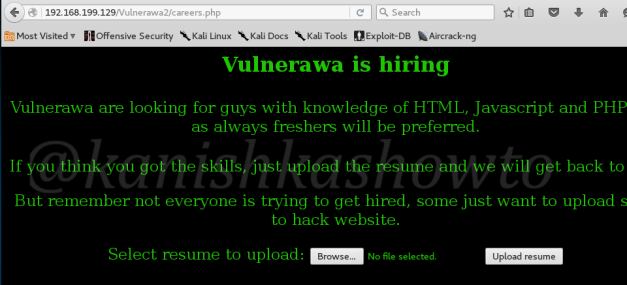
After the shell is successfully created, let’s start a listener with Metasploit as shown below. Remember to set the same payload we set while creating the payload.



Set the lhost and lport as shown below. They should match with the values in the shell we created. Type command “run” to start the listener.



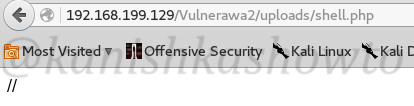
Now you need to find a site vulnerable to file upload. For this howto, I’m using my own vulnerable webapp “Vulnerawa”. To know more about Vulnerawa go here. Vulnerawa has a file upload vulnerability in its careers page.



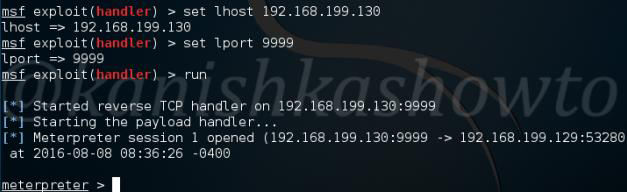
Go to its file upload page and upload the shell. That shouldn’t be a big problem.



Now go to the shell we just uploaded through the website.Normally its located in the uploads directory ( In real websites, you need to locate it ). The shell will look like below.



In the listener we startedan the attacker system, we should have already got the meterpreter shell. Happy hacking.



**Share This Now**