Upload shell to hack a website : Part3 – Weevely

Posted by  *kanishka10* on  *July 4, 2016*

Upload shell to hack a website: Part2-webshells in Kali Linux

Hello aspiring hackers. It would be completely unfair to discuss about web shells without discussing about Weevely.

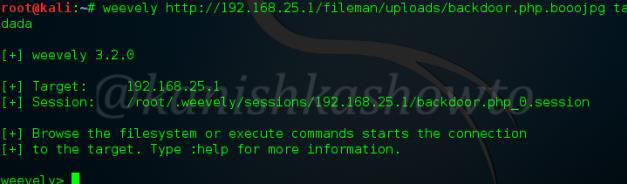
Weevely is a command line web shell dynamically extended over the network at runtime, designed for remote administration and penetration testing or bad things. It provides a ssh-like terminal just dropping a PHP script on the target server, even in restricted environments. The best thing about Weevely is its stealth functionality. So today we will see how Weevely functions.

It is inbuilt installed in Kali Linux although here I have downloaded from Github. So let us first generate a shell as shown below. “tadada” is the famous ( or rather infamous ) password we have assigned for our shell and the name assigned to our shell is backdoor. Now let us upload this shell to our target. In this howto, I have uploaded it into both Wamp server and Linux web server. Go here

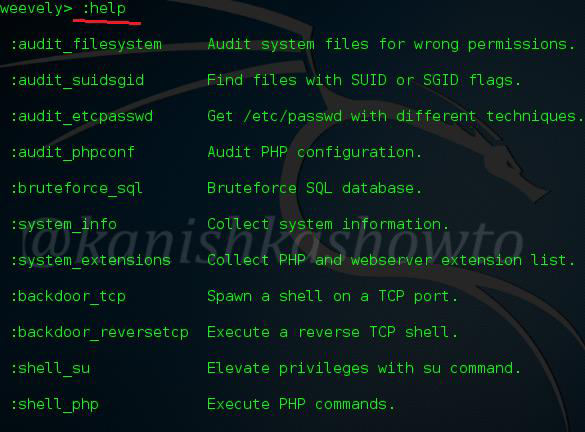
to see how to upload the shell.



After uploading the shell, we can connect to our shell using the command shown below. Well we made a connection.

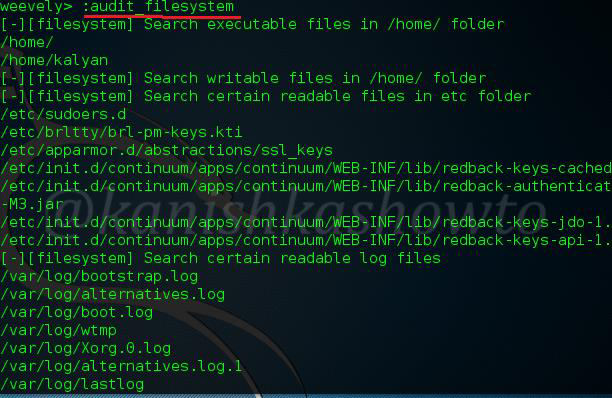


Now let us type command “:help” to see all the commands weevely provides. We will see usage of each command.



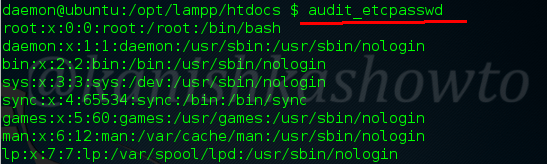
:audit\_filesystem

This command, as the name implies is used to audit the file system of the remote web server. The below screenshot shows the result of this command on a Linux web server.



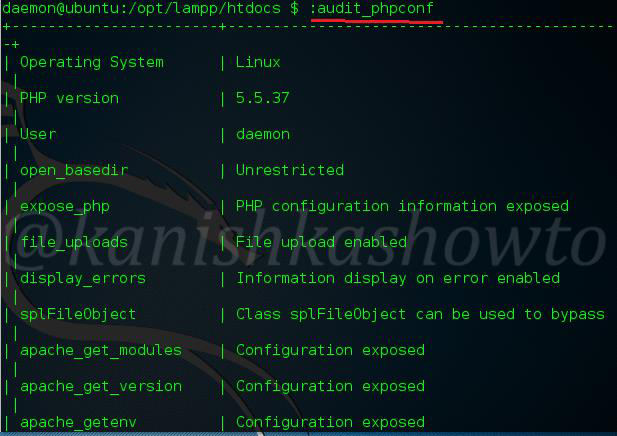
:audit\_etcpasswd

This command needs no explanation. It is used to view the passwd file of our target and obviously will work only on Linux.



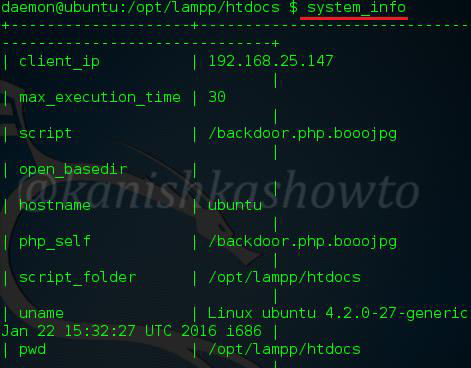
:audit\_phpconf

This command lets us have a look at the php configuration on the remote web server as shown below. We can get lot of information which can be useful in further hacks.



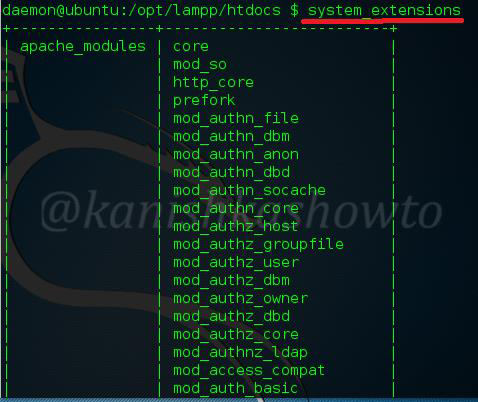
:system\_info

This command is used to know the whole system information. Below we can see lot of info about our target system.

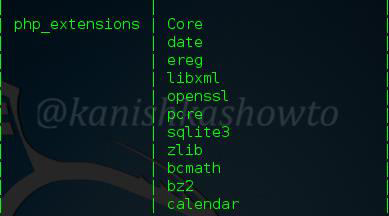


:system\_extensions

This command shows us the system extensions enabled on the web server. Here are the apache\_modules



and the php\_extensions enabled on the web server.

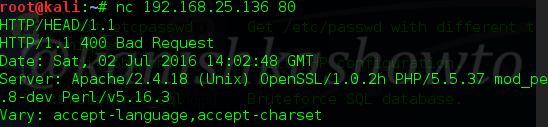


:backdoor\_tcp

If you have gone through the above link, you already know what is a backdoor. We can create a backdoor on the web server as shown below. Here we have created a shell backdoor using netcat on port 80.



Now open another terminal and type the command shown below. The IP address is our target’s address. It directly provides us a connection to port 80 of the target. You can also use other ports to connect to but the port should be open on our target.



:backdoor\_reversetcp

We also saw the reverse backdoors in our previous howtos. Here, we are creating a backdoor to our attacker machine on port 1122. The IP address should be our attacker machine’s.

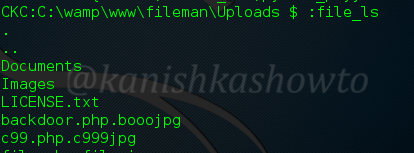


Once we create a reverse backdoor, we just need to listen on the port we specified above using netcat as shown below.



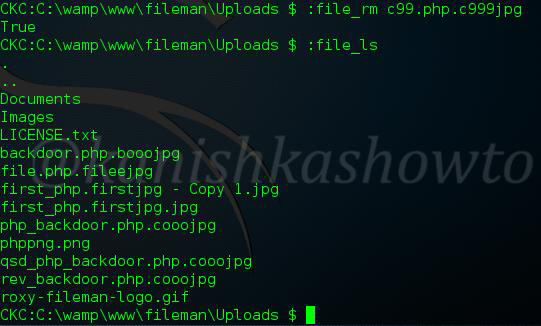
:file\_ls

This is akin to “ls” command in Linux. It is used to see the contents of the directory.



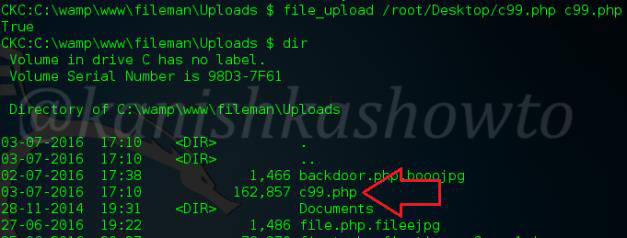
:file\_rm

It is used to delete any file from the directory. For example, I deleted the file c99.php.c999jpg as shown below.If our command has worked successfully, the terminal will return a true as shown below.



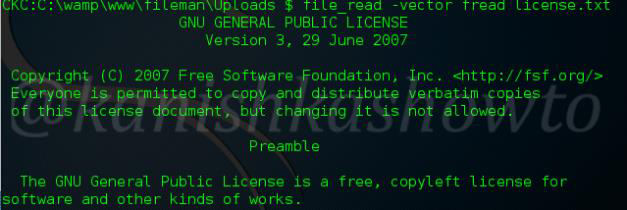
:file\_upload

This is used to upload files. I have uploaded the c99 shell below. Go here to know more about the c99 shell and how it is used to hack the websites.



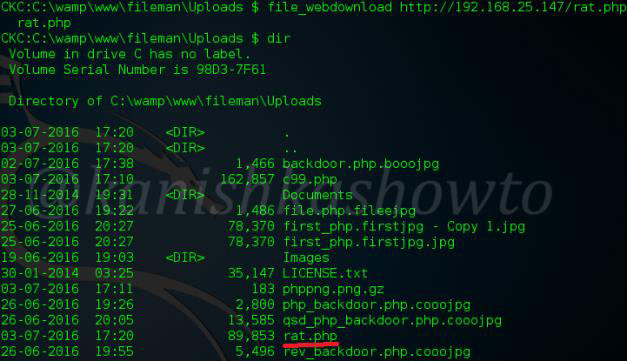
:file\_read

Used to read files.



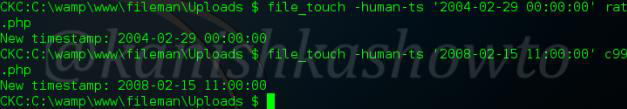
:file\_webdownload

What if file upload doesn’t work? We can download any files from the internet. Suppose imagine we want to download a virus into our target and file upload doesn’t function ( in rare case ). We can host the virus on any free uploading site and download it using command shown below.

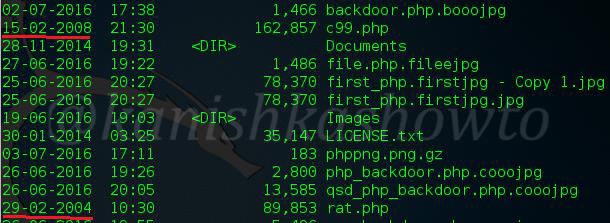


:file\_touch

Now this one is important. This command is used to change time stamps. Let us change time stamps for files we have just uploaded. This is useful in raising less suspicions on the other side.

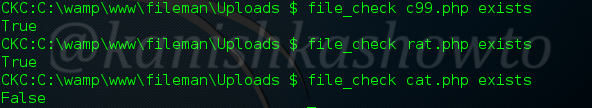


As we can see, time stamps of our files have been successfully changed.



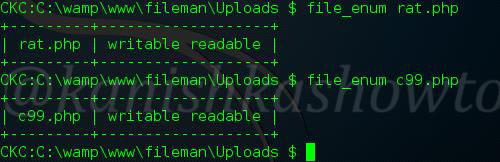
:file\_check

This command is used to see if a file exists as shown below.



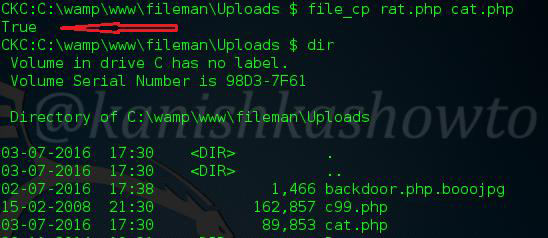
:file\_enum

To enumerate the permissions of the files.



:file\_cp

To make a copy of a file.



:file\_edit

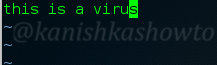
To edit a file not only in this directory but also other directories. For example, let us edit a file in the home directory with the name virus.



This are the contents of the file. Oh bad english.



Let’s correct it. Actually this is used to edit files and change their script.



For example, we can edit the index page to deface the website.



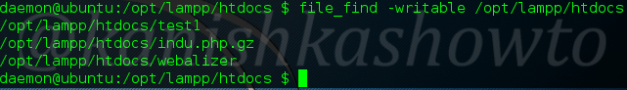
:file\_cd

To change directories.



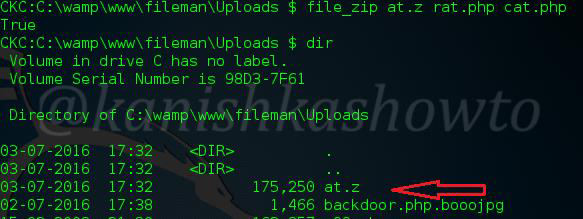
:file\_find

To search for files with specific properties. For example, we have searched for all writable files in the directory. Similarly we can also search for executable files.



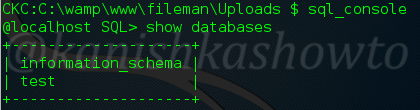
:file\_zip

Weevely provides us many functions to compress and decompress files. These include tar,bzip, gzip and zip. Here I am showing you an example of compressing two files into a zip archive.



:sql\_console

Used to connect to the sql console.



:bruteforce\_sql

We are not always lucky to have an unprotected sql connection. In that case, this command can be used to bruteforce the credentals.



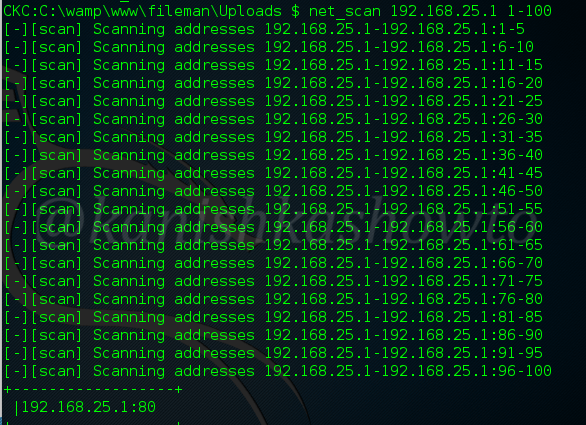
:sql\_dump

After we get the credentials, we can dump the database we want using this command.



:net\_scan

In this howto itself, we saw how to create a backdoor and we also discussed that an open port is required for creating this backdoor. We can scan for open ports using this command. We can see just port 80 is open.



:net\_ifconfig

Used to check all the network interfaces of the system.

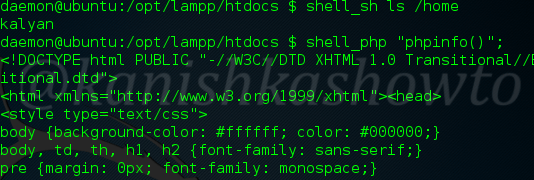


:shell\_sh

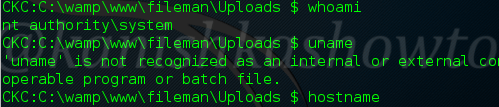
This command is used to execute any shell command on the system.

:shell\_php

Shell\_php command is used to execute php commands on the target server. Here I have executed phpinfo() command.



Once we get a shell, we can also execute all the standard commands of the shell like whoami, uname and hostname etc..etc.



Well that was weevely for you. Hope that was helpful.

v