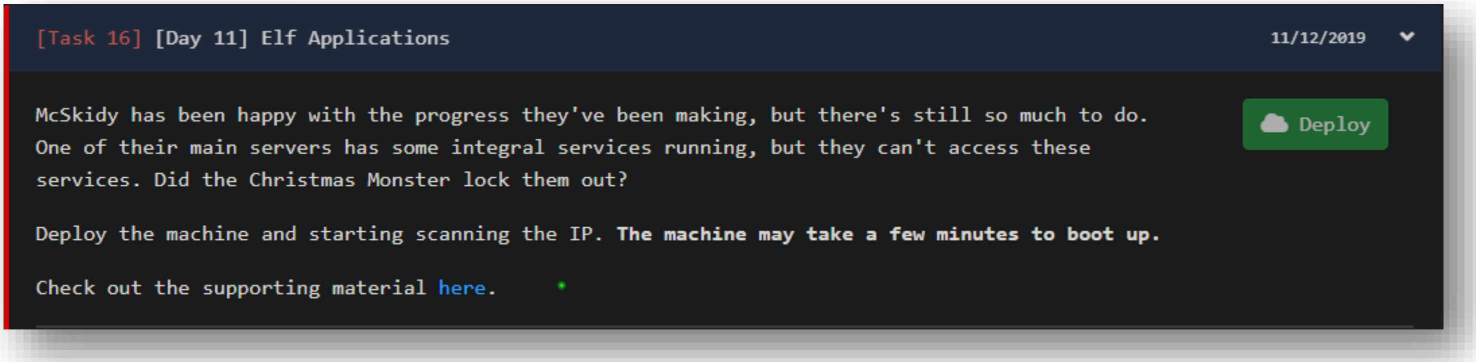
https://docs.google.com/document/d/1qCMuPwBR0gWIDfk_PXt0Jr220JIJAQ-N4foDZDVX59U/edit#



[Task 16] [Day 11] Elf Applications 11/12/2019

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.**

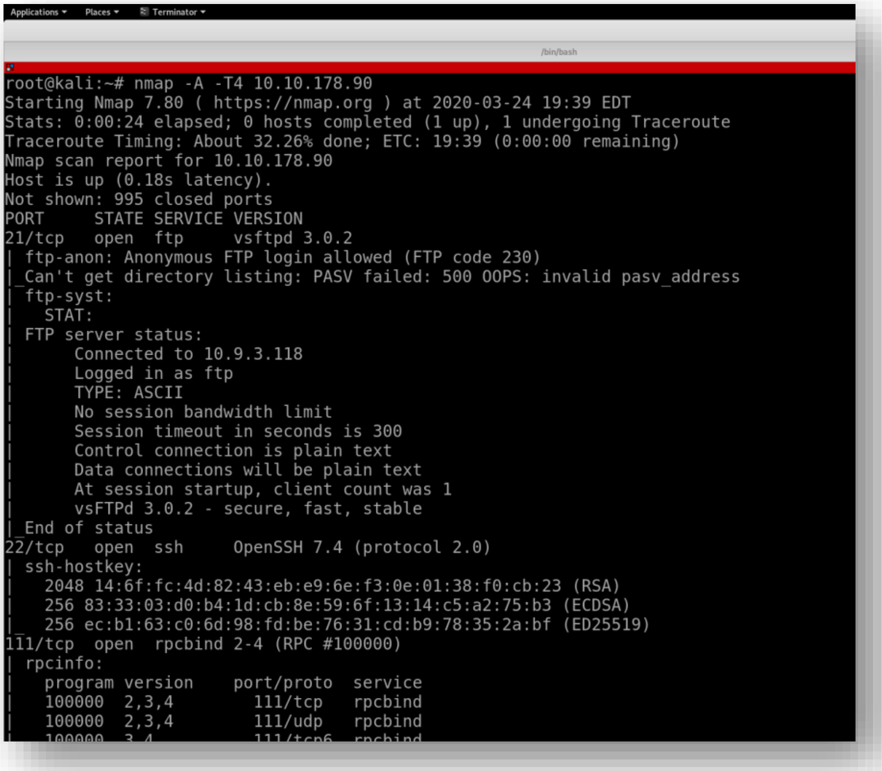
Check out the supporting material here.

Objectives

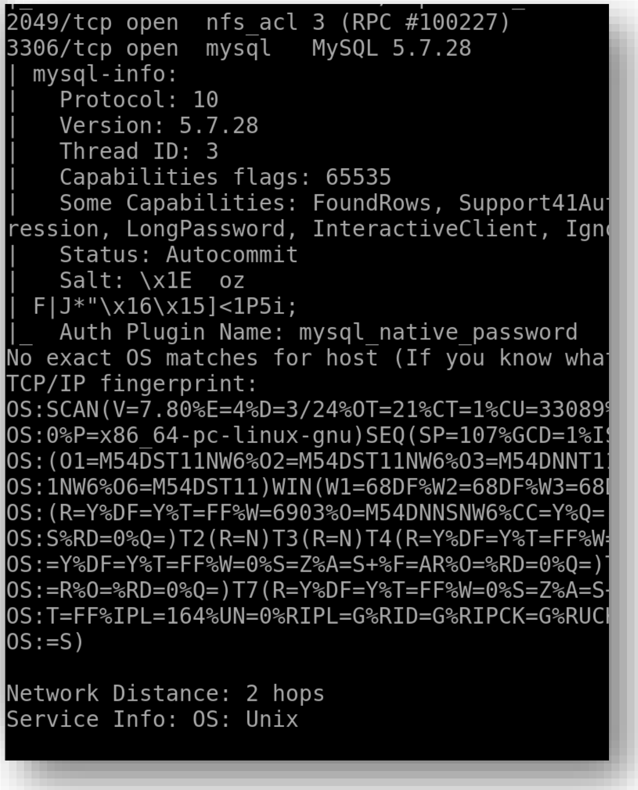
1. What is the password inside the creds.txt file?
2. What is the name of the file running on port 21?
3. What is the password after enumerating the database?

1. What is the password inside the creds.txt file?

- Lets scan the machine with nmap



```
root@kali:~# nmap -A -T4 10.10.178.90
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-24 19:39 EDT
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing Traceroute
Traceroute Timing: About 32.26% done; ETC: 19:39 (0:00:00 remaining)
Nmap scan report for 10.10.178.90
Host is up (0.18s 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 10.9.3.118
|      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 1
|      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)
| 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
```



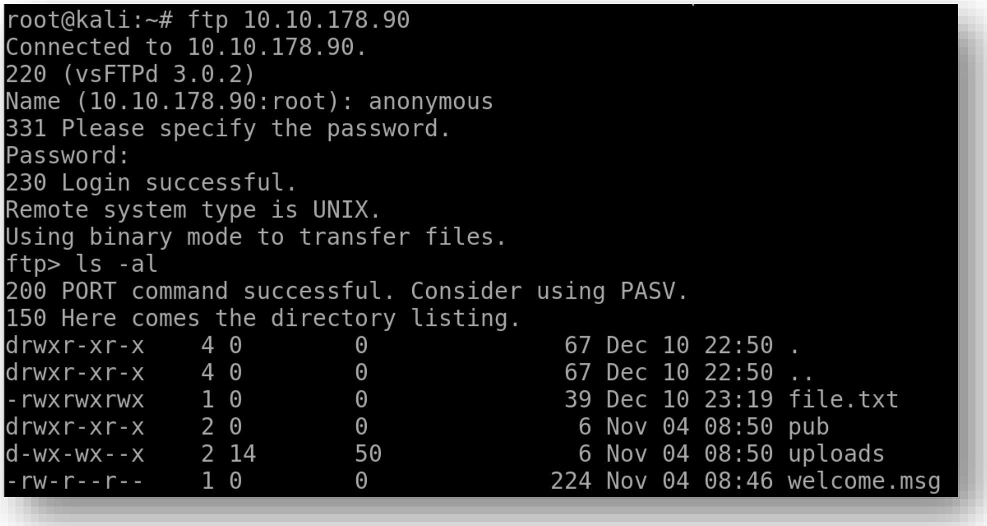
```
2049/tcp open  nfs_acl 3 (RPC #100227)
3306/tcp open  mysql   MySQL 5.7.28
| mysql-info:
|   Protocol: 10
|   Version: 5.7.28
|   Thread ID: 3
|   Capabilities flags: 65535
|   Some Capabilities: FoundRows, Support41Au
ression, LongPassword, InteractiveClient, Ign
|   Status: Autocommit
|   Salt: \x1E  oz
| F|J*"\x16\x15]<1P5i;
|_  Auth Plugin Name: mysql_native_password
No exact OS matches for host (If you know wha
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=3/24%OT=21%CT=1%CU=33089
OS:0%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%I
OS:(O1=M54DST11NW6%O2=M54DST11NW6%O3=M54DNNT1
OS:1NW6%O6=M54DST11)WIN(W1=68DF%W2=68DF%W3=68
OS:(R=Y%DF=Y%T=FF%W=6903%O=M54DNNSNW6%CC=Y%Q=
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=FF%W
OS:=Y%DF=Y%T=FF%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=FF%W=0%S=Z%A=S
OS:T=FF%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUC
OS:=S)

Network Distance: 2 hops
Service Info: OS: Unix
```

Open ports include:

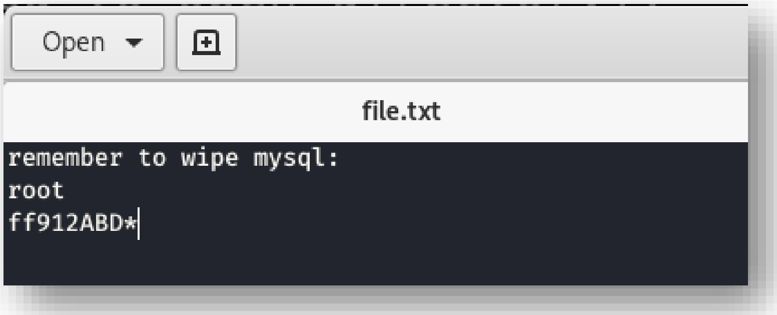
PORT	21/tcp	22/tcp	111/tcp	2049/tcp	3306/tcp
SERVICE	ftp	Ssh	Rpcbind	Nfs_acl	mysql

- Lets try to connect to ftp server and see what files are available
- Nmap shows that anonymous FTP login is allowed. Default anonymous username and password are: anonymous:anonymous



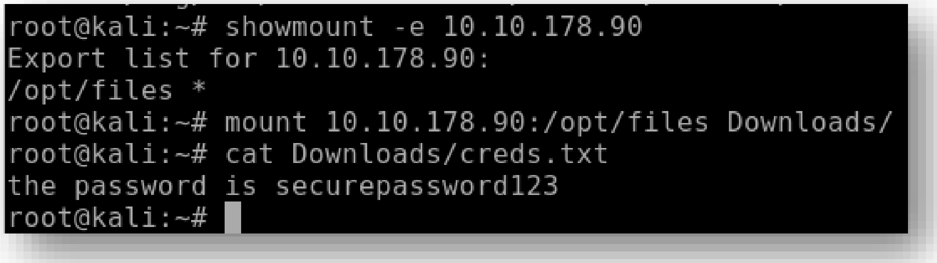
```
root@kali:~# ftp 10.10.178.90
Connected to 10.10.178.90.
220 (vsFTPd 3.0.2)
Name (10.10.178.90:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    4 0        0              67 Dec 10 22:50 .
drwxr-xr-x    4 0        0              67 Dec 10 22:50 ..
-rwxrwxrwx    1 0        0              39 Dec 10 23:19 file.txt
drwxr-xr-x    2 0        0               6 Nov 04 08:50 pub
d-wx-wx--x    2 14       50              6 Nov 04 08:50 uploads
-rw-r--r--    1 0        0             224 Nov 04 08:46 welcome.msg
```

- Once connected, ls command is used to show all files in root directory
- Can use get command to download files. File.txt and welcome.msg are downloaded. The pub directory is empty, and we do not have permission to view the uploads directory
- Examining file.txt:



```
remember to wipe mysql:
root
ff912ABD*
```

- Looks to be the login to the mysql server on port 3306
- There is nothing else on this ftp server
- Lets try the next available port/service, NFS



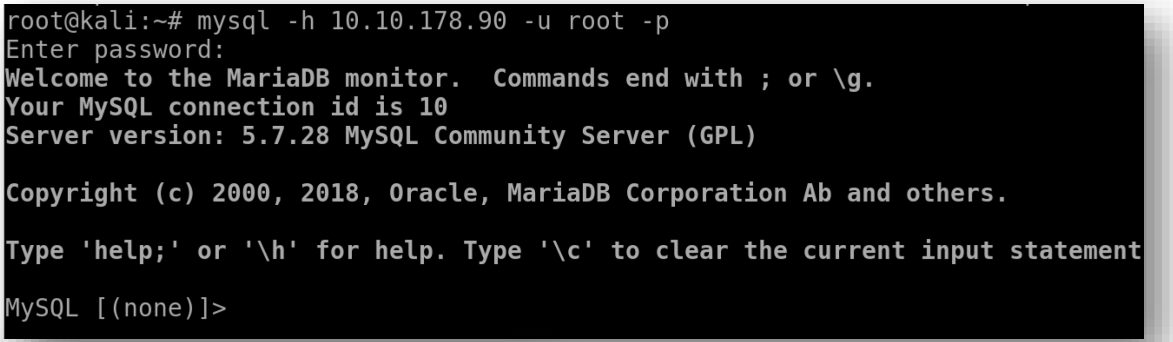
```
root@kali:~# showmount -e 10.10.178.90
Export list for 10.10.178.90:
/opt/files *
root@kali:~# mount 10.10.178.90:/opt/files Downloads/
root@kali:~# cat Downloads/creds.txt
the password is securepassword123
root@kali:~# 
```

- Use showmount command to see if any shares are available; /opt/files is available
- Mount that network share to Downloads/ directory, and read the creds.txt file

- The password inside the creds.txt file is securepassword123

2. **What is the name of the file running on port 21?**
   - Port 21 is the ftp server; that file we found was named **‘file.txt’** with the mysql credentials

3. **What is the password after enumerating the database?**
   - Lets use the file.txt credentials to log into the mysql server

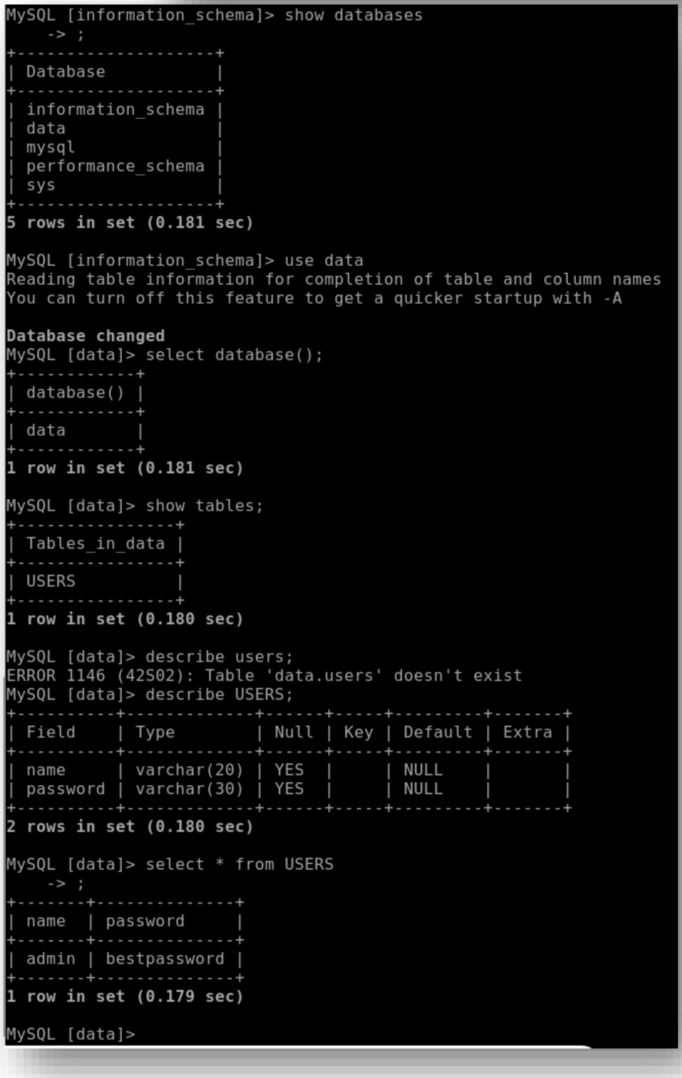


```
root@kali:~# mysql -h 10.10.178.90 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 5.7.28 MySQL Community Server (GPL)

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)]>
```



```
MySQL [information_schema]> show databases
    -> ;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| data               |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.181 sec)

MySQL [information_schema]> use data
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [data]> select database();
+------------+
| database() |
+------------+
| data       |
+------------+
1 row in set (0.181 sec)

MySQL [data]> show tables;
+----------------+
| Tables_in_data |
+----------------+
| USERS          |
+----------------+
1 row in set (0.180 sec)

MySQL [data]> describe users;
ERROR 1146 (42S02): Table 'data.users' doesn't exist
MySQL [data]> describe USERS;
+----------+-------------+------+-----+---------+-------+
| Field    | Type        | Null | Key | Default | Extra |
+----------+-------------+------+-----+---------+-------+
| name     | varchar(20) | YES  |     | NULL    |       |
| password | varchar(30) | YES  |     | NULL    |       |
+----------+-------------+------+-----+---------+-------+
2 rows in set (0.180 sec)

MySQL [data]> select * from USERS
    -> ;
+-------+--------------+
| name  | password     |
+-------+--------------+
| admin | bestpassword |
+-------+--------------+
1 row in set (0.179 sec)

MySQL [data]>
```

- Use commands to enumerate the database; to show all databases use ‘show databases’
- To select a database use ‘use <database name>’
- To show the tables in the database use ‘show tables’
- To describe a particular table use ‘describe <table name>’
- To view the table, we can use SQL such as:
- SELECT * FROM USERS
- This will select all the rows from the USERS table
- In our case there is only one entry in the table, admin, with a plaintext password, bestpassword