Austin Brown

CPE 434-01

3/29/2021

Lab 11 Part 2

PreTask

Limit login attempts, encryption, and multi-factor authentication will all work.

Subtask 1

1.

```
asb0034@blackhawk.ece.uah.edu's password:
Last login: Mon Mar 29 12:53:40 2021 from c-68-35-162-131.hsd1.al.comcast.net
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
        LANGUAGE = (unset),
        LC_ALL = (unset),
        LANG = "C.UTF-8"
    are supported and installed on your system.
perl: warning: Falling back to the standard locale ("C").
-bash-4.2$ ssh echo
asb0034@echo's password:
Last login: Mon Mar 29 12:54:00 2021 from blackhawk
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
        LANGUAGE = (unset),
        LC_ALL = (unset),
        LANG = "C.UTF-8"
    are supported and installed on your system.
perl: warning: Falling back to the standard locale ("C").
```

2.

```
odroid@odroid:~$ ssh -p 22 -l root 192.168.5.2
root@192.168.5.2's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0 armv7l)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Mon Mar 29 18:06:18 2021 from 192.168.5.1
root@odroid:~#
root@odroid:~#
```

3.

```
odroid@odroid:~$ ssh -p 22 -l root 192.168.5.2
root@192.168.5.2's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0 armv7l)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Mon Mar 29 18:15:52 2021 from 192.168.5.1
root@odroid:~#
```

4.

```
Last login: Mon Mar 29 18:15:52 2021 from 192.168.5.1
root@odroid:~# apt-get install libpam-google-authenticator
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libllvm3.8 libmircommon5
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  libqrencode3
The following NEW packages will be installed:
  libpam-google-authenticator libqrencode3
0 upgraded, 2 newly installed, 0 to remove and 86 not upgraded.
144 not fully installed or removed.
Need to get 52.0 kB of archives.
After this operation, 155 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ports.ubuntu.com/ubuntu-ports xenial/universe armhf libqrencode3 arm
Get:2 http://ports.ubuntu.com/ubuntu-ports xenial/universe armhf libpam-google-au
Fetched 52.0 kB in 0s (215 kB/s)
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
```

5.

```
root@odroid:~# exit
logout
Connection to 192.168.5.2 closed.
odroid@odroid:~$ ssh -p 22 -l root 192.168.5.2
root@192.168.5.2's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0 armv7l)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Mon Mar 29 18:24:22 2021 from 192.168.5.1
root@odroid:~#
```

6.

```
odroid@odroid:~$ hydra -l asb0034 -P hack.txt ssh://192.168.5.2 -s 22
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military

Hydra (http://www.thc.org/thc-hydra) starting at 2021-03-29 18:32:24
[WARNING] Many SSH configurations limit the number of parallel tasks,
[DATA] max 11 tasks per 1 server, overall 64 tasks, 11 login tries (l:
[DATA] attacking service ssh on port 22
[22][ssh] host: 192.168.5.2   login: asb0034   password: 1234
```

7. I have not changed the password.

8. Installed Authenticator

9.

```
$ google-authenticator

Do you want authentication tokens to be time-based (y/n) y
https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/asb0034@odroi
```

10.

```
Your new secret key is: VGY655MFNTMJ5XLR
Your verification code is 009187
Your emergency scratch codes are:
  27394518
  36166075
  21006618
  48604580
  68061058
```

11.

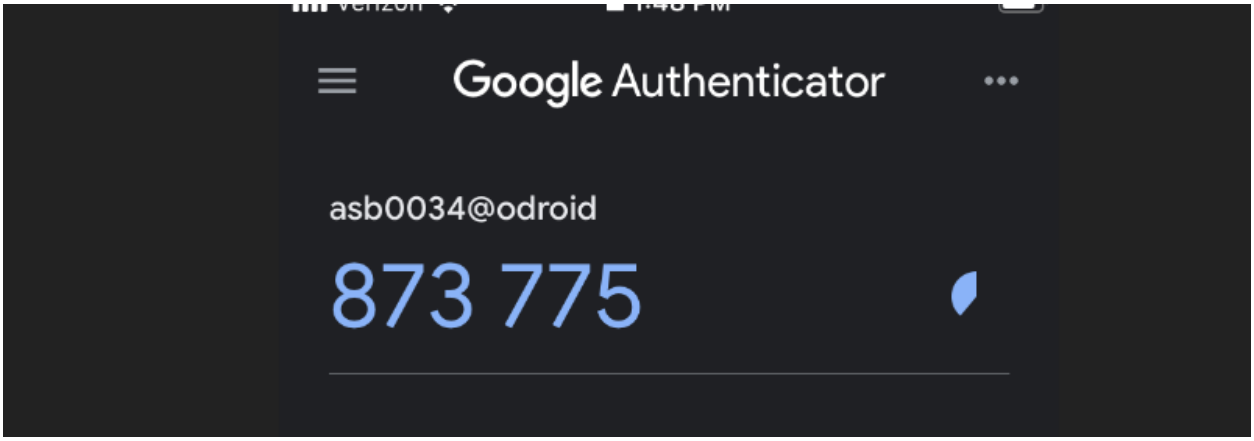
Update file – save info for later

Prevent token from being used more than once – prevent man in the middle

Increase time token is valid – account for latency

Limit login attempts – prevent brute forcing

12.



15.

```
$ exit
logout
root@odroid:~# login asb0034
Password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0 armv7l)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
```

No difference. I could login.

16.

```
odroid@odroid:~$ hydra -l asb0034 -P hack.txt ssh://192.168.5.2 -s 22
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military

Hydra (http://www.thc.org/thc-hydra) starting at 2021-03-29 18:51:13
[WARNING] Many SSH configurations limit the number of parallel tasks,
[DATA] max 11 tasks per 1 server, overall 64 tasks, 11 login tries (l
[DATA] attacking service ssh on port 22
[22][ssh] host: 192.168.5.2   login: asb0034   password: 1234
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-03-29 18:51:22
```

I could get into the account. This is likely because 2FA is not configured yet.

17. Hydra is not installed on guest.

Subtask 3

19.

```
# Change to yes to enable challenge-response passwords (beware
# some PAM modules and threads)
ChallengeResponseAuthentication yes

# Change to no to disable tunnelled clear text passwords
#PasswordAuthentication yes

# Kerberos options
#KerberosAuthentication no
#KerberosGetAFSToken no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
```

```
# Standard Un*x password updating.
@include common-password
auth required pam_google_authenticator.so nullok
```

20.

```
root@odroid:~# ssh -p 22 -l asb0034 192.168.5.2
Password:
Verification code:
```

I was not allowed to login until I entered the code from google authenticator.

22.

```
odroid@odroid:~$ hydra -l asb0034 -P hack.txt ssh://192.168.5.2 -s 22
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military c

Hydra (http://www.thc.org/thc-hydra) starting at 2021-03-29 19:47:13
[WARNING] Many SSH configurations limit the number of parallel tasks, i
[DATA] max 11 tasks per 1 server, overall 64 tasks, 11 login tries (l:1
[DATA] attacking service ssh on port 22
1 of 1 target completed, 0 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-03-29 19:47:23
```

The attack failed because hydra didn't know the key.

Tampering

23.

NTP servers are used to sync times across various systems.

24.

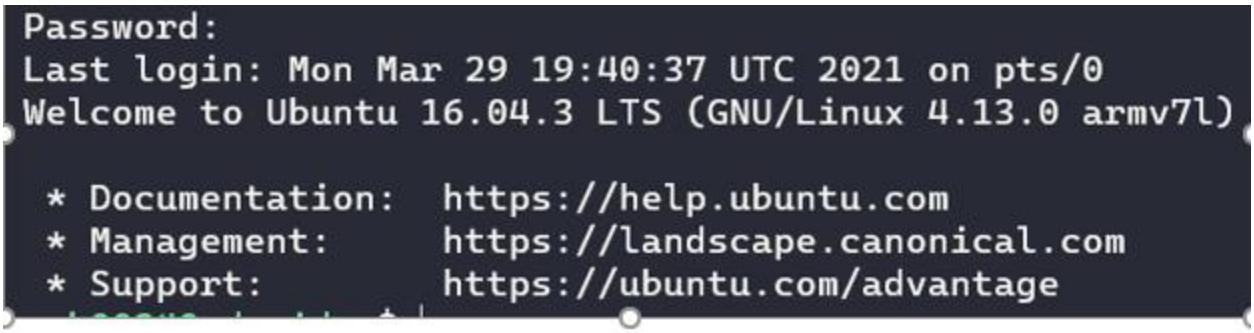
```
root@odroid:~# date --set="23 MAY 2020 18:2:00"
Sat May 23 18:02:00 UTC 2020
root@odroid:~#
```

```
Mon Mar 29 19:52:26 UTC 2021
odroid@odroid:~$
```

```
root@odroid:~# date --set="23 MAY 2020 18:2:00"
Sat May 23 18:02:00 UTC 2020
root@odroid:~#
```

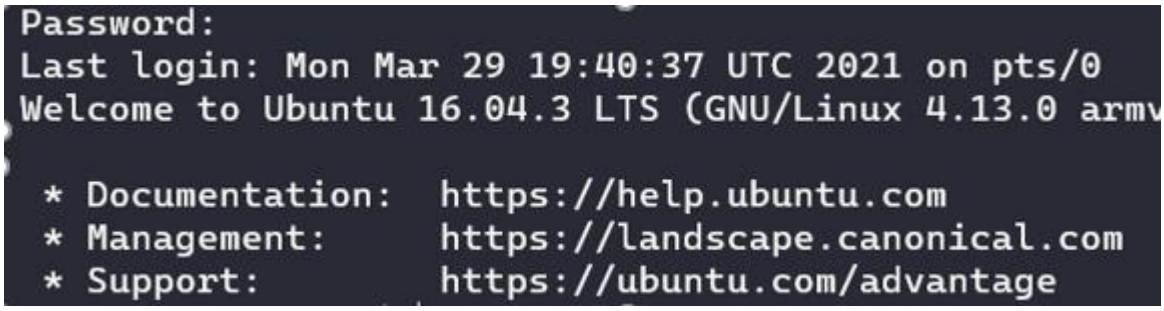
The times are different.

25.

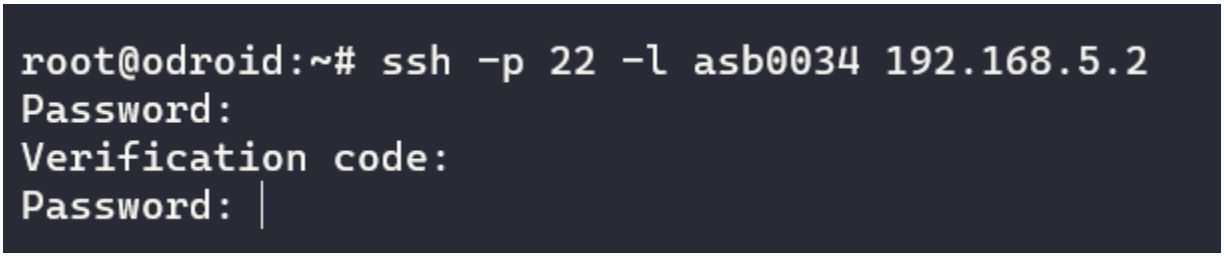


I can login. The date corrects itself.

26



27.



I cannot log in. Entering a verification code does nothing.

Finishing

28.

```
# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no
```

29.

```
# Standard Un*x password updating.
@include common-password
```

30.

```
root@odroid:~# sudo systemctl restart sshd.service
root@odroid:~#
```

31.

```
odroid@odroid:~$ hydra -l asb0034 -P hack.txt ssh://192.168.5.2 -s 22
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military

Hydra (http://www.thc.org/thc-hydra) starting at 2021-03-29 20:08:20
[WARNING] Many SSH configurations limit the number of parallel tasks,
[DATA] max 11 tasks per 1 server, overall 64 tasks, 11 login tries (l:
[DATA] attacking service ssh on port 22
[22][ssh] host: 192.168.5.2   login: asb0034   password: 1234
```

32.