

Andrew Ma

Lab 11 Part 2

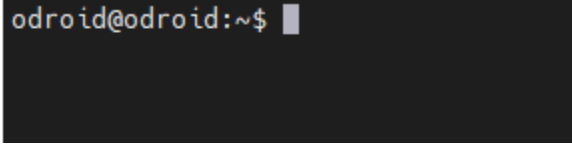
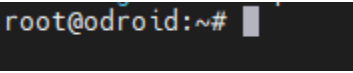
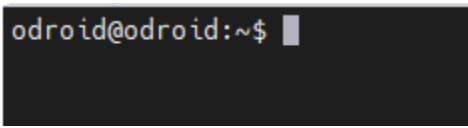
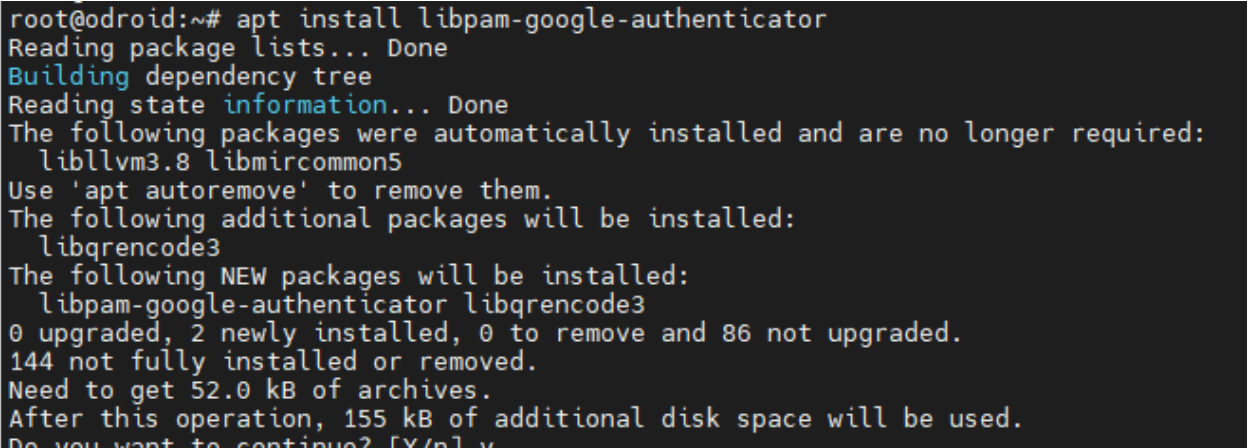
CPE 435

3/29/21

Pretask 1

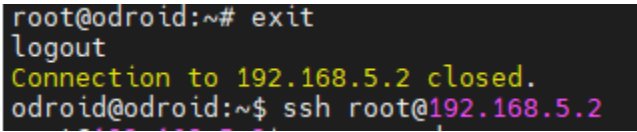
1. One strategy could be using stronger passwords that would not be in a password wordlist. Another strategy could be disabling password login and only allowing ssh with a private key.

Subtask 1

1.  Host: odroid@172.22.4.50
2.  Guest: root@192.168.5.2
3. 
4. 

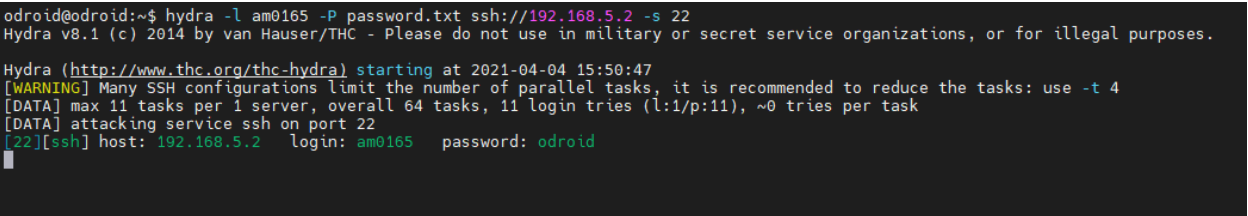
```

root@odroid:~# apt 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

```
5. 

```

root@odroid:~# exit
logout
Connection to 192.168.5.2 closed.
odroid@odroid:~$ ssh root@192.168.5.2

```
6. 

```

odroid@odroid:~$ hydra -l am0165 -P password.txt ssh://192.168.5.2 -s 22
Hydra v8.1 (c) 2014 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 2021-04-04 15:50:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 11 tasks per 1 server, overall 64 tasks, 11 login tries (l:1/p:11), ~0 tries per task
[DATA] attacking service ssh on port 22
[22][ssh] host: 192.168.5.2  login: am0165  password: odroid

```

Yes, I was able to hack into the account. I ran the hydra command with username am0165 and the password list with “odroid” as the 11th password guess.

```
odroid@odroid:~$ hydra -l am0165 -P password.txt ssh://192.168.5.2 -s 22
Hydra v8.1 (c) 2014 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 2021-04-04 15:50:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 11 tasks per 1 server, overall 64 tasks, 11 login tries (l:1/p:11), ~0 tries per task
[DATA] attacking service ssh on port 22
[22][ssh] host: 192.168.5.2 login: am0165 password: odroid
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-04-04 15:50:58
odroid@odroid:~$
```

7.

8.

10:52



Setup your first account

Use the QR code or setup key in your 2FA settings
(by Google or third-party service). If you're having
trouble, go to g.co/2sv



Scan a QR code



Enter a setup key

[Import existing accounts?](#)

```

root@odroid:~# ssh am0165@192.168.5.2
am0165@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: Sun Apr  4 15:50:34 2021 from 192.168.5.1
$ 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/am0165@odroid%3Fsecret%3DP4V206XDFKHI7D
G6



Your new secret key is: P4V206XDFKHI7DG6
Your verification code is 097745
Your emergency scratch codes are:
24570130
46999010
23174369
83982285
43410506

Do you want me to update your "/home/am0165/.google_authenticator" file (y/n) █

```

9.

```

Your new secret key is: P4V206XDFKHI7DG6
Your verification code is 097745
Your emergency scratch codes are:
24570130
46999010
23174369
83982285
43410506

```

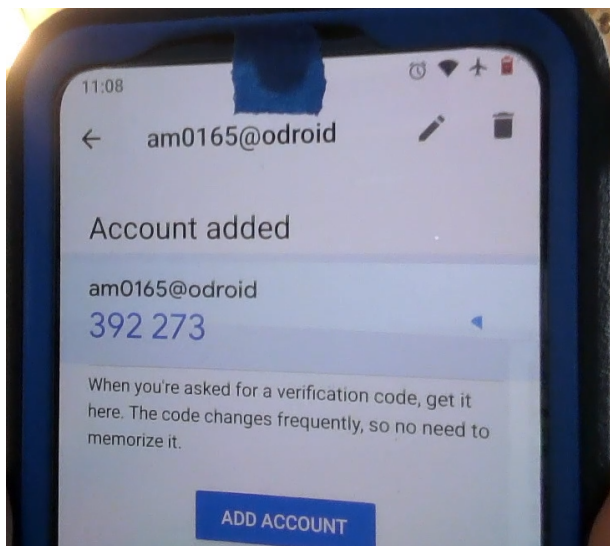
10.

11. There were 4 questions. The first question is for updating the local file, and it is for saving the secret key and emergency scratch codes. It is important incase we lose access to the google authenticator we can still get access with the emergency codes. The second question is disallowing multiple uses of the same authentication token. This is important

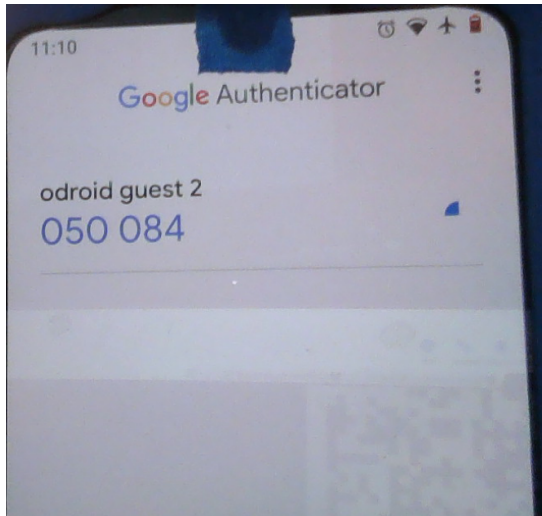
because it forces people to wait 30 seconds, so if the code doesn't work then it is possible that there was a MITM that used the code in the 30 second window. The third question is To expand the time window from 1:30 min to 4 min. This is to allow more flexibility in the time synchronization. The fourth question is for rate limiting attempts. It is important because it limits attackers to 3 attempts every 30 seconds.

```
Do you want me to update your "/home/am0165/.google_authenticator" file (y/n) y
Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n) n
By default, tokens are good for 30 seconds and in order to compensate for
possible time-skew between the client and the server, we allow an extra
token before and after the current time. If you experience problems with poor
time synchronization, you can increase the window from its default
size of 1:30min to about 4min. Do you want to do so (y/n) n
If the computer that you are logging into isn't hardened against brute-force
login attempts, you can enable rate-limiting for the authentication module.
By default, this limits attackers to no more than 3 login attempts every 30s.
Do you want to enable rate-limiting (y/n) n
$
```

```
$ cat .google_authenticator
P4V206XDFKHI7DG6
" TOTP_AUTH
24570130
46999010
23174369
83982285
43410506
$
```



- 12.
13. N/A



14.

15. There is no difference. Yes, I was able to login to the second user account, because ssh was not configured to use 2fa.

```
root@odroid:~# ssh am0165@192.168.5.2
am0165@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: Sun Apr  4 15:53:18 2021 from 192.168.5.2
$
```

```
Hydra (http://www.thc.org/thc-hydra) finished at 2021-04-04 15:50:58
odroid@odroid:~$ hydra -l am0165 -P password.txt ssh://192.168.5.2 -s 22
Hydra v8.1 (c) 2014 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 2021-04-04 16:18:22
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 11 tasks per 1 server, overall 64 tasks, 11 login tries (l:1/p:11), ~0 tries per task
[DATA] attacking service ssh on port 22
[22][ssh] host: 192.168.5.2  login: am0165  password: odroid
```

16.

Yes I was able to hack it because ssh was not configured to use 2fa, so nothing changed.

```
root@odroid:~# hydra -l am0165 -P password.txt ssh://192.168.5.2 -s 22
Hydra v8.1 (c) 2014 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 2021-04-04 16:21:57
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 64 tasks, 1 login try (l:1/p:1), ~0 tries per task
[DATA] attacking service ssh on port 22
[22][ssh] host: 192.168.5.2  login: am0165  password: odroid
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-04-04 16:21:58
root@odroid:~#
```

17.

Yes I was also able to hack the am0165 account on the guest machine from the root account.

18.

```
root@odroid:~#
```

19.

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

```
# Change to no to disable tunnelled clear text passwords
```

```
auth required pam_google_authenticator.so nullok
~
~
```

```
root@odroid:~# vi /etc/ssh/sshd_config
root@odroid:~# vi /etc/pam.d/sshd
root@odroid:~# sudo systemctl restart sshd.service
root@odroid:~#
```

20. This time I had to type in the verification code after typing in the password.

```
root@odroid:~# ssh am0165@192.168.5.2
Password:
Verification code:
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: Sun Apr  4 16:13:11 2021 from 192.168.5.2
$
```

```
odroid@odroid:~$
```

21.

22. No, this time I was not able to hack into the account. This is because the 2FA was set up properly on the google authenticator and on the ssh config.

```
odroid@odroid:~$ hydra -l am0165 -P password.txt ssh://192.168.5.2 -s 22
Hydra v8.1 (c) 2014 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 2021-04-04 16:28:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 11 tasks per 1 server, overall 64 tasks, 11 login tries (l:1/p:11), ~0 tries per task
[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 2021-04-04 16:28:44
odroid@odroid:~$
```

23. NTP is network time protocol, and a NTP server is used for synchronizing the time of computer clients.

```
odroid@odroid:~$ date
Sun Apr  4 16:31:31 UTC 2021
odroid@odroid:~$
```

24. Hacking

```
root@odroid:~# date
Sun Apr  4 16:31:00 UTC 2021
root@odroid:~#
```

Backup:

```
root@odroid:~# date -s "19 APR 2012 11:14:00"
Thu Apr 19 11:14:00 UTC 2012
root@odroid:~# date
Sun Apr  4 16:32:22 UTC 2021
```

25. Yes I was able to login normally with the verification code.

```
odroid@odroid:~$ ssh am0165@192.168.5.2
Password:
Verification code:
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: Sun Apr  4 16:26:35 2021 from 192.168.5.2
$
```

26. N/A

```
root@odroid:~# timedatectl set-ntp 0
root@odroid:~# date -s "19 APR 2012 11:14:00"
Thu Apr 19 11:14:00 UTC 2012
root@odroid:~# date
Thu Apr 19 11:14:00 UTC 2012
root@odroid:~#
```

- 27.

I was unable to login even after multiple tries and different verification codes.

```
odroid@odroid:~$ ssh am0165@192.168.5.2
Password:
Verification code:
Password:
Verification code:
Password:
Verification code:
am0165@192.168.5.2's password:
Permission denied, please try again.
am0165@192.168.5.2's password:
Permission denied, please try again.
am0165@192.168.5.2's password:
Received disconnect from 192.168.5.2 port 22:2: Too many authentication failures
Connection to 192.168.5.2 closed by remote host.
Connection to 192.168.5.2 closed.
odroid@odroid:~$
```

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

28.

```
#auth required pam_google_authenticator.so nullok
```

29.

```
root@odroid:~# service sshd restart
root@odroid:~#
```

30.

```
odroid@odroid:~$ hydra -l am0165 -P password.txt ssh://192.168.5.2 -s 22
Hydra v8.1 (c) 2014 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 2021-04-04 16:38:11
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 11 tasks per 1 server, overall 64 tasks, 11 login tries (l:1/p:11), ~0 tries per task
[DATA] attacking service ssh on port 22
[22][ssh] host: 192.168.5.2 login: am0165 password: odroid
```

31.

Yes I was able to run hydra and guess the correct password.

```
root@odroid:~# sudo apt-get remove 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 libqrencode3
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  libpam-google-authenticator
0 upgraded, 0 newly installed, 1 to remove and 86 not upgraded.
After this operation, 103 kB disk space will be freed.
Do you want to continue? [Y/n] y
```

32.