

PCAP ANALYSIS LAB

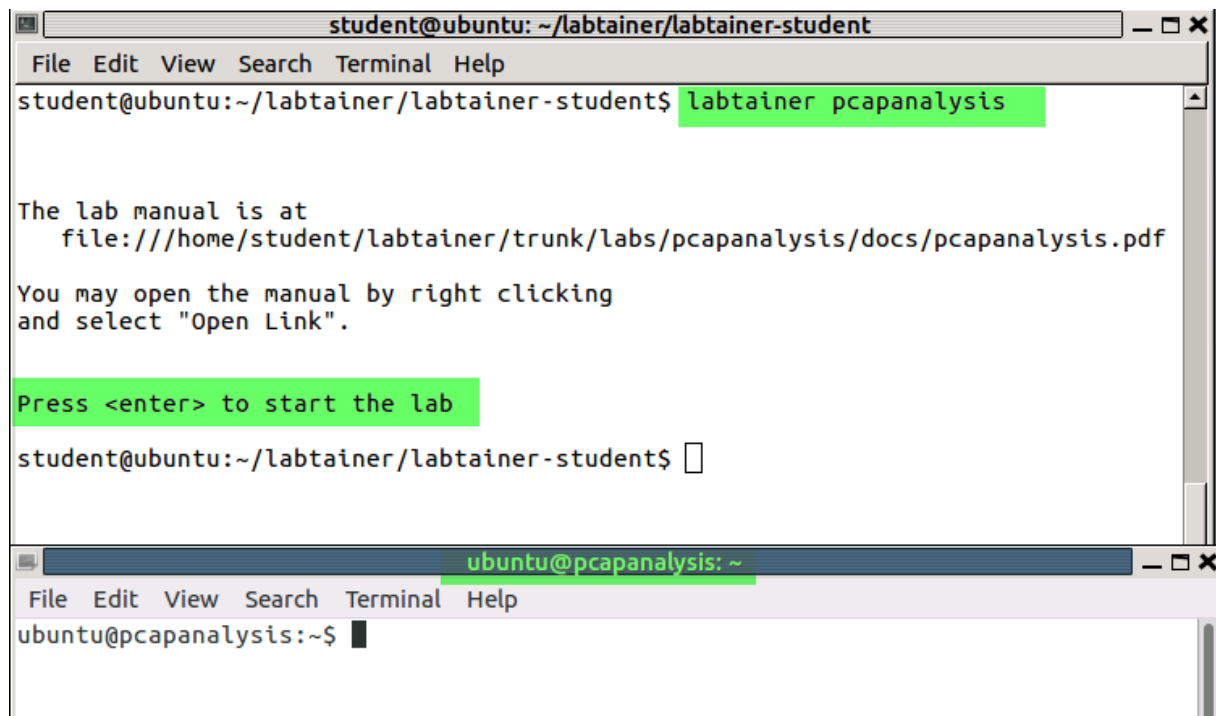
Overview

This lab introduces the analysis of PCAP files using the Tshark tool. You will analyze an existing PCAP file, looking for a specific invalid login attempt. PCAP stands for “packet capture”, and is a standard file format for storing traffic recorded from a network.

Performing the lab

The lab is started from the labtainer working directory on your Linux host e.g., a Linux VM. From there, issue the command:

```
labtainer pcapanalysis
```



The resulting virtual terminal is connected to a computer that contains the PCAP of interest.

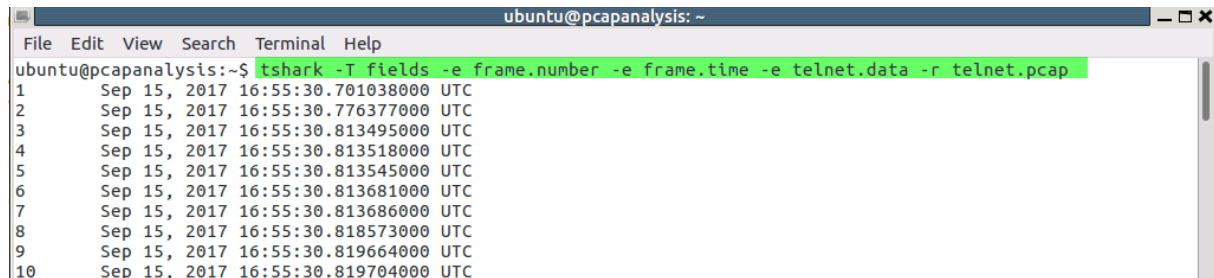
Tasks

1. run tshark to perform PCAP Analysis

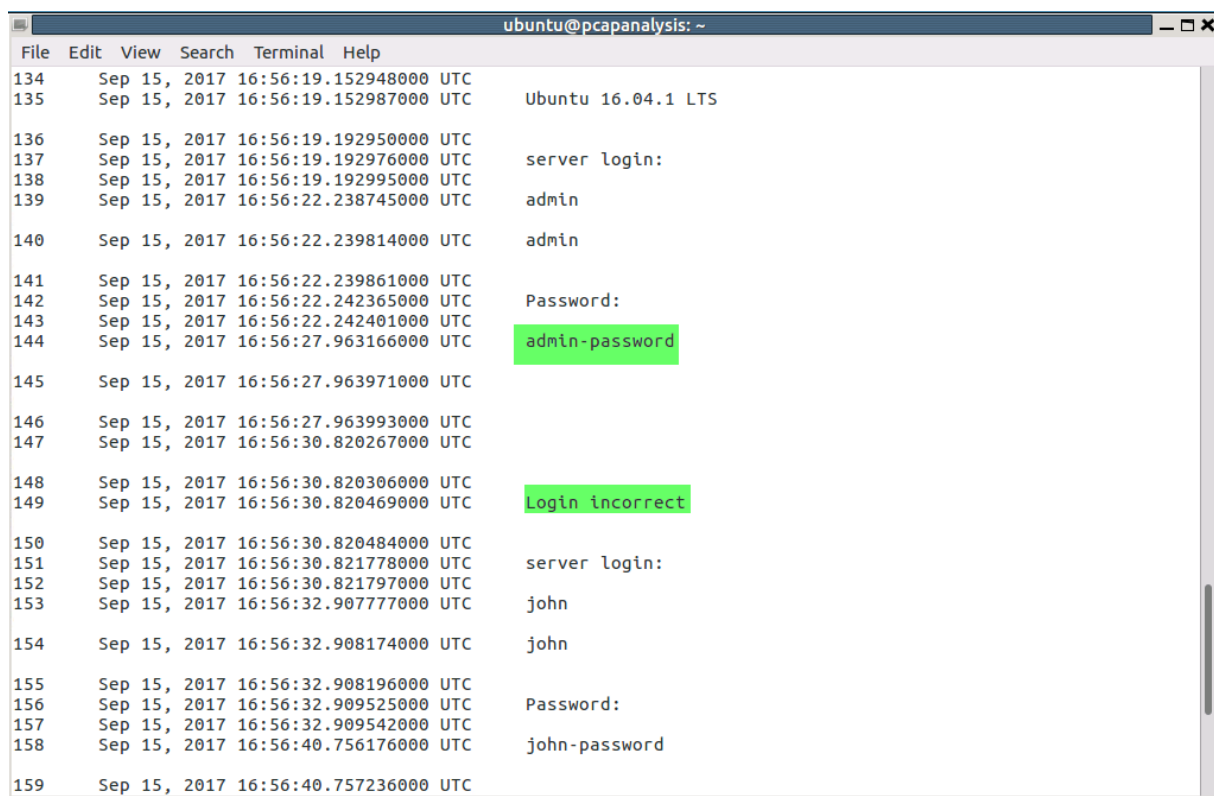
- A) To see various options available for tshark, do:
man tshark

B) Sample Tshark command to display specific fields:

```
tshark -T fields -e frame.number -e frame.time -e telnet.data -r telnet.pcap
```



```
ubuntu@pcapanalysis: ~  
File Edit View Search Terminal Help  
ubuntu@pcapanalysis:~$ tshark -T fields -e frame.number -e frame.time -e telnet.data -r telnet.pcap  
1 Sep 15, 2017 16:55:30.701038000 UTC  
2 Sep 15, 2017 16:55:30.776377000 UTC  
3 Sep 15, 2017 16:55:30.813495000 UTC  
4 Sep 15, 2017 16:55:30.813518000 UTC  
5 Sep 15, 2017 16:55:30.813545000 UTC  
6 Sep 15, 2017 16:55:30.813681000 UTC  
7 Sep 15, 2017 16:55:30.813686000 UTC  
8 Sep 15, 2017 16:55:30.818573000 UTC  
9 Sep 15, 2017 16:55:30.819664000 UTC  
10 Sep 15, 2017 16:55:30.819704000 UTC
```



```
ubuntu@pcapanalysis: ~  
File Edit View Search Terminal Help  
134 Sep 15, 2017 16:56:19.152948000 UTC  
135 Sep 15, 2017 16:56:19.152987000 UTC Ubuntu 16.04.1 LTS  
  
136 Sep 15, 2017 16:56:19.192950000 UTC  
137 Sep 15, 2017 16:56:19.192976000 UTC server login:  
138 Sep 15, 2017 16:56:19.192995000 UTC admin  
139 Sep 15, 2017 16:56:22.238745000 UTC admin  
  
140 Sep 15, 2017 16:56:22.239814000 UTC  
  
141 Sep 15, 2017 16:56:22.239861000 UTC  
142 Sep 15, 2017 16:56:22.242365000 UTC Password:  
143 Sep 15, 2017 16:56:22.242401000 UTC admin-password  
144 Sep 15, 2017 16:56:27.963166000 UTC  
  
145 Sep 15, 2017 16:56:27.963971000 UTC  
  
146 Sep 15, 2017 16:56:27.963993000 UTC  
147 Sep 15, 2017 16:56:30.820267000 UTC  
  
148 Sep 15, 2017 16:56:30.820306000 UTC  
149 Sep 15, 2017 16:56:30.820469000 UTC Login incorrect  
  
150 Sep 15, 2017 16:56:30.820484000 UTC  
151 Sep 15, 2017 16:56:30.821778000 UTC server login:  
152 Sep 15, 2017 16:56:30.821797000 UTC john  
153 Sep 15, 2017 16:56:32.907777000 UTC john  
  
154 Sep 15, 2017 16:56:32.908174000 UTC  
  
155 Sep 15, 2017 16:56:32.908196000 UTC  
156 Sep 15, 2017 16:56:32.909525000 UTC Password:  
157 Sep 15, 2017 16:56:32.909542000 UTC john-password  
158 Sep 15, 2017 16:56:40.756176000 UTC  
  
159 Sep 15, 2017 16:56:40.757236000 UTC
```

NOTE: this command should be issued as one line

2. display the single packet containing invalid “admin” password

Locate the single frame containing the password provided when the user attempted to login as the “admin” user.

Use Tshark to display just this frame by using the `-Y frame.number==N` option.
Note, N is the frame number.

```
ubuntu@pcapanalysis:~$ tshark -T fields -Y frame.number==149 -e frame.time -e telnet.data -r telnet.pcap
Sep 15, 2017 16:56:30.820469000 UTC Login incorrect
ubuntu@pcapanalysis:~$
```

Labtainers

Stop the labtainer

When the lab is completed, or you would like to stop working for a while, run

`stoplab`

```
student@ubuntu:~/labtainer/labtainer-student$ stoplab
Results stored in directory: /home/student/labtainer_xfer/pcapanalysis
```

```
student@ubuntu:~/labtainer/labtainer-student$ checkwork pcapanalysis
pcapanalysis lab is not running, looking for previous results...
pulling labtainer.grader from mftthomps
Done with pull
[2018-11-24 07:31:41,423 - ERROR : gradelab:207 - autoGrade() ] trouble with docker exec pcapan
alysis-igrader bash -c 'su - instructor -c "cd;./local/bin/instructor.py"'
Error: No such container:path: pcapanalysis-igrader:/home/instructor/pcapanalysis.grades.txt
Error: No such container:path: pcapanalysis-igrader:/home/instructor/pcapanalysis.grades.json
No grades.txt file at /home/student/labtainer_xfer/pcapanalysis
student@ubuntu:~/labtainer/labtainer-student$
```

from the host labtainer working directory. You can always restart the labtainer to continue your work. When the labtainer is stopped a zip file is created and copied to a location displayed by the `stoplab` command. When the lab is completed, send that zip to the instructor.