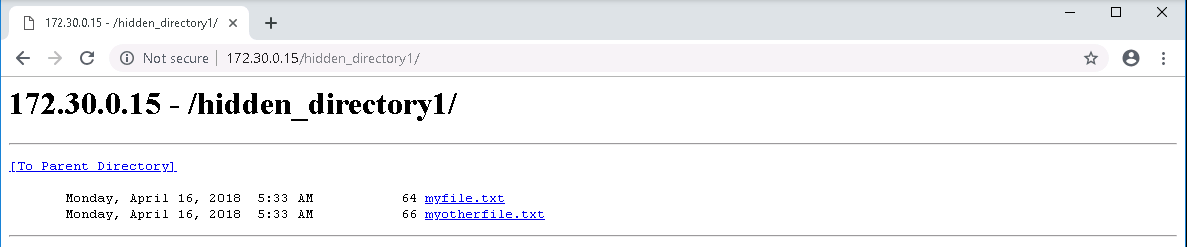
# Cybersecurity

## Activity 2.2.2 Server Vulnerabilities

Copy and paste screenshots and/or answer questions from the activity.

#3

d. Save a screenshot of the directory as evidence.



#7 Navigate to the Local Disk C:\ drive (refer to Figure 1 above if necessary) and open the

inetpub directory within it.

1. Document the directory structure within the inetpub folder listing the following in

particular; you will need them later in this activity:

* + The names of subfolders and files in inetpub
    1. Custerr
    2. Ftproot
    3. Hidden\_directory1
    4. History
    5. Logs
    6. Mailroot
    7. temp
    8. wwwroot
  + The names of the files in wwwroot
    1. Iisstart.html
    2. Iisstart.png
    3. Web.config

1. Explain how the contents of the hidden\_directory1 folder relate to the screenshot

you took in step 3d.

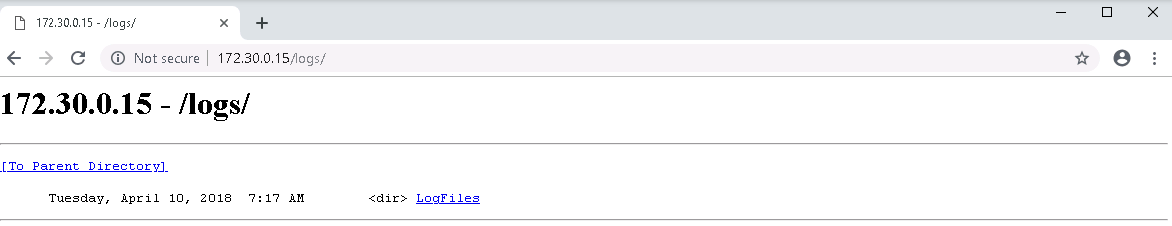
they are the same

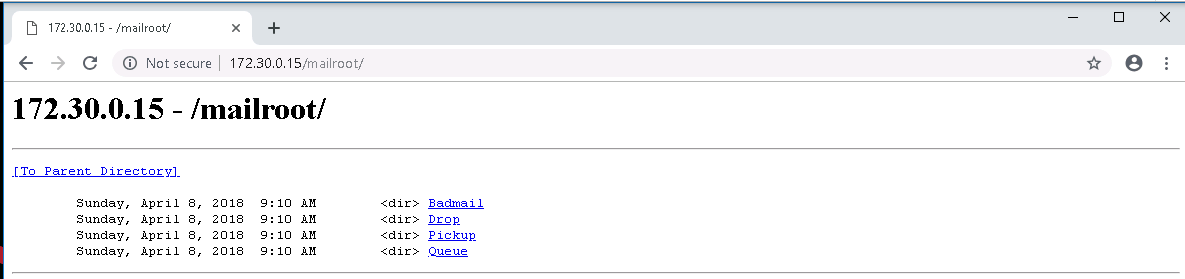
1. Explain why hidden\_directory2 caused an error in step 3.

It does not exist

#9 Craft two of your own forceful browsing addresses and try them out in the Chrome

browser on the login machine.

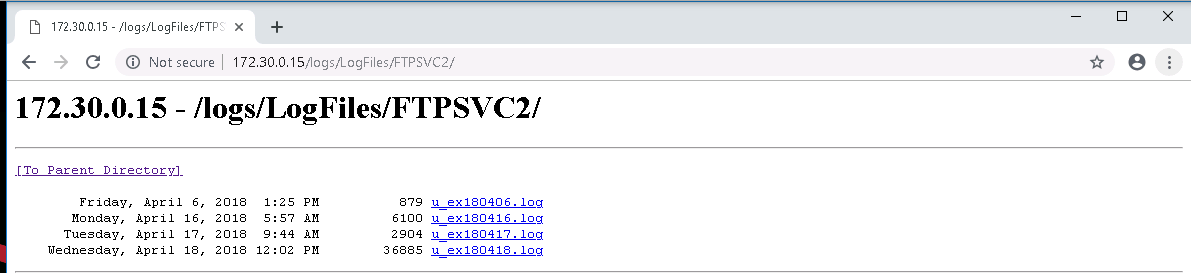




#12 Record what you see.

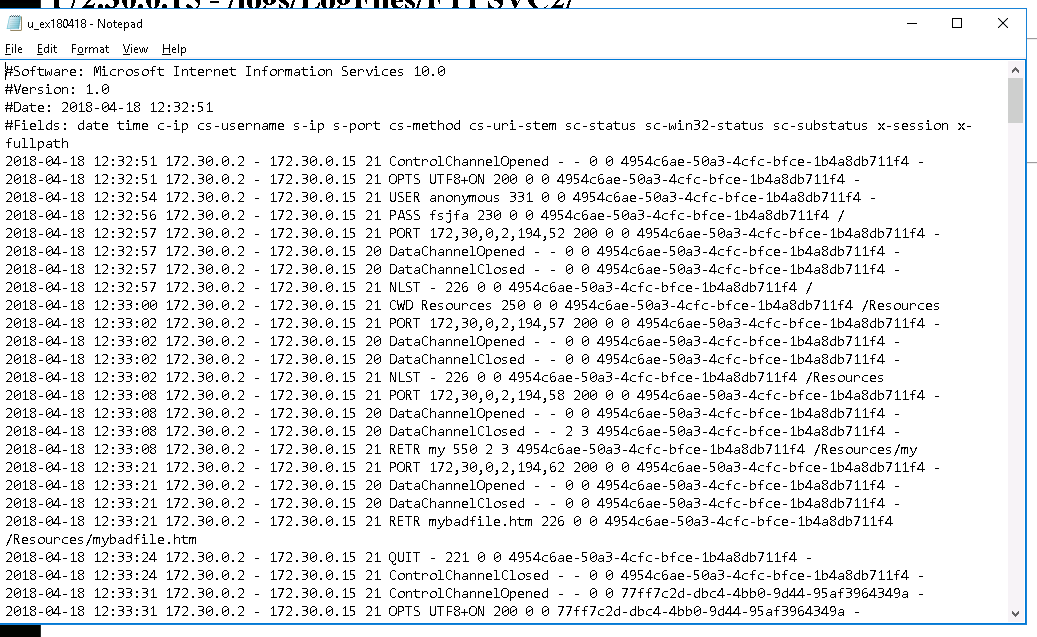
1. Are there sub-directories? If so, can you navigate inside of them?
   1. Yes, logs/LogFiles/{directory}
2. What files can you see? Record their type(s).
   1. “Weird Name”.log
3. Save a screenshot of your browser as evidence of your ability to access the log

file directory.



1. Browsers cannot display log files, but the files can be downloaded. Download

and open a log file.

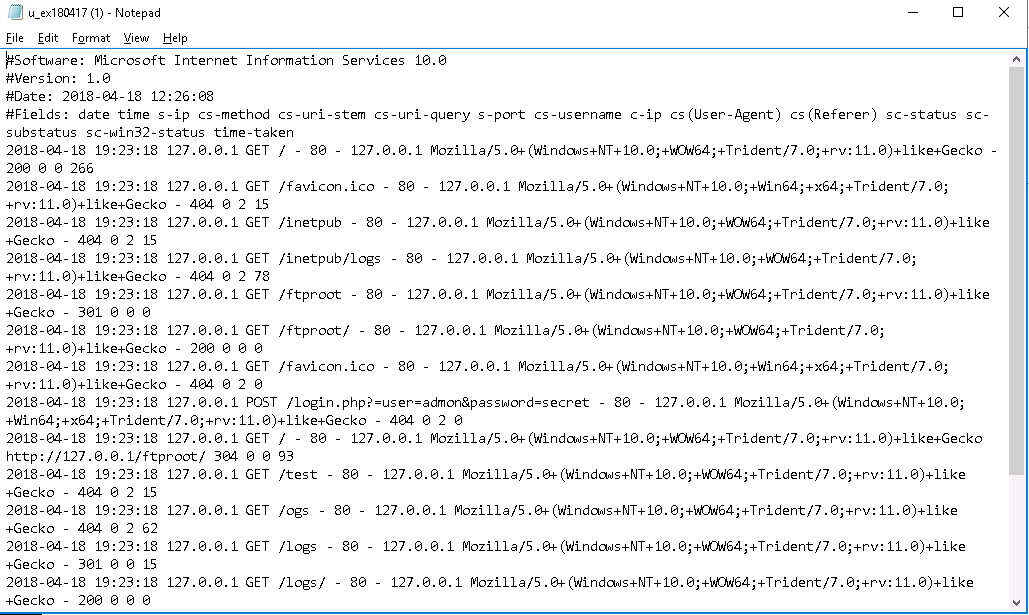


1. In one of the log files, there’s information that would be very valuable to a

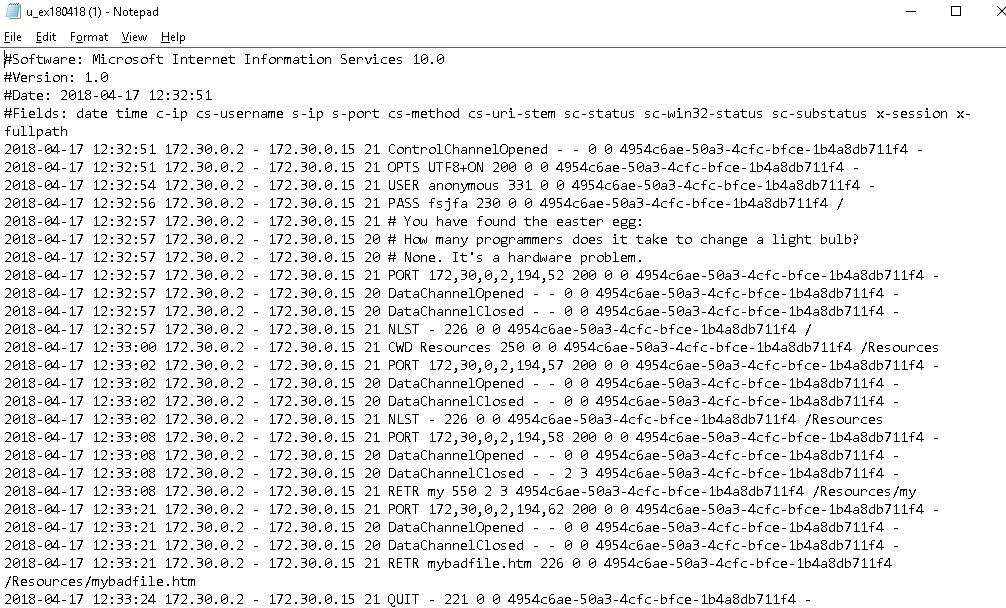
malicious hacker. What is the file and what does it contain?

User=admin & password=secret

1. Save a screenshot as evidence of your ability to access the log file.



Screenshot the “easter egg”…did you find it??



#16

1. What does this tell you about the web server?

This tells us about the webserver all the files that are inside it and the access and uploads to them

1. Save a screenshot of the result as evidence.
   1. I REALLY DON’T WANT TO BOOT UP THE CYBER LAB SORRY!!!!!

#18 Find and save a screenshot of any malicious content as evidence.

I REALLY DON’T WANT TO BOOT UP THE CYBER LAB SORRY!!!!!