# Cybersecurity

## Activity 2.2.3 Server Analysis

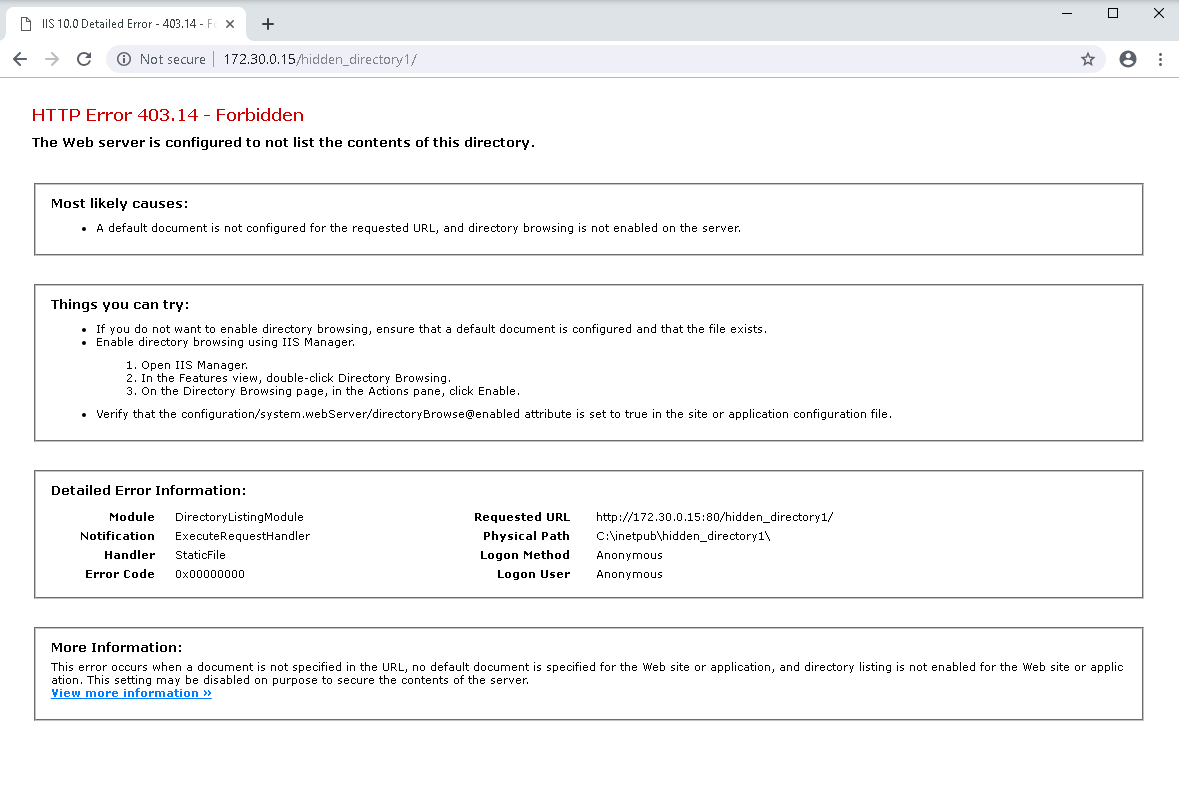
Copy and paste screenshots and/or answer questions from the activity.

#10 On the login machine, use a browser to attempt a forceful browsing of 172.30.0.15.

1. Were you able to get the directory listing?

NOPE

1. Save a screenshot of the result as evidence.



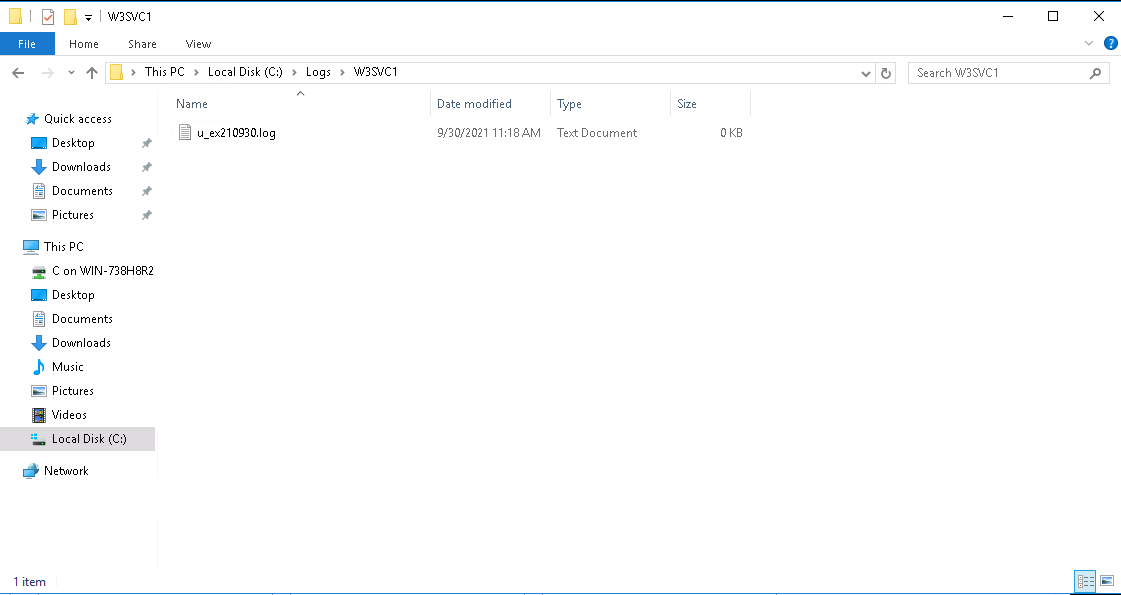
#13 In the Log File section of the center pane, the Directory field defines the location of the

IIS log files. What is it currently set to?



#16

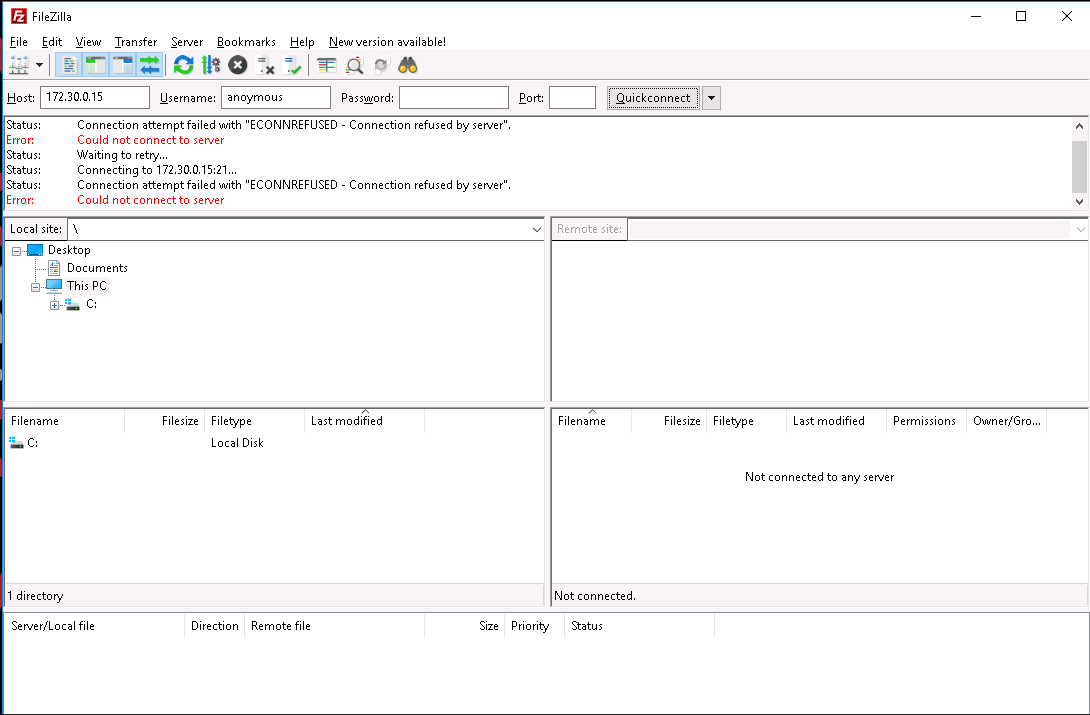
1. In File Explorer on TargetWindows1, find the new location of the log file. It should have today’s date for its Date Modified property.



#30 Check the web site to confirm that FTP access has been disabled.

Were you able to connect and upload a file?

Save a screenshot of the result as evidence.



Write a brief report to describe the remediation strategy you took for each of the three vulnerabilities in this activity. Your report should address the following questions:

1. What vulnerability did you address?
   1. Forceful browsing, and FTP transfer
2. Which admin tool did you use to address this vulnerability?
   1. IIS Server Manager
3. Summarize the configuration changes you made for remediation.
   1. Disabled FTP on the server and disabled directory browsing