# Cybersecurity

## Activity 2.2.4 Secure the Server

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

#2 On your local school computer, do some open research on SMTP to find out what service it provides.

1. What is its primary purpose?

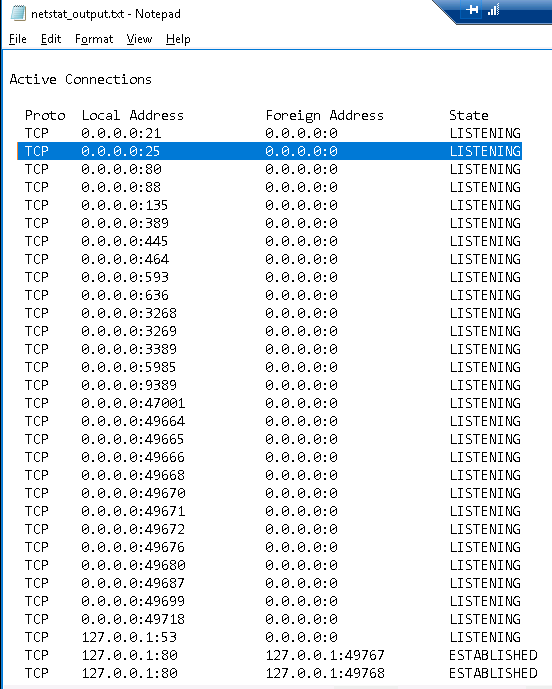
Email service

1. Is it needed for a web server? Why or why not?

No, unless you need to send mail????

#8 Look through netstat\_output.txt to locate the entry associated with the SMTP service. Highlight the entry with your mouse.

Save a screenshot of the result as evidence that the service is currently running.



#9 What can you learn about the web server from the error message displayed in your window?

* The physical path to the web page

#12 Create a plan before you start your remediation.

1. What are all the vulnerabilities you plan on checking for?

SMTP and Error Messages

1. How can each be remediated?

Disable SMTP in IIS Manager

Edit Error Message settings in IIS Manager

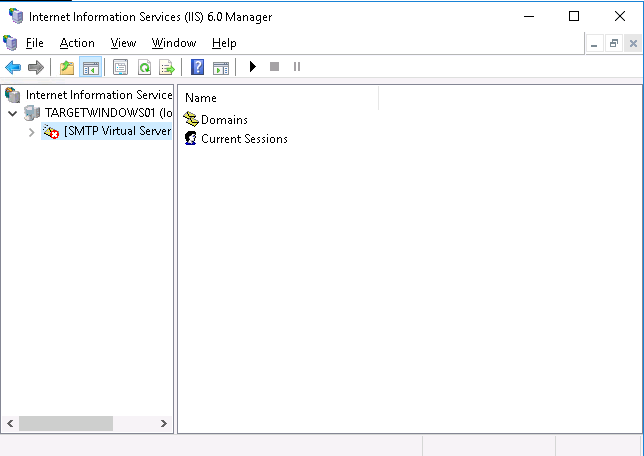
#16 Create documentation of your protection measures.

Include in your documentation:

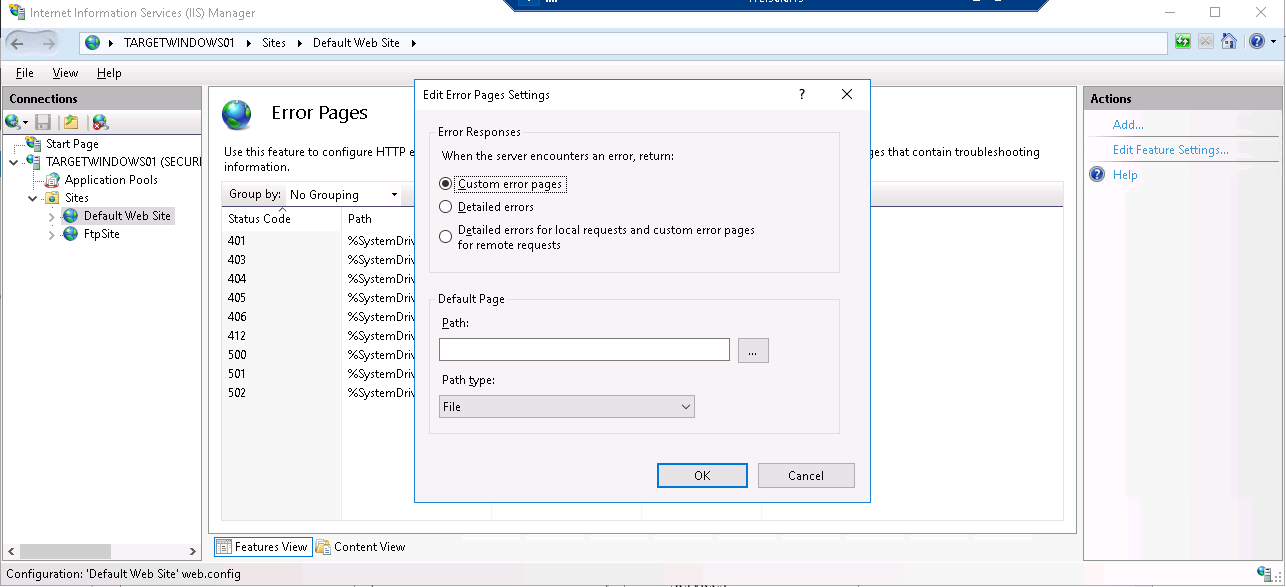
1. The name of the service/feature that you are addressing.
2. An explanation of how you remediated it.

Screenshots to show your remediation work.

SMTP – rt click & stop



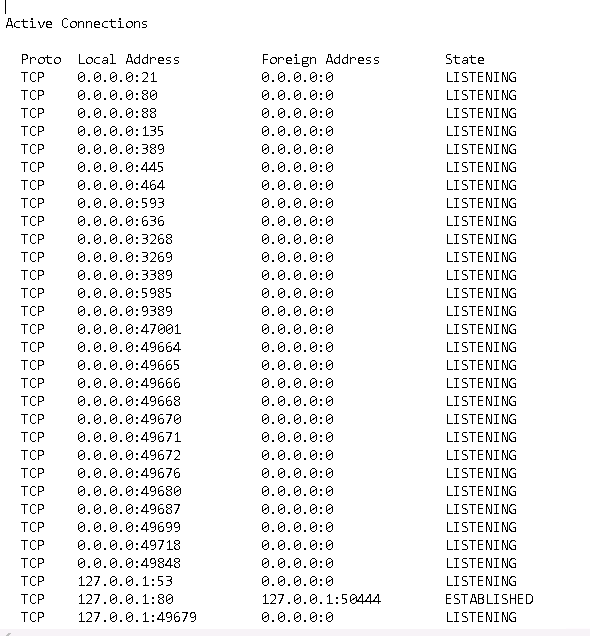
Error Messages – Edit Feature Settings > Custom Error Pages



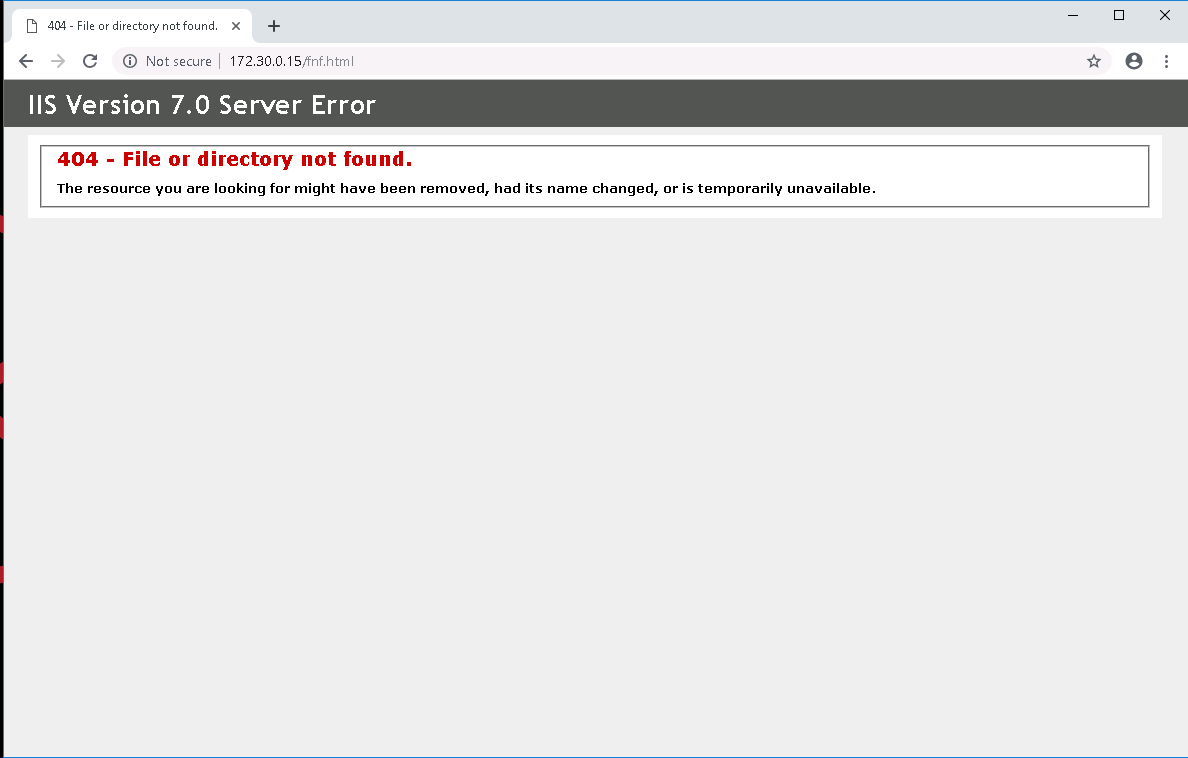
**Verify…**

17-19 Save a screenshot as evidence of each resolution.

1. Run the appropriate utility to make sure SMTP service is no longer running.



1. Using the web browser on the login machine, verify that error messaging is no longer a security weakness.



1. Verify that all additional remediation steps you took have addressed the vulnerabilities that you uncovered.

DONE