Lab 02: Metasploit Framework Fundamentals and Armitage

Marko Shaffer

Information Security, Franklin University

ISEC 325: Comm/Network Security

Professor Rick Rozzell

6 / 20 / 2021

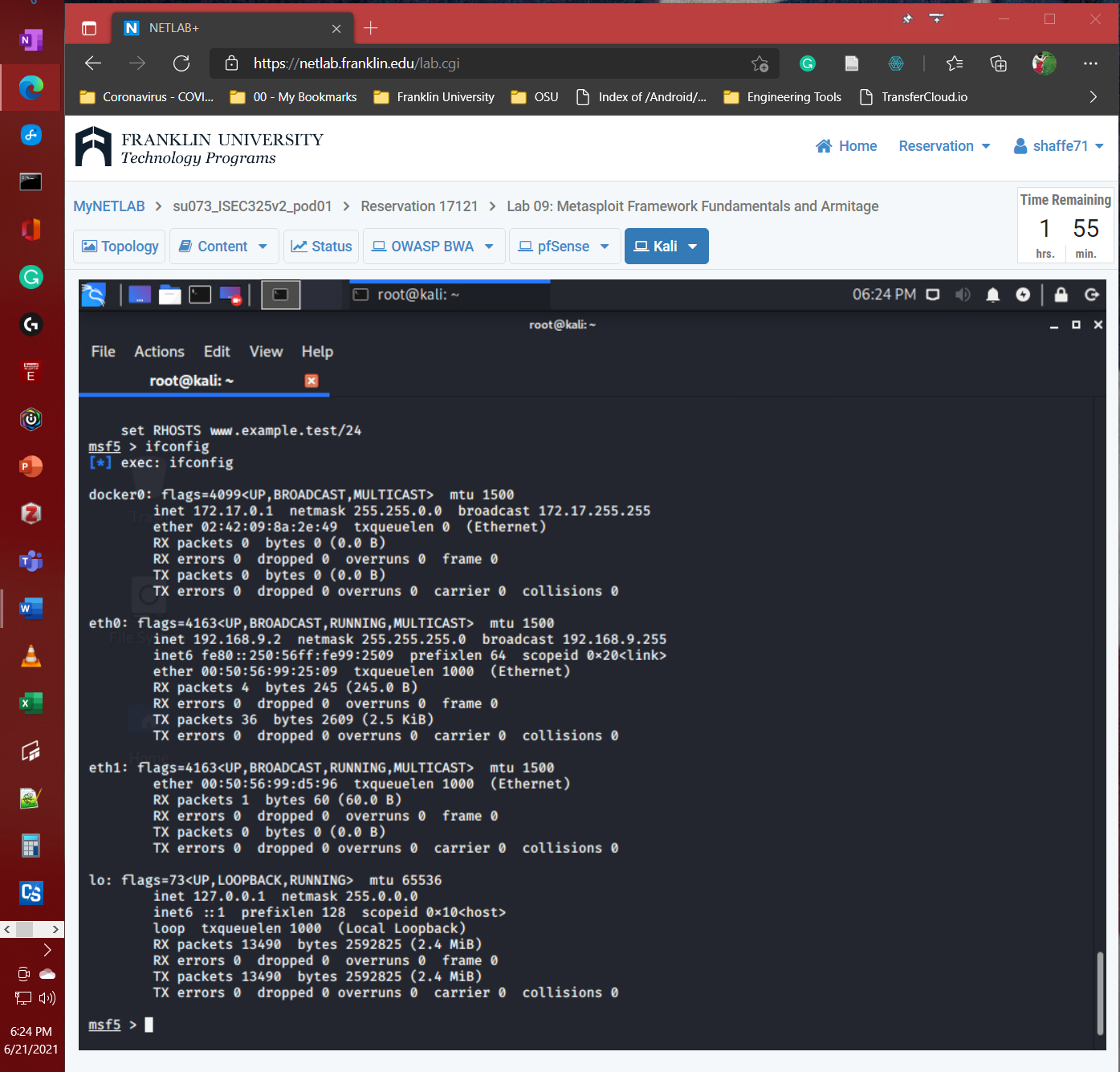
### Lab 02: Metasploit Framework Fundamentals and Armitage

## Follow the instructions from "Lab 09: Metasploit Framework Fundamentals and Armitage."

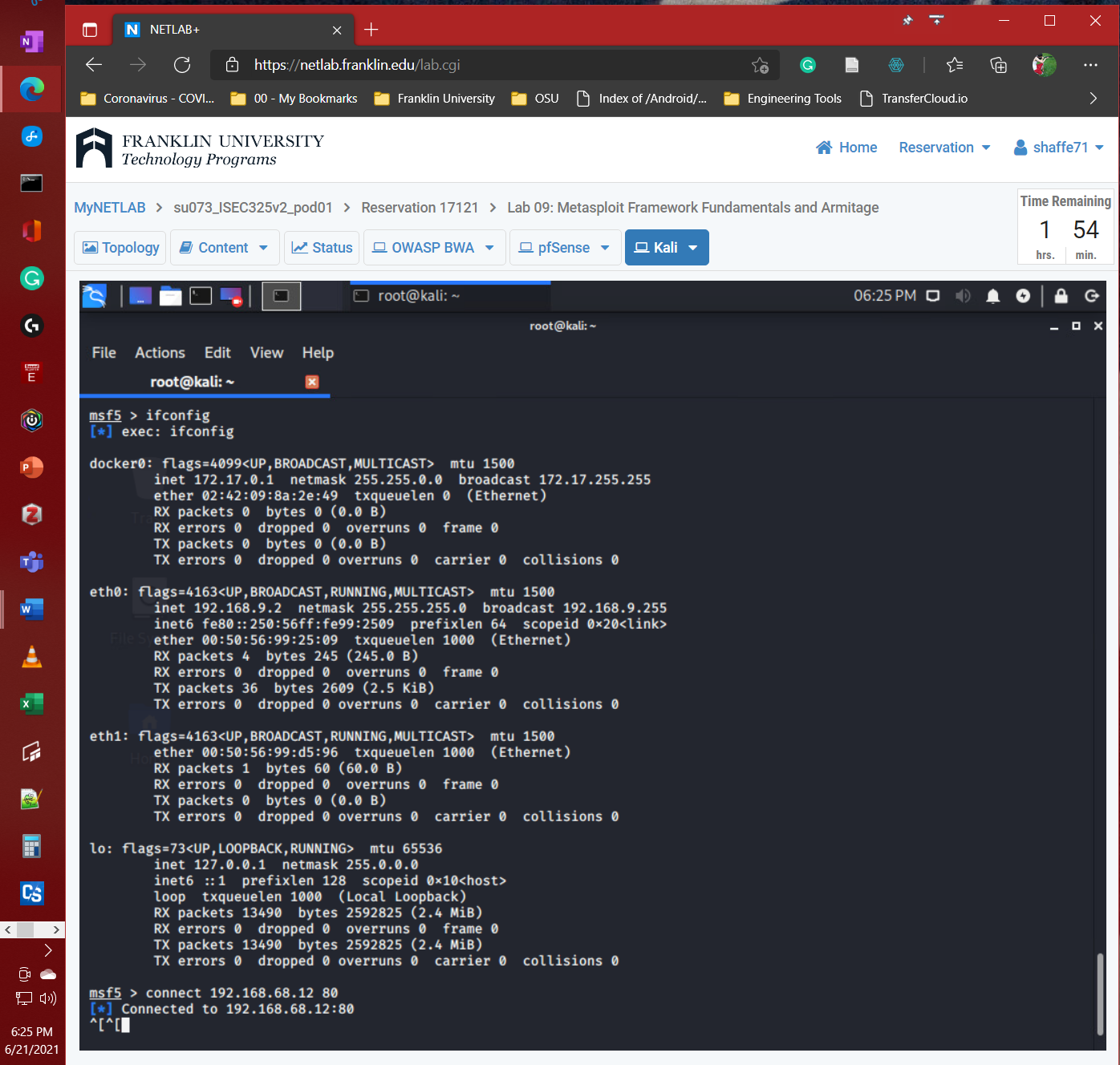
* + Note: For all of the screenshots in the following steps, make sure to include the entire browser window to show that you are logged in to Netlab.

## Start with Section 1, "Getting Familiar with Metasploit," and capture screenshots of the following:

* 1. **Step 11 output**

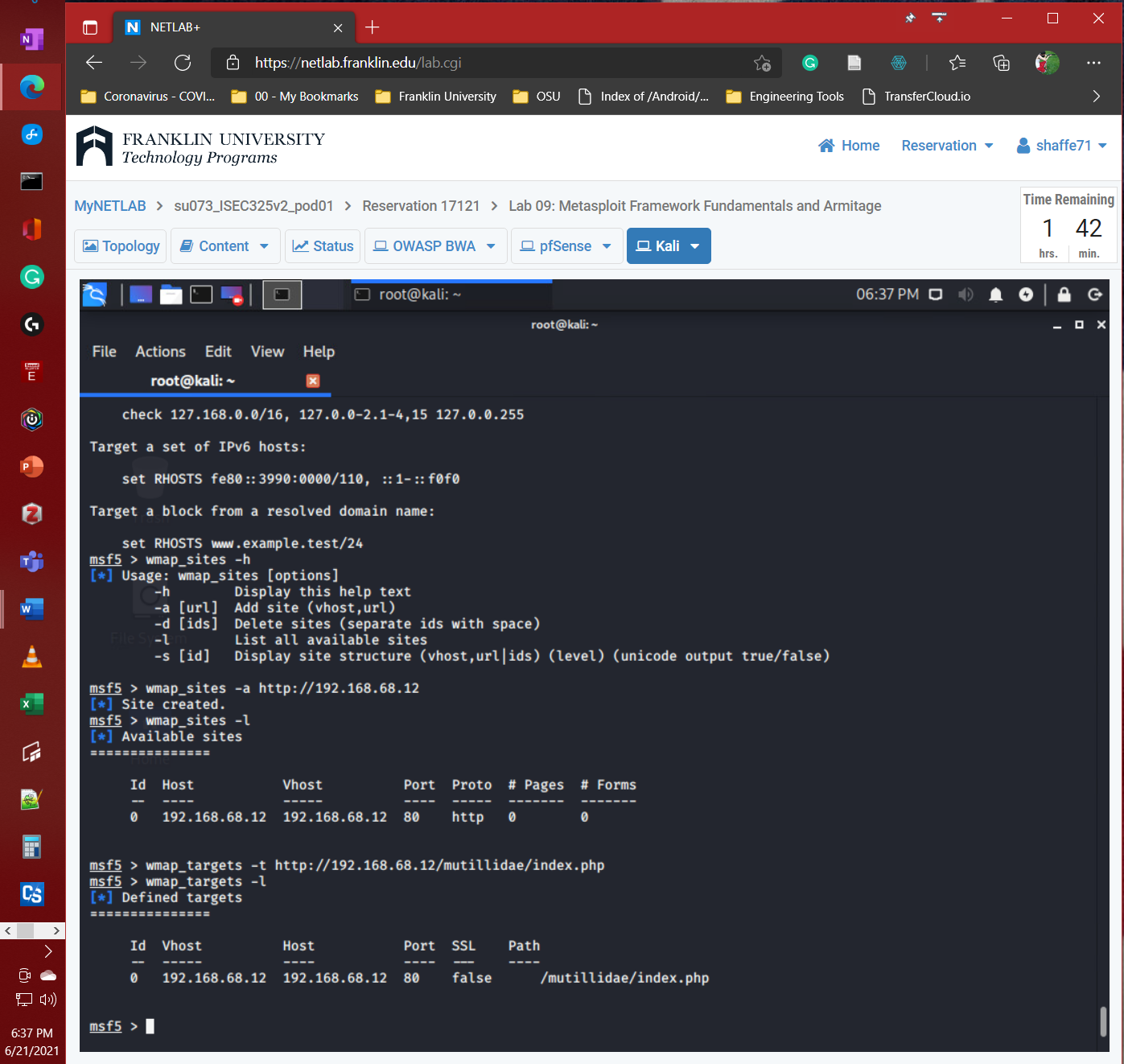


* 1. **Step 12 output**

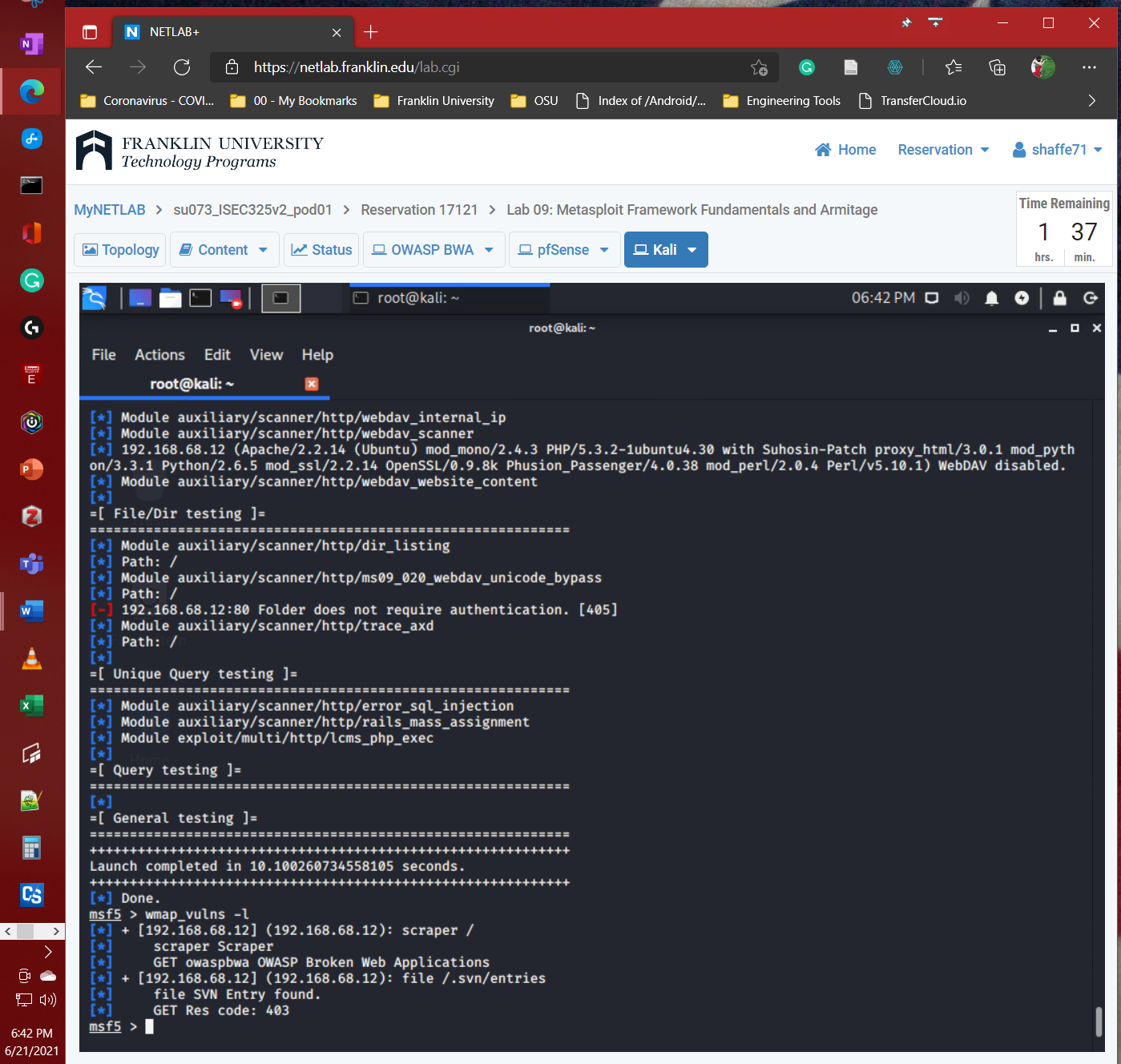


## Continue with Section 2, "Vulnerability Scanning Using the WMAP Module," and capture screenshots of the following:

* 1. **Step 7 output**

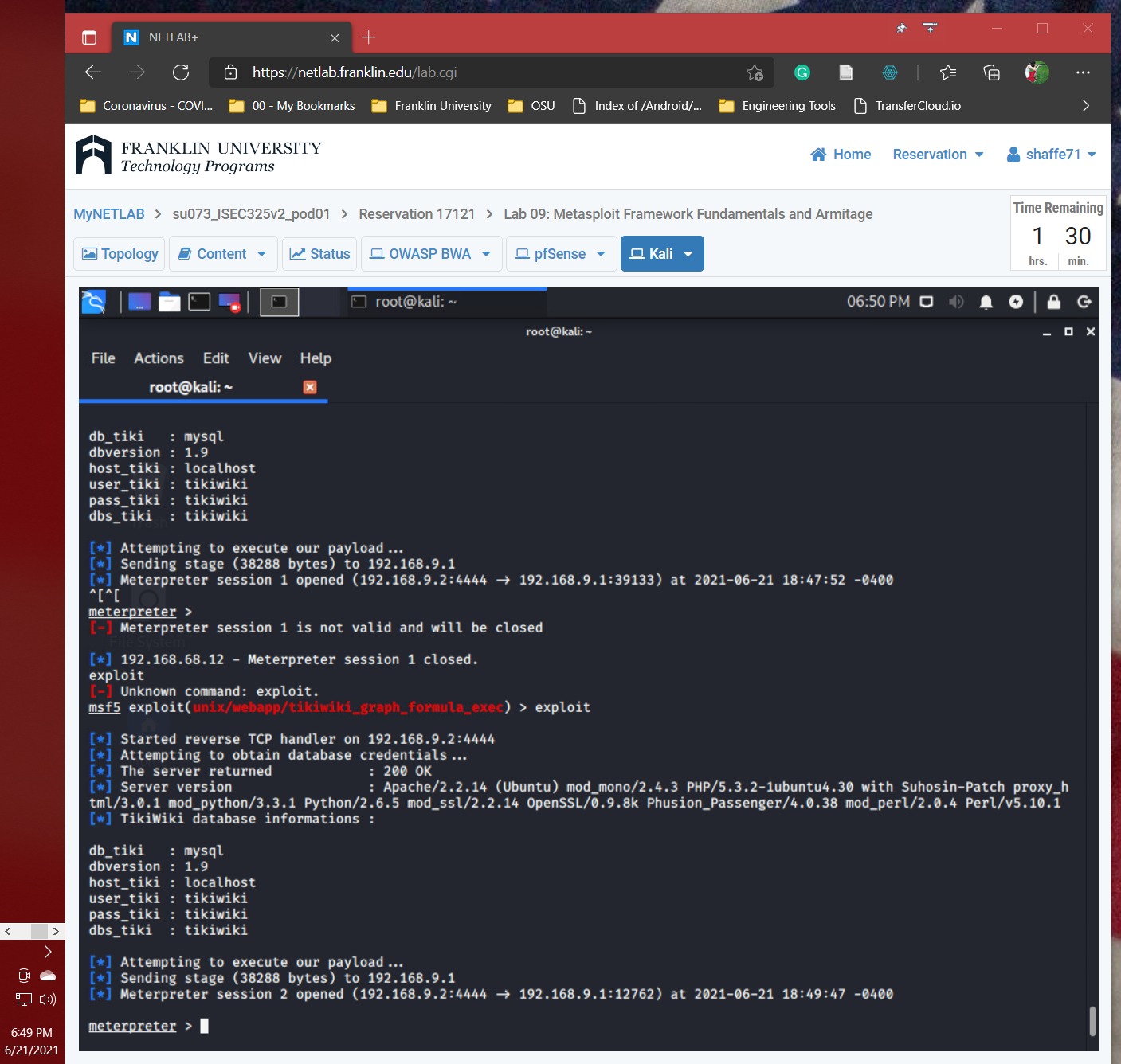


* 1. **Step 12 output**

****

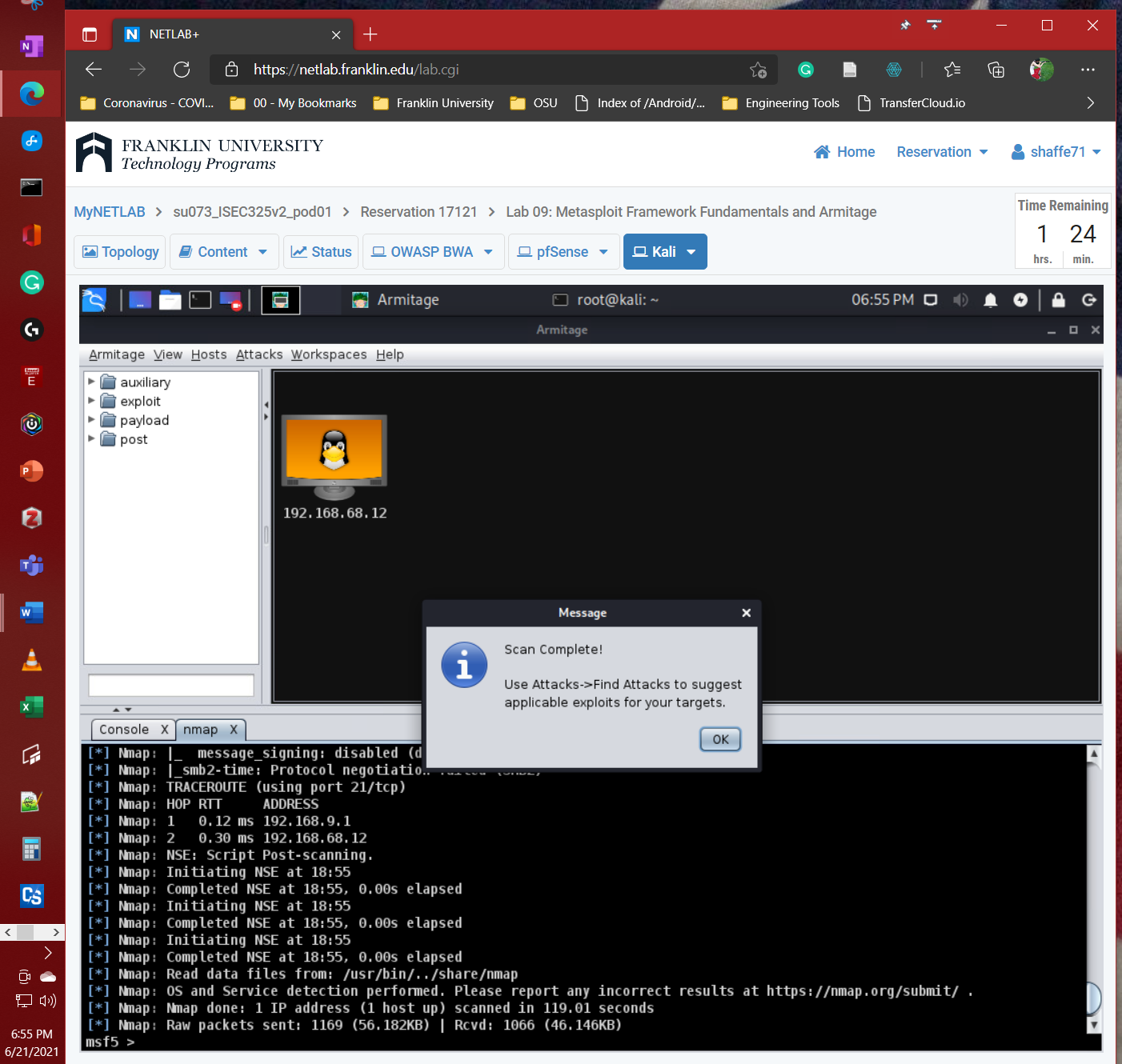
## Continue to Section 3, "Configuring Exploits and Payloads," and capture a screenshot of the following:

* 1. **Step 9 output**



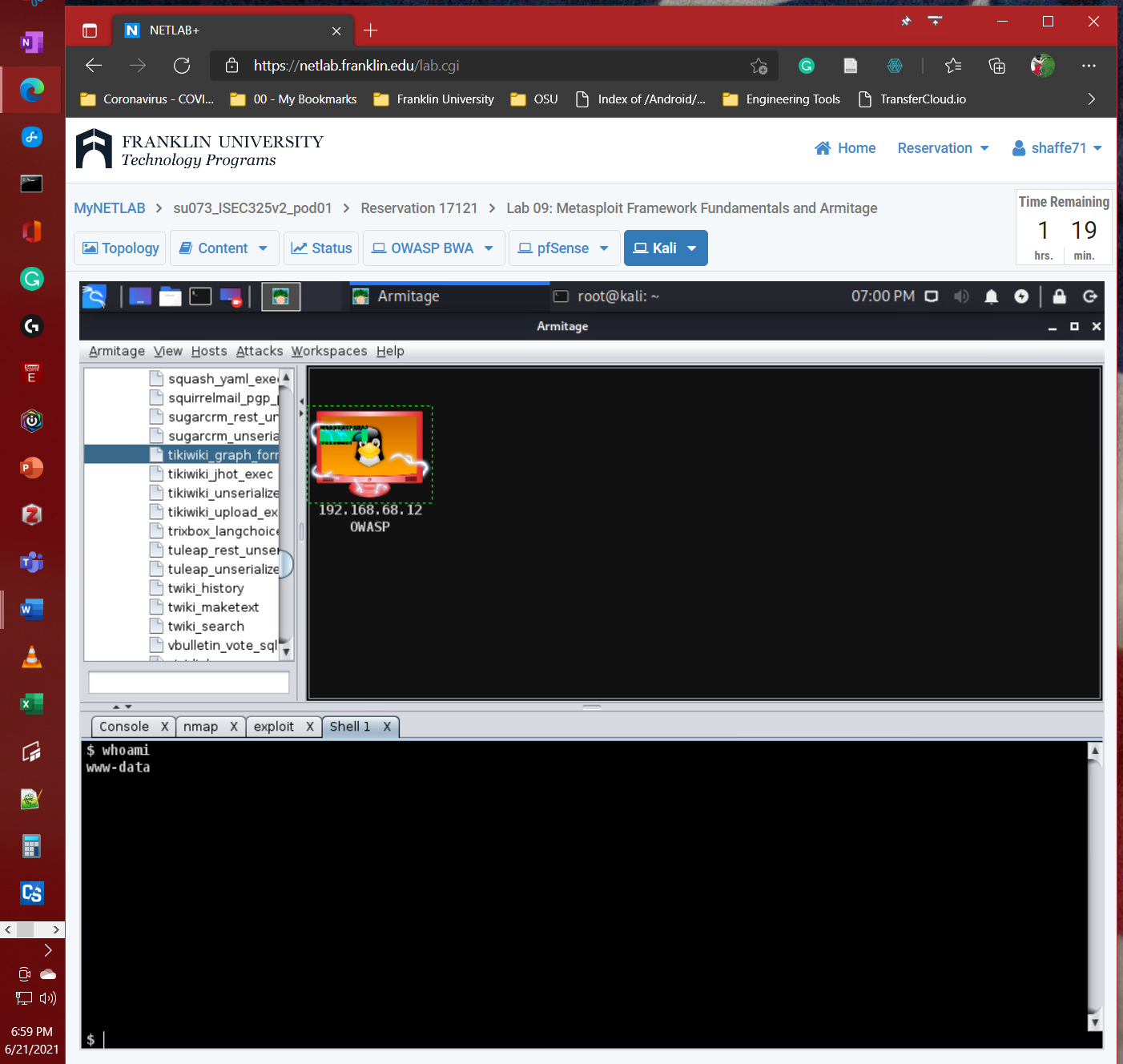
## Continue to Section 4, "Starting Armitage and Scanning Hosts," and capture a screenshot of the following:

* 1. **Step 7 output**

****

## Continue to Section 5, "Finding and Executing Attacks in Armitage," and capture a screenshot of the following:

* 1. **Step 8 output**



## Summary and Reflection: In a few paragraphs, reflect on what you learned through this lab assignment. Was there anything surprising or unexpected? Was there anything worth investigating further?

My previous experience with Metasploit is watching people use it during Def Con conferences. However, I have never set it up before to avoid running something from it that could get me in trouble. We began lab 9 by initializing the Metasploit database is setup then start the Postgres database server. The final step to start working with the Metasploit you must run the console for Metasploit. We then used Netcat to try and connect to the OWASP web server. We then go over the basic command for using Metasploit. Inside Metasploit, they also provide a WMAP plugin tool to run vulnerability scanning. We used WMAP to scan the OWASP web server to find which vulnerability Metasploit has a exploit and payload. The final step was running the found exploit and payload to gain a remote connection to the OWASP web server.

The second part of the lab was using Armitage, which provides a GUI interface to complete the same thing we did through the console. Overall, nothing was surprising or unexpected. I think it would be beneficial to look at Metasploit again in a more in-depth fashion.

# References

Enter Sources Here