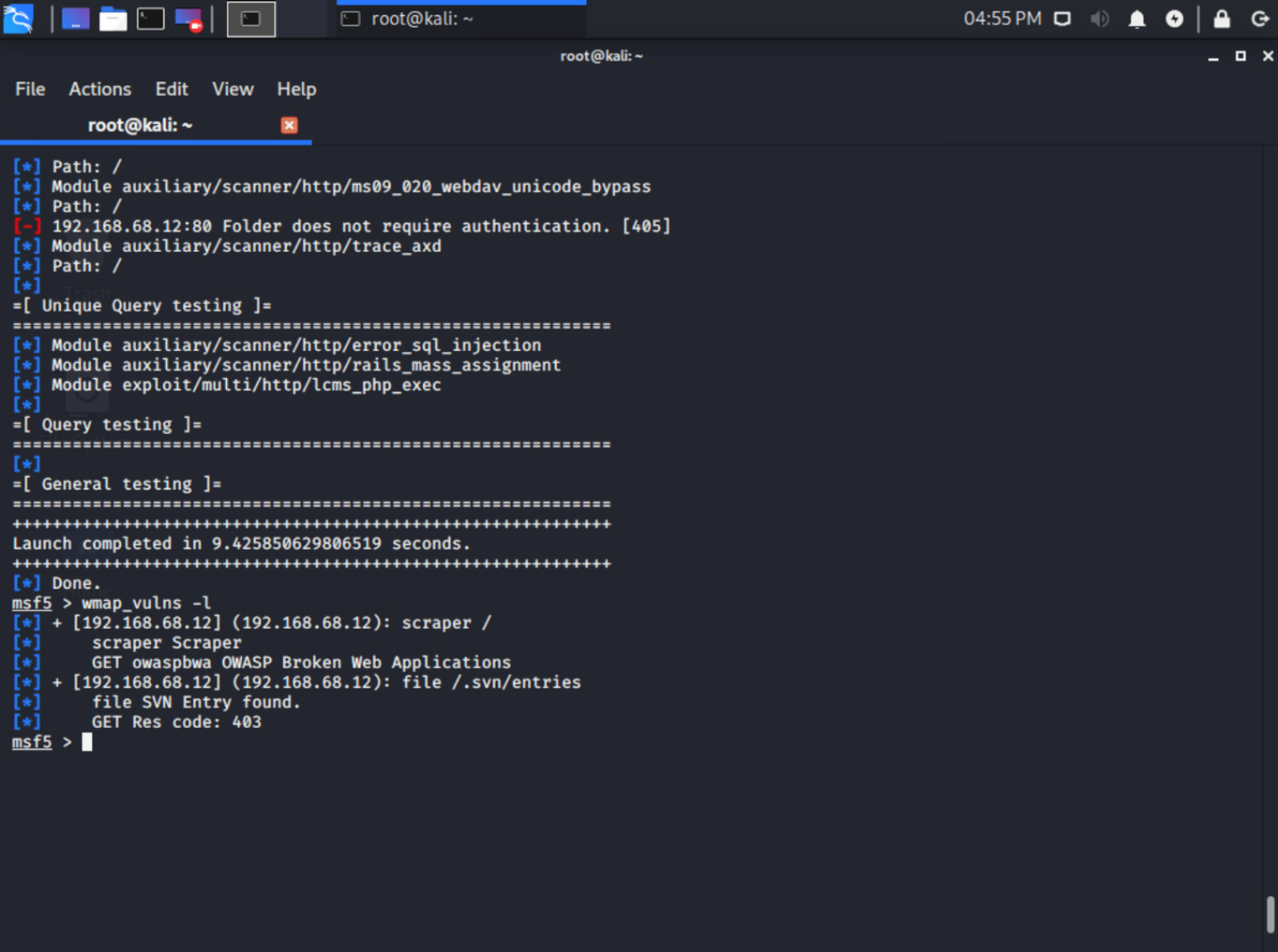
**Section 2, Step 12** – Take a Screenshot of the output from the *wmap\_vulns -l* command below:

**

**Section 3, Step 9** – Take a Screenshot of the output after you run the *exploit* command to start the meterpreter shell below:

A screenshot of a computer

Description automatically generated

**Questions**

1. What is *meterpreter* and what types of things can we do with it at this point? (do some research for more information about it…) Meterpreter is a Metasploit attack payload that allows an attacker to remote into another computer through a terminal window. The command allows for various ports to be used depending on how the payload is configured, so at this point if we have a way to communicate with a target machine, we might be able to gain access to it and send remote commands.
2. What phase of the hacking process would the steps in this lab typically be performed? The phase of the hacking process performed in this lab would be step 2 scanning and step 3 gaining access.