**Lab 4: Using Ethical Hacking Techniques to Exploit A Vulnerable Workstation.**

**By**

**Natnael Kebede**



**University of Dallas**

**2020**

This Paper Submitted in Partial Fulfillment of the Requirements for

CYBS 7359 – Penetration Testing and Vulnerability Assessment

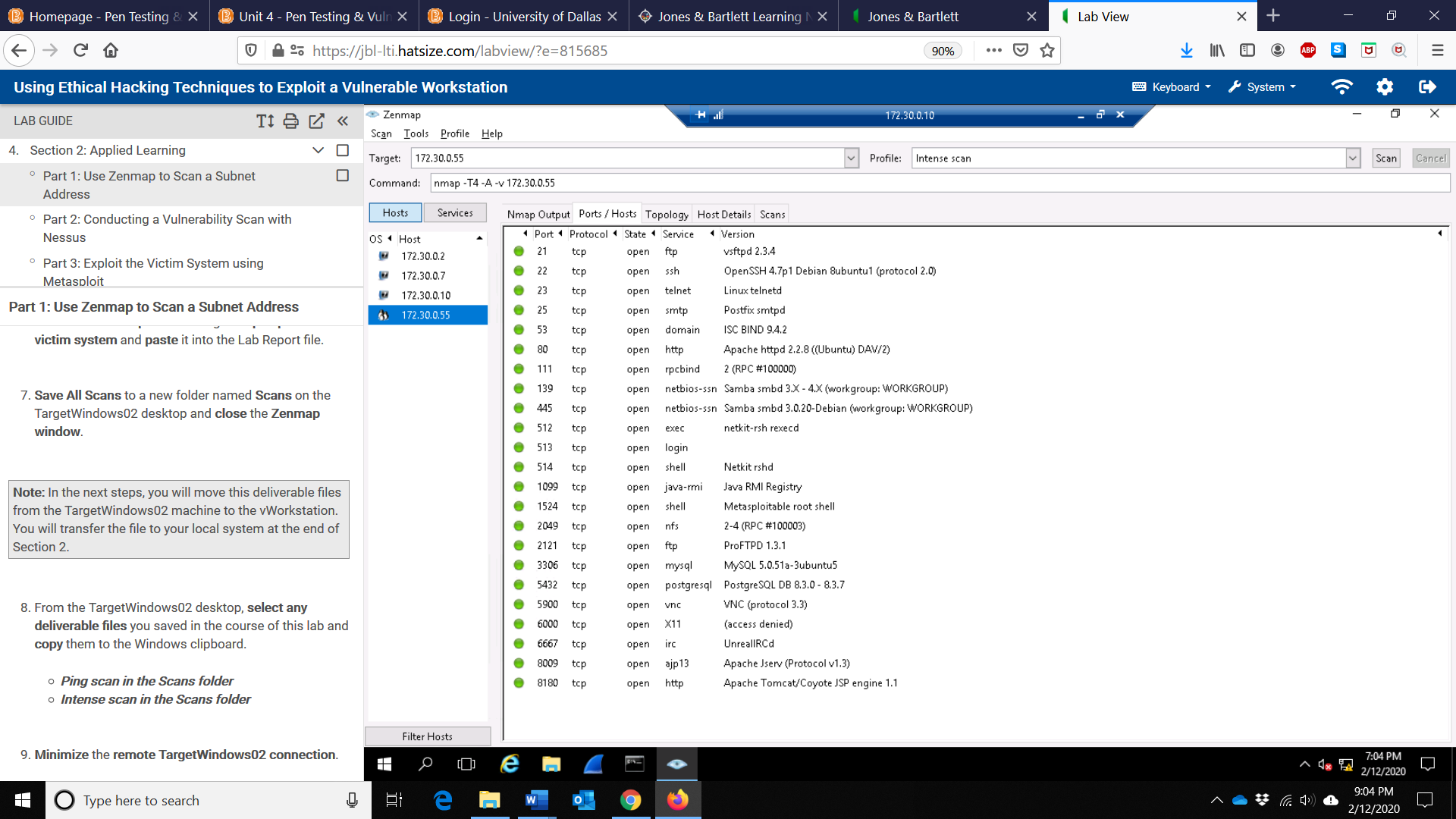
Spring 2020

Presented to Dr. Renita Murimi

**Section 2**

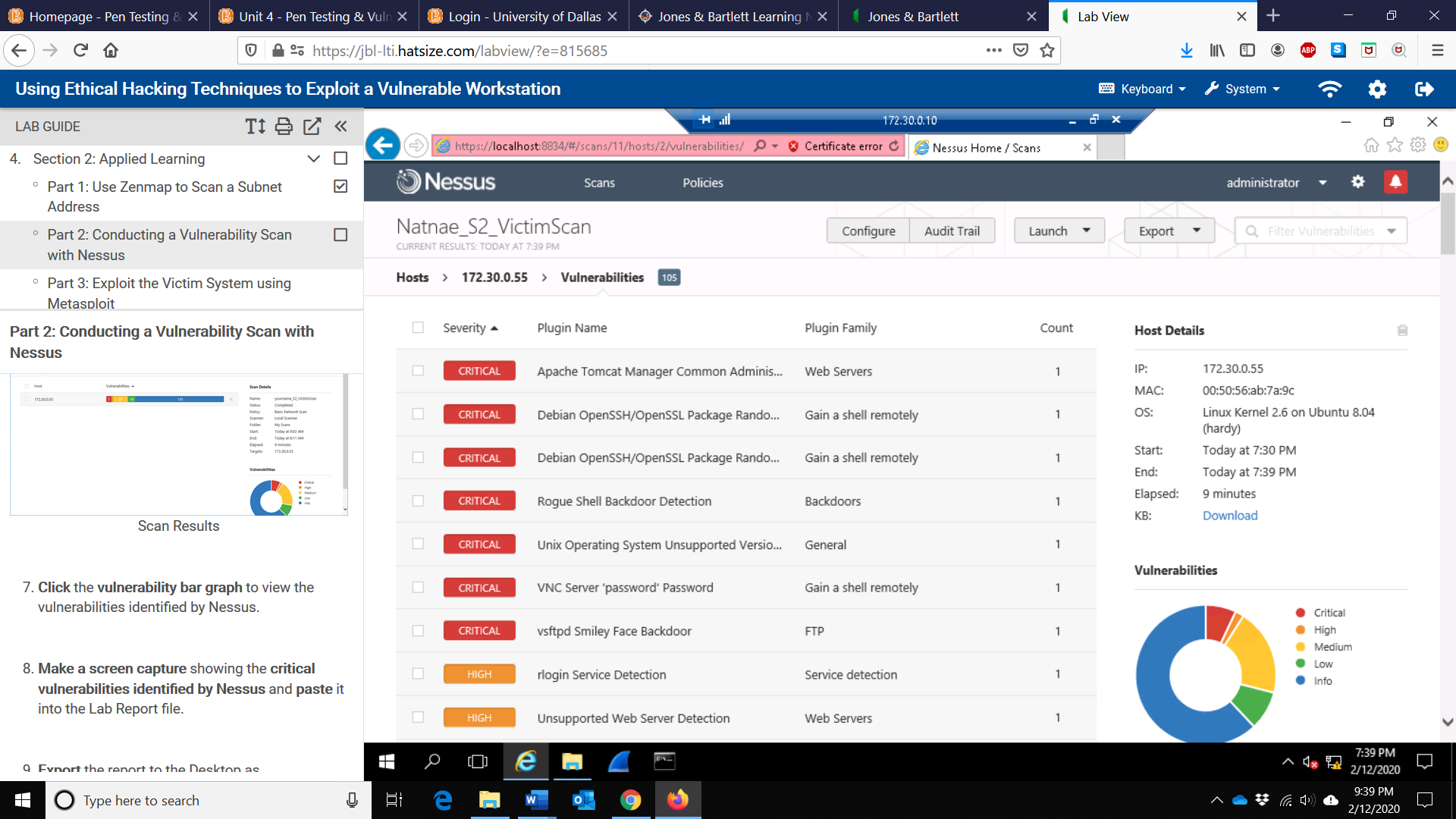
**Part 1**

1. Make a screen capture showing the open ports on the victim system and paste it into the Lab Report file.

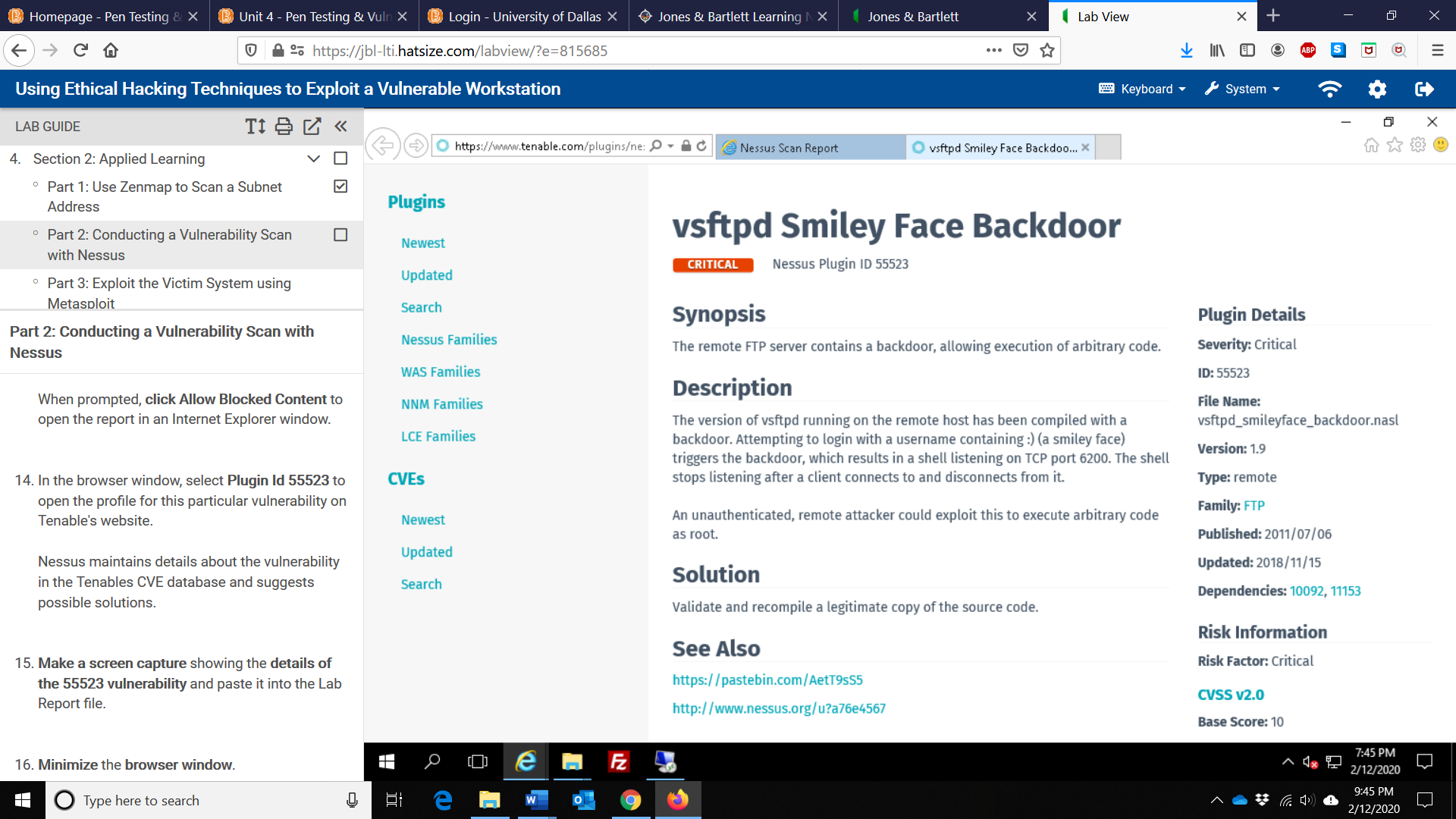


**Part 2**

1. Make a screen capture showing the critical vulnerabilities identified by Nessus and paste it into the Lab Report file.

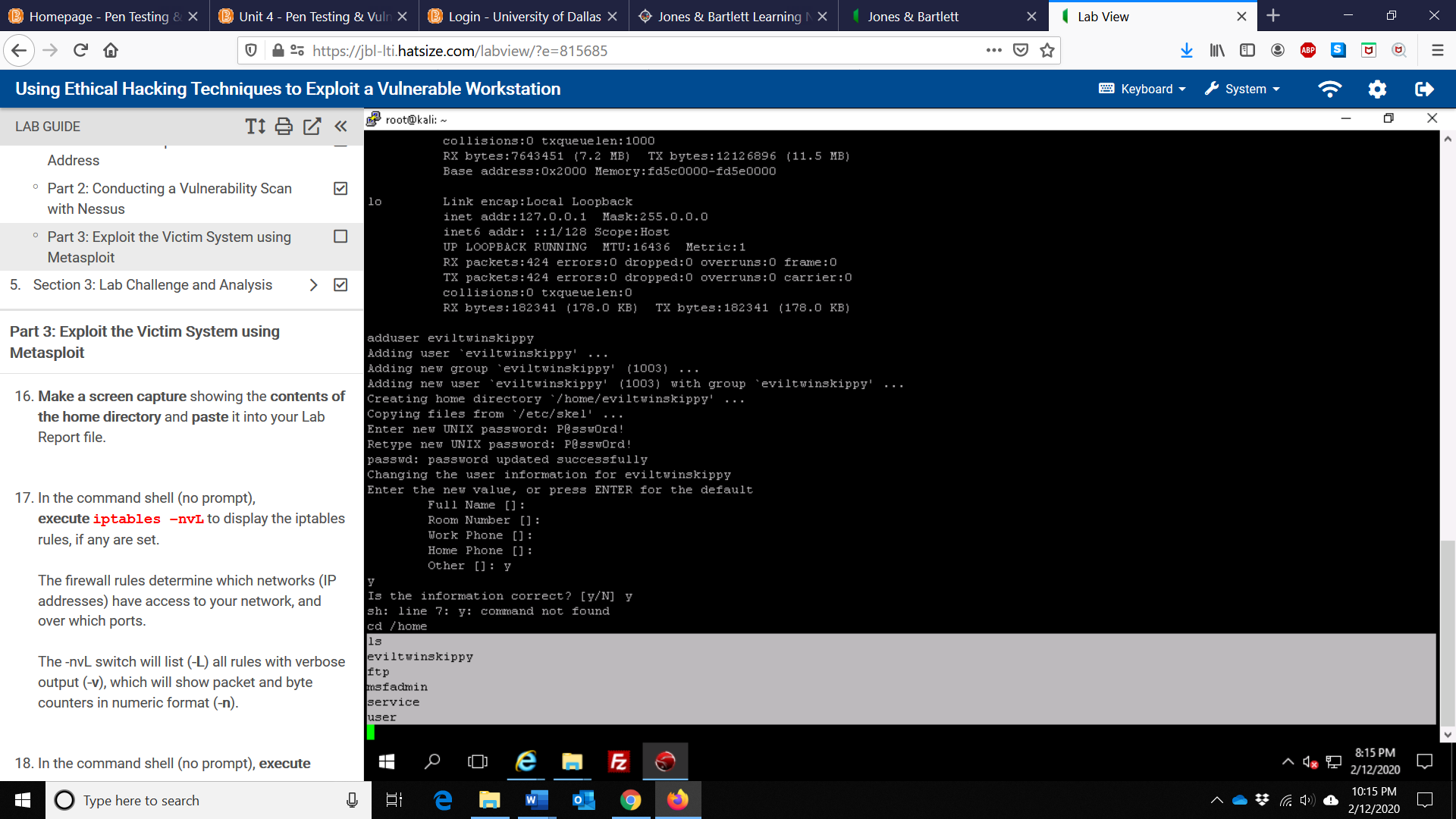


1. Make a screen capture showing the details of the 55523 vulnerability and paste it into the Lab Report file.

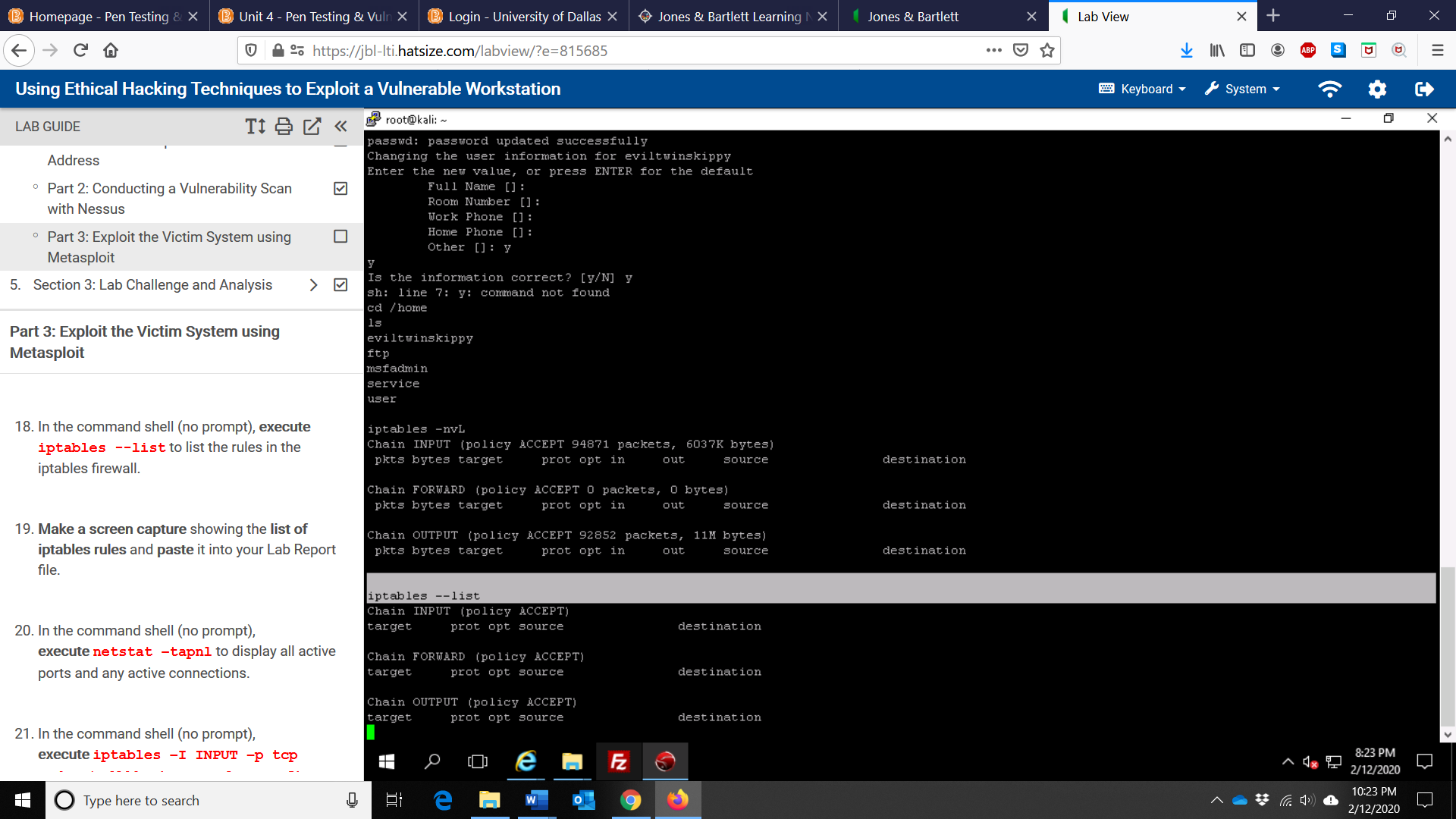


**Part 3**

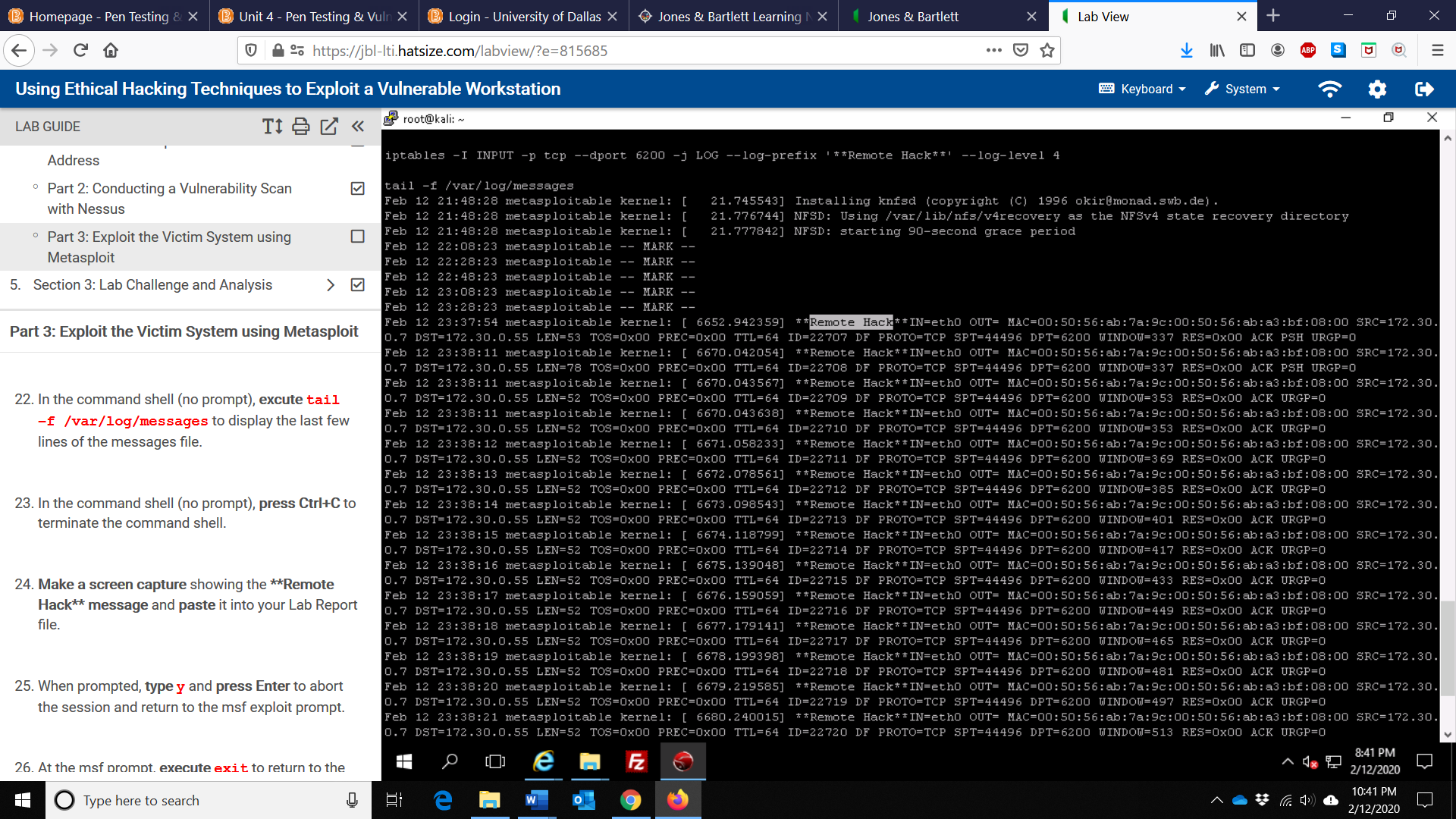
1. Make a screen capture showing the contents of the home directory and paste it into your Lab Report file.



1. Make a screen capture showing the list of iptables rules and paste it into your Lab Report file.



1. Make a screen capture showing the \*\*Remote Hack\*\* message and paste it into your Lab Report file.



1. In the browser window, locate the recommended solution for the vstftpd vulnerability and document that information in your Lab Report file.

Solution: Validate and recompile a legitimate copy of the source code

**Deliverables (other)**

Files downloaded from the virtual environment:

* Zenmap Ping scan
* Zenmap Intense scan
* Natnael\_S2\_VictimScan