**Lab 10: Securing the Network with an Intrusion Detection System (IDS)**

**By**

**Natnael Kebede**



**University of Dallas**

**2020**

This Paper Submitted in Partial Fulfillment of the Requirements for

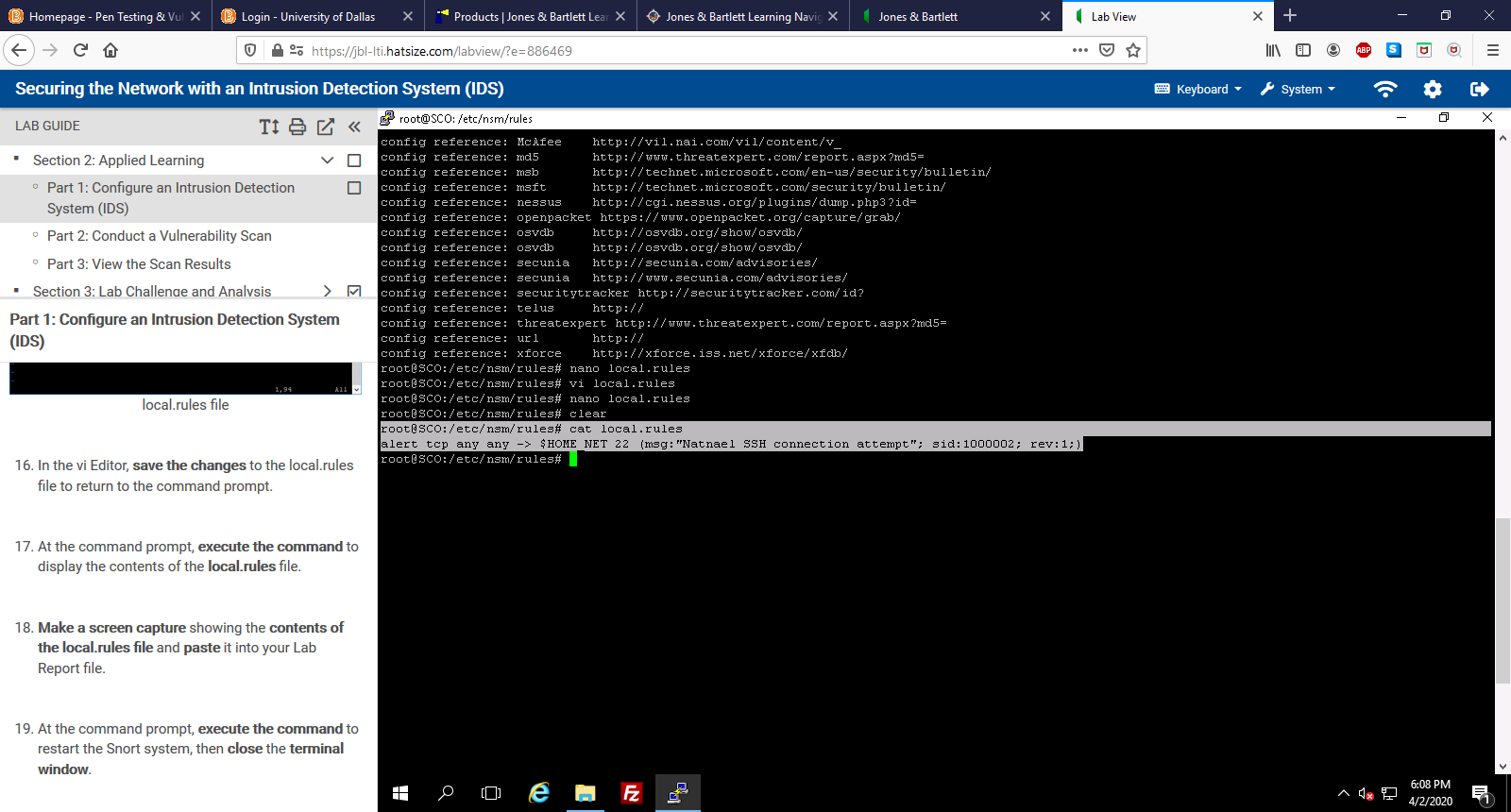
CYBS 7359 – Penetration Testing and Vulnerability Assessment

Spring 2020

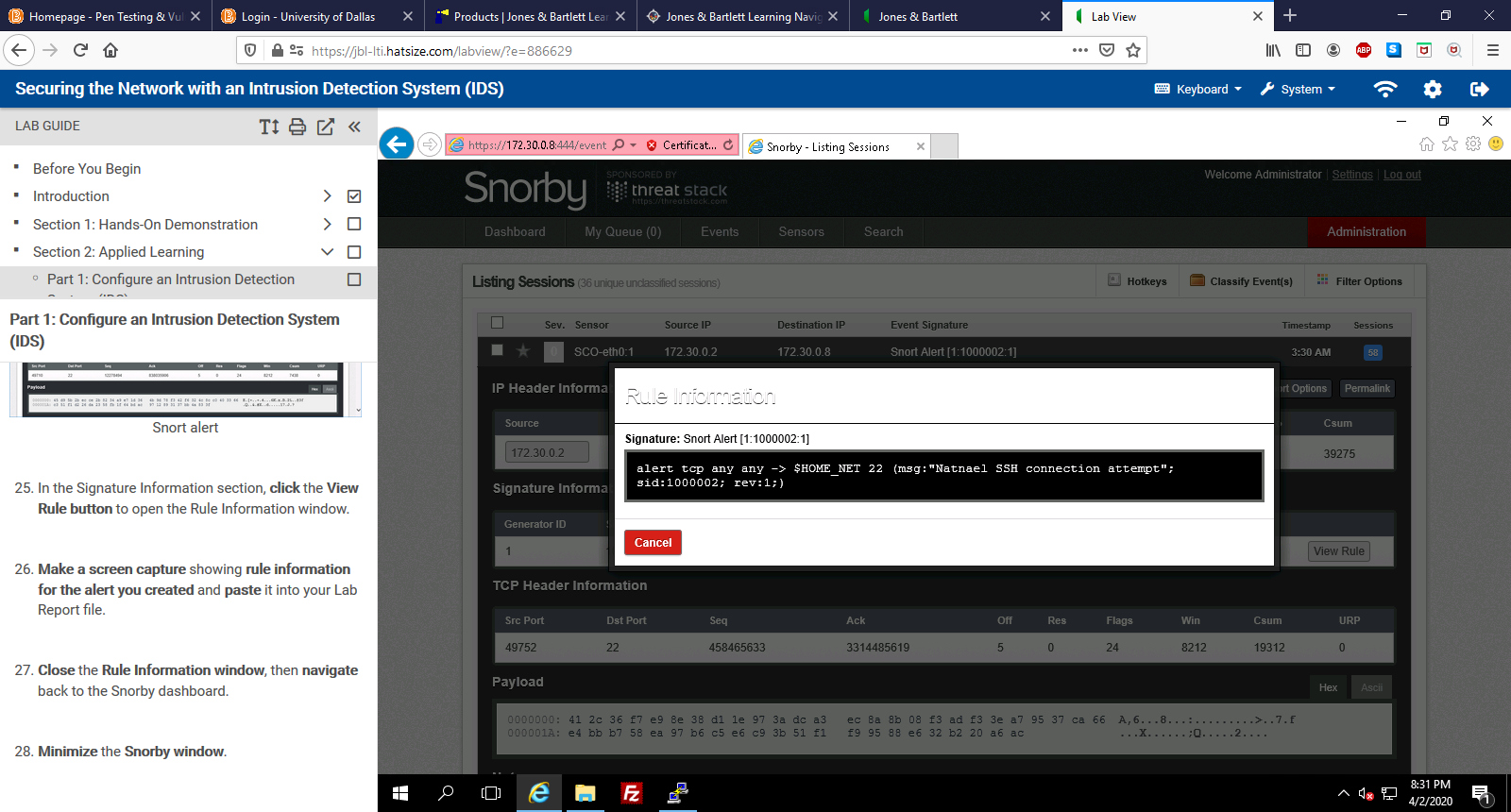
Presented to Dr. Renita Murimi

**Section 2**

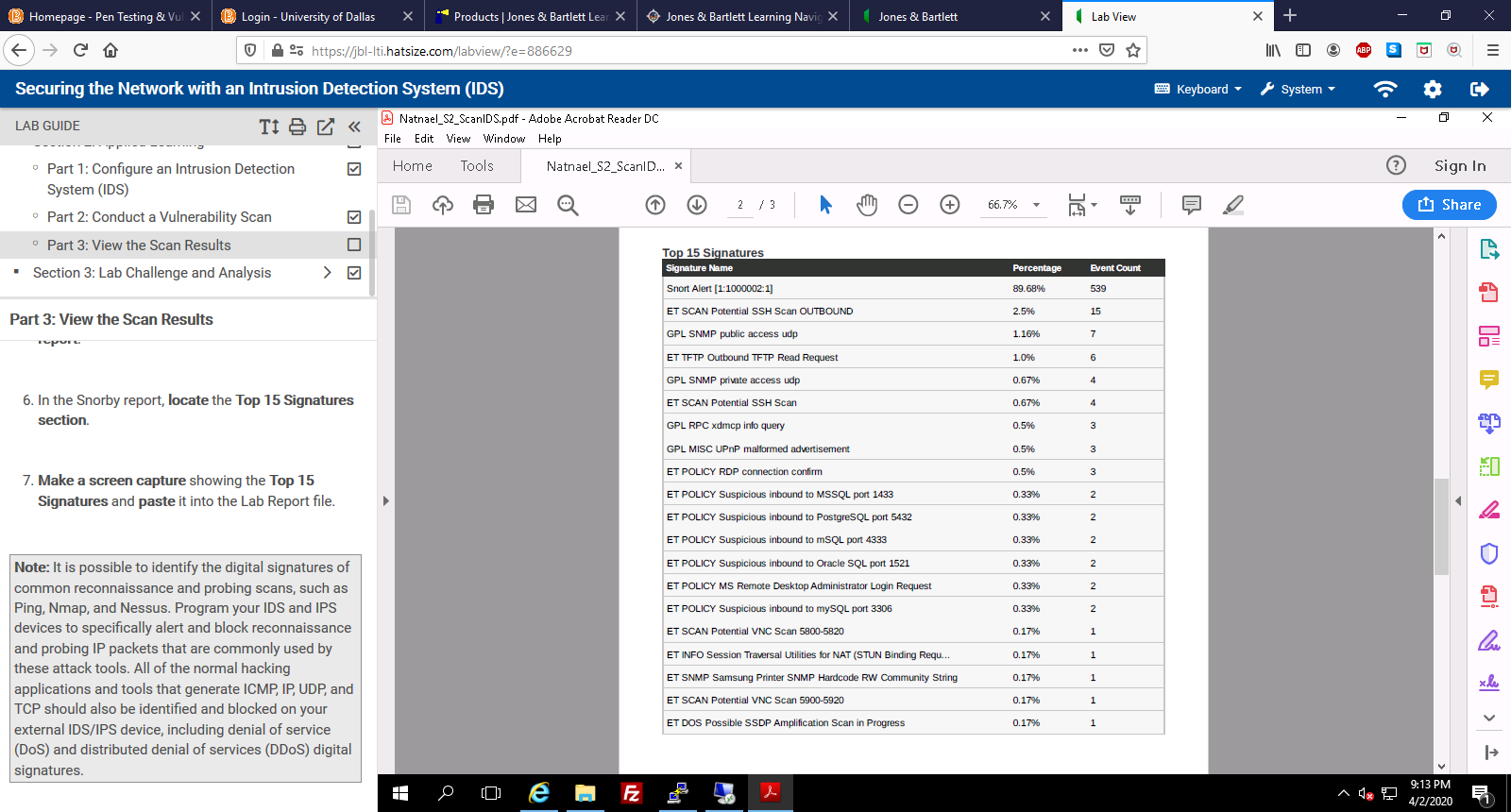
1. Make a screen capture showing the contents of the local.rules file and paste it into your Lab Report file.



1. Make a screen capture showing the rule information for the alert you created and paste it into your Lab Report file.



1. Make a screen capture showing the Top 15 Signatures and paste it into the Lab Report file.



1. In the Lab Report file, research and describe three of the signature alerts captured in the Snortby report.

|  |  |
| --- | --- |
| Signature Alert | Description |
| ET SCAN Potential SSH Scan | Snort has identified an outgoing SSH 22 connection to a specific IP address |
| GPL SNMP private access udp | Snort has detected traffic that may indicate the presence of the SNMP protocol or vulnerabilities in the SNMP protocol on the network. |
| ET TFTP Outbound TFTP Read Request | Snort has perceived a device that is grabbing configuration files or executables to assist with operation. This is a normal netboot operation for network devices such as a router. However, the information gathered via a hidden tool can be handy for an intruder. |