**Lab 1: Assessing and Securing Systems on a Wide Area Network (WAN)**

**By**

**Natnael Kebede**



**University of Dallas**

**2020**

This Paper Submitted in Partial Fulfillment of the Requirements for

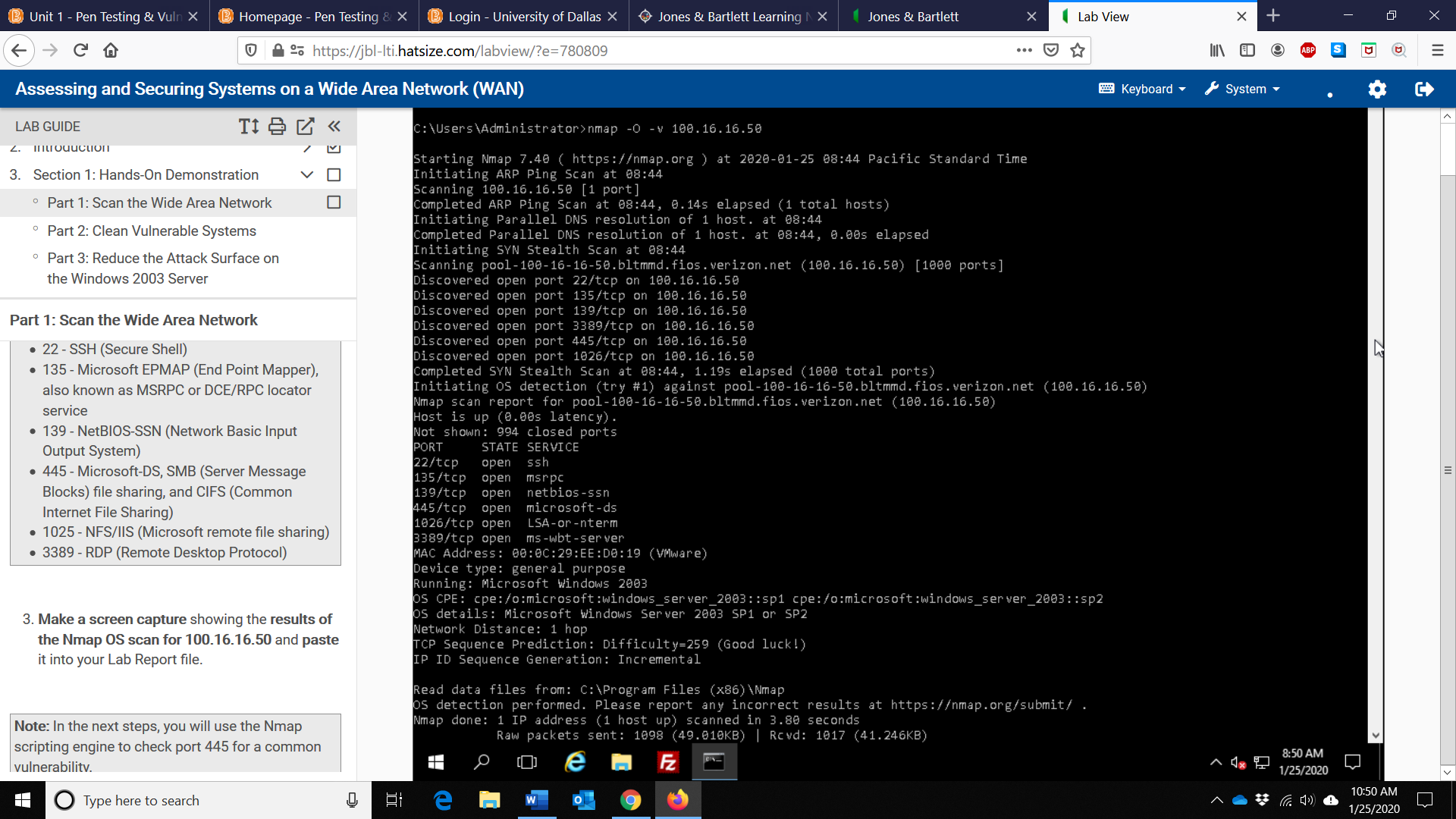
CYBS 7359 – Penetration Testing and Vulnerability Assessment

Spring 2020

Presented to Dr. Renita Murimi

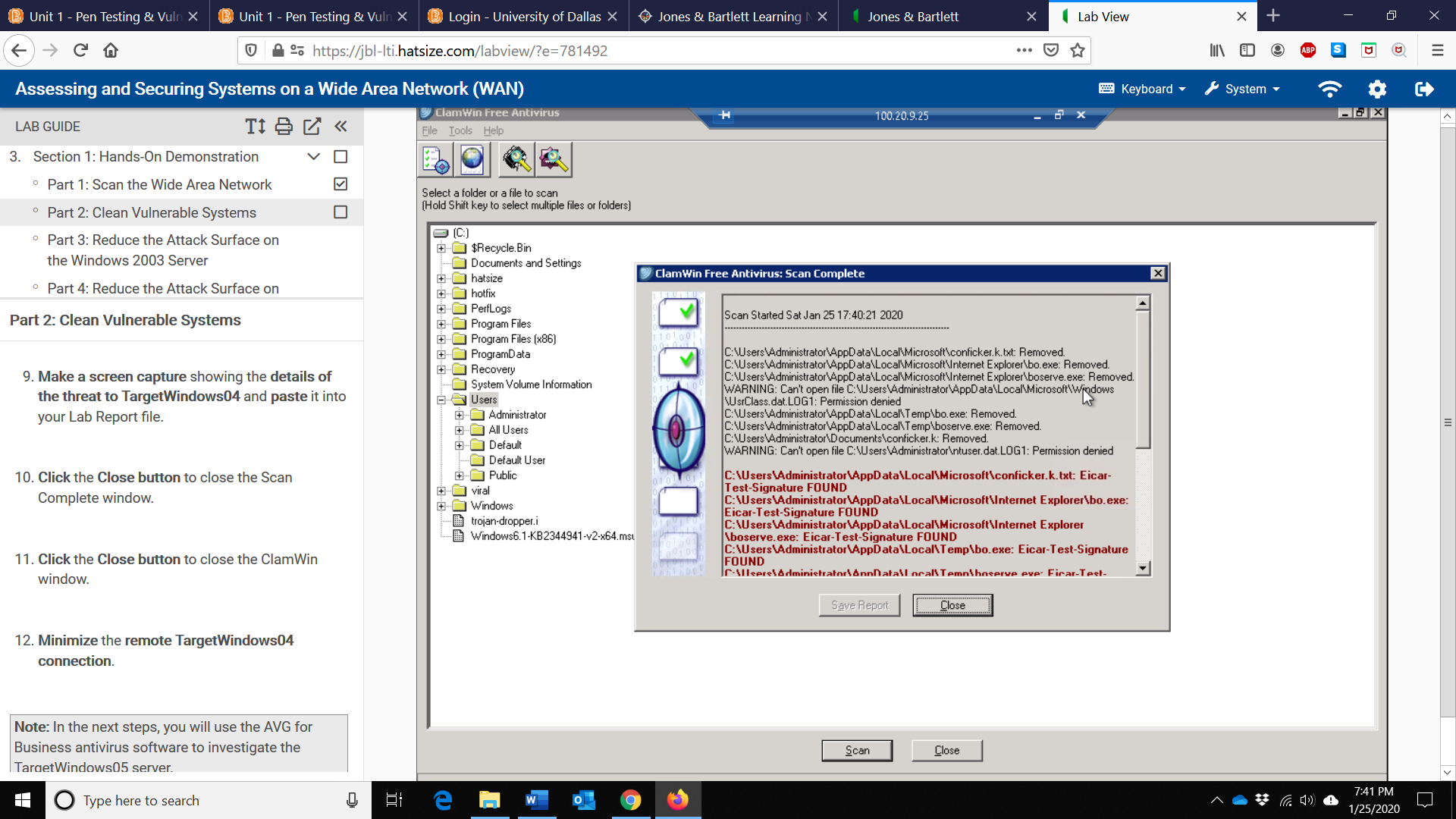
**Section 1**

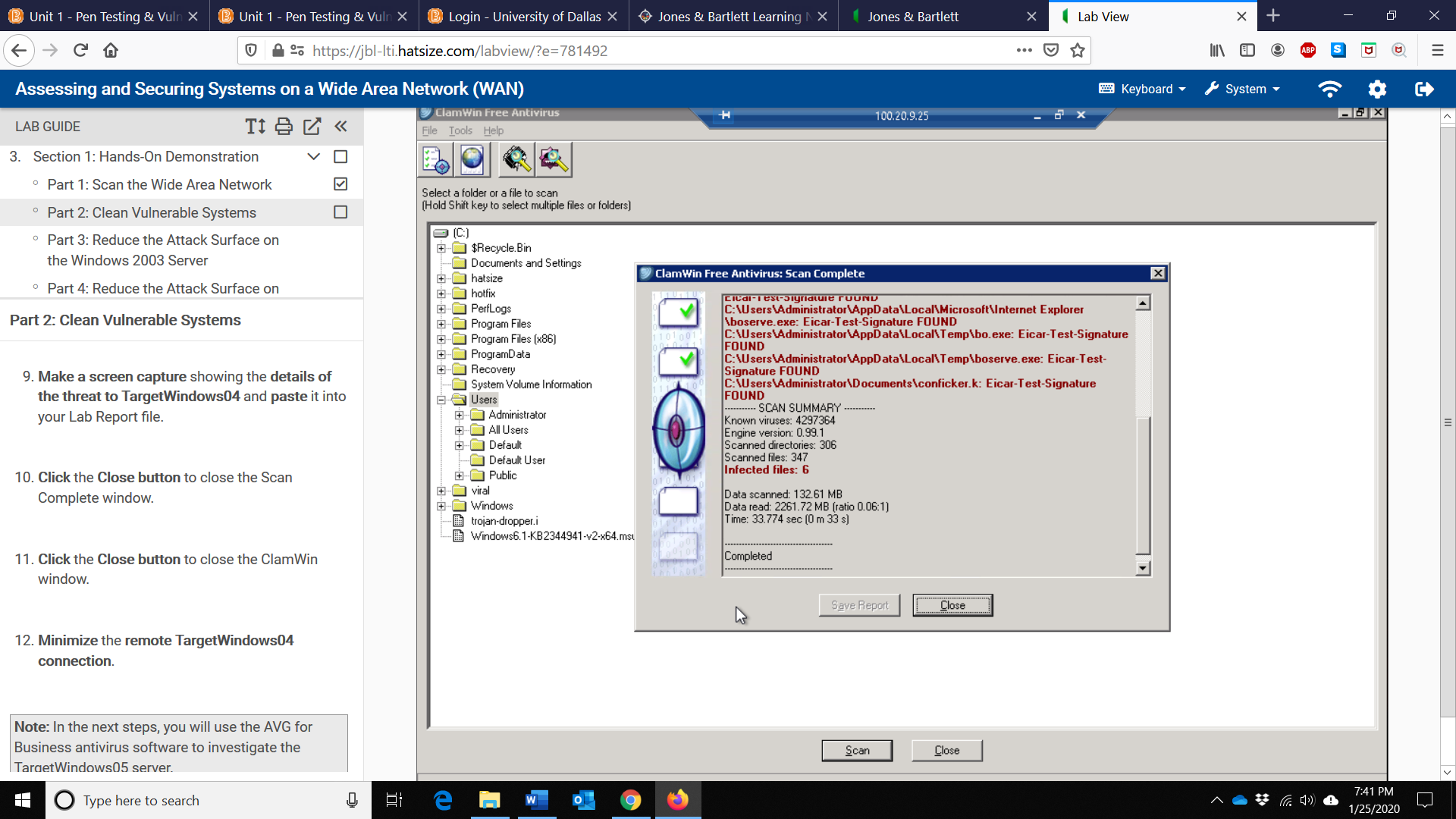
1. Make a screen capture showing the results of the Nmap OS scan for 10.16.16.50 and paste it into your Lab Report file.



1

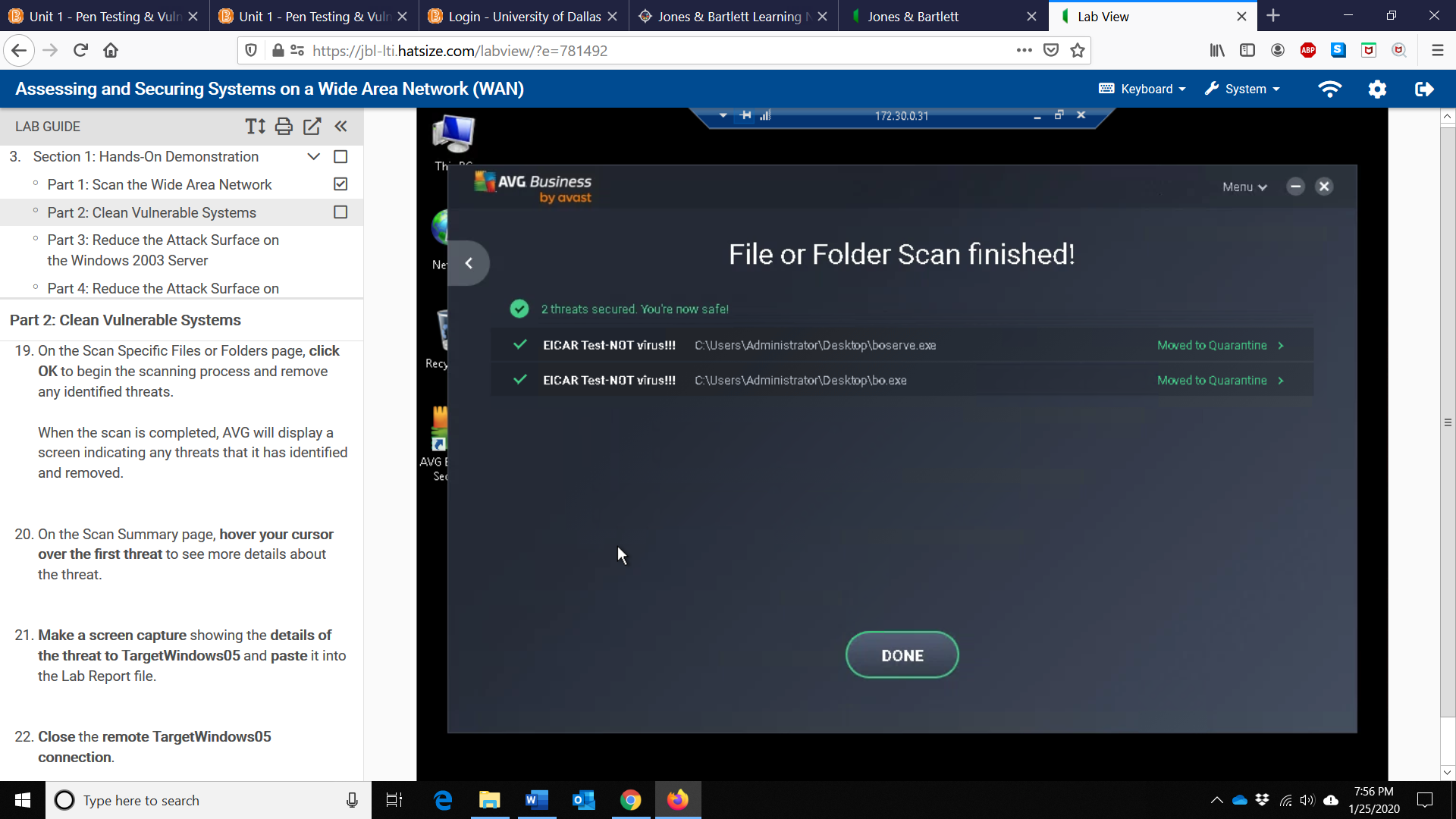
1. Make a screen capture showing the details of the threat to TargetWindows04 and paste it into your Lab Report file.

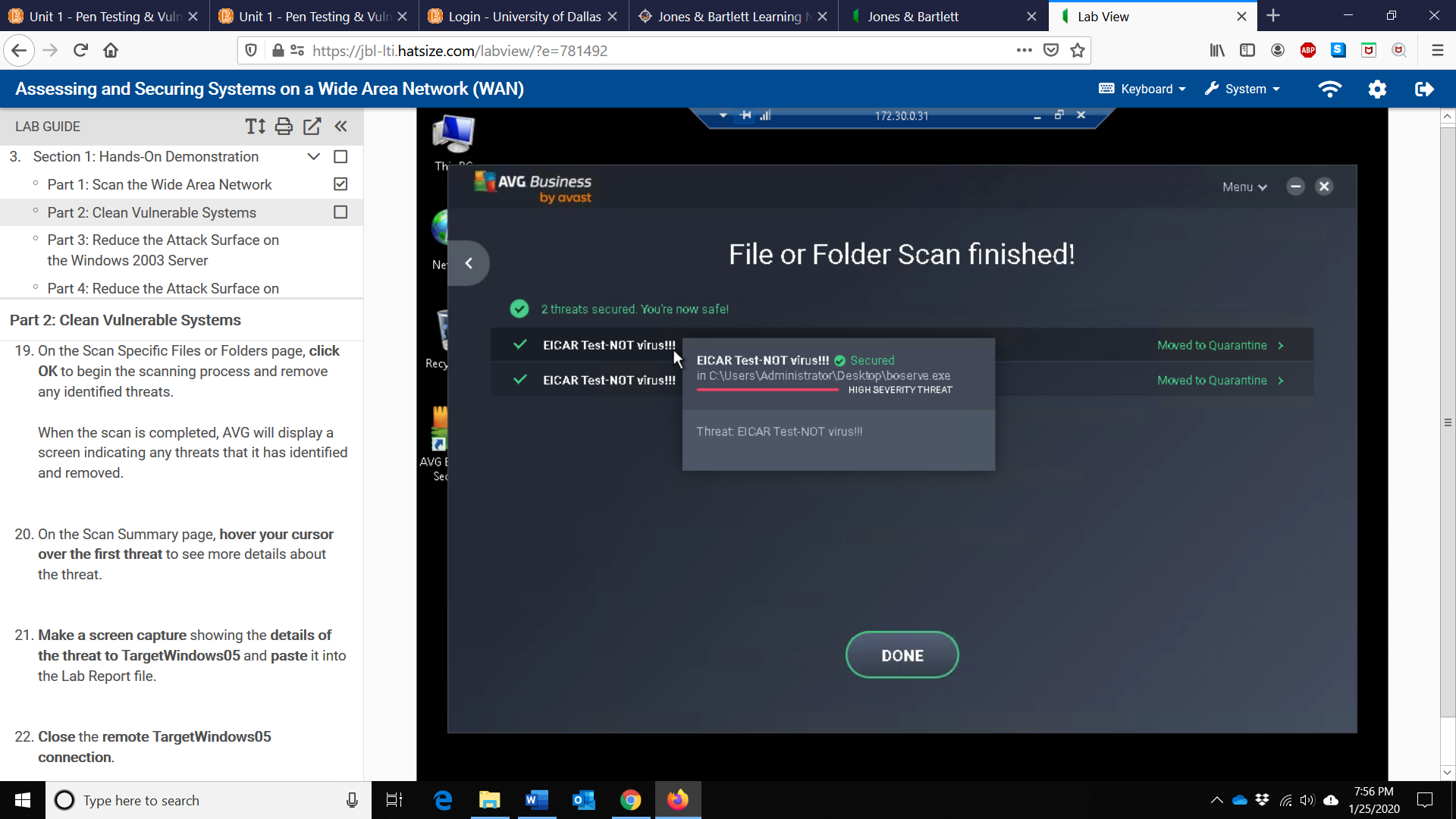




2

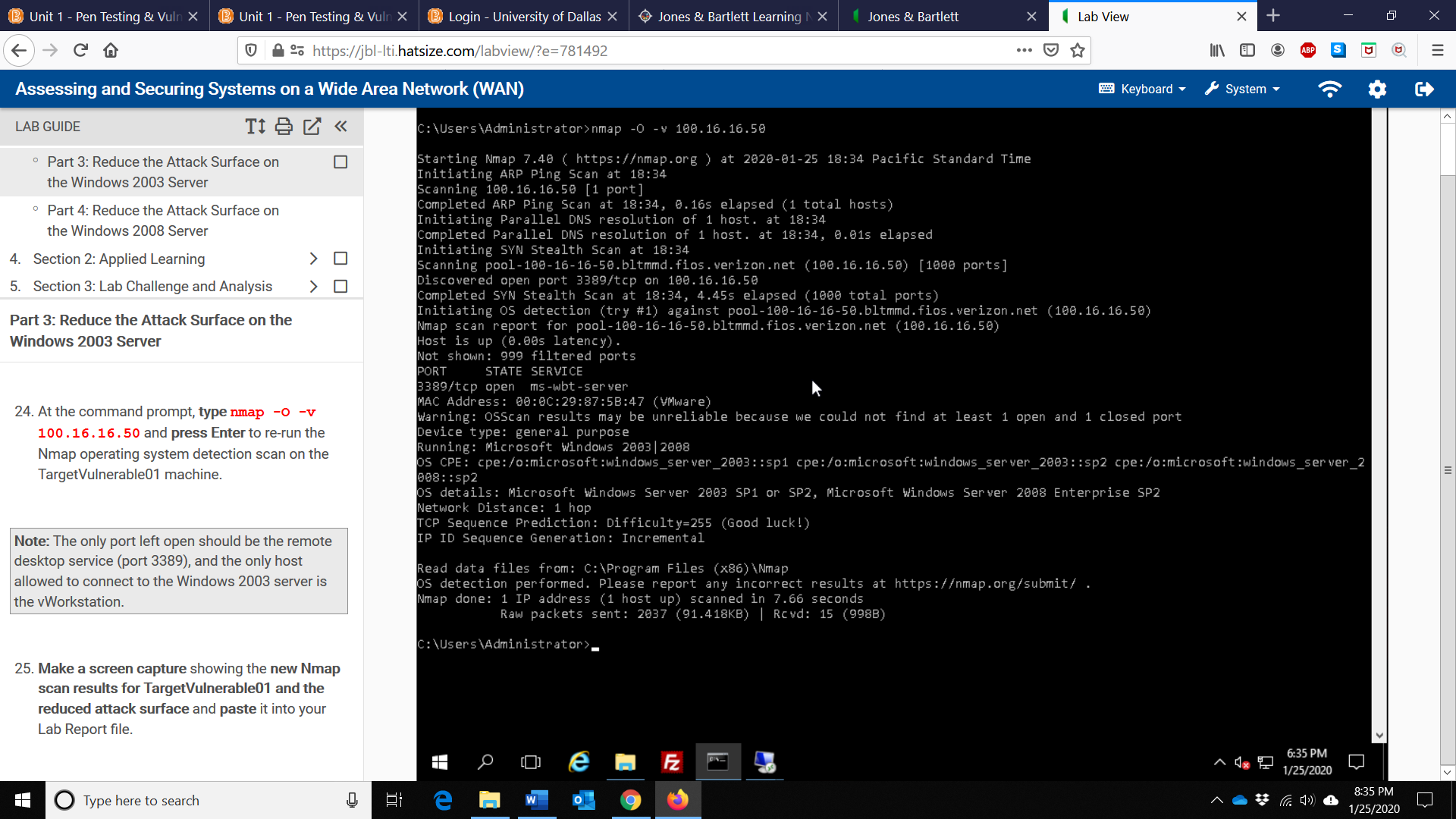
1. Make a screen capture showing the details of the threat to TargetWindows05 and paste it into your Lab Report file.





3

1. Make a screen capture showing the new Nmap scan results for TragetVulnerable01 and the reduced attack surface and paste it into your Lab Report file.



1. In your Lab Report file, compare the results of the two scans for this computer and explain how your actions in Part 3 of this lab hardened security on this machine.

Comparing the two scans of the Windows 2003 system machine (100.16.16.50) reveals that an existing vulnerable machine with six open ports (22-SSH, 135-Microsoft EPMAP, 139-NetBIOS-SSN, 445-Microsoft-DS,SMB, 1025-NFS/IIS, and 3389-RDP) was later made to be less risky by minimizing the number of open ports that could be a source of any exploit. The actions in Part 3 of this lab consisted of configuring the host-based firewall and enabling it to help reduce the attack surface (exposure) on the machine, which in-turn hardened security on this machine by eliminating the vulnerable open ports that were identified in the initial scan (leaving 3389-RDP only to make remote connections in the lab).

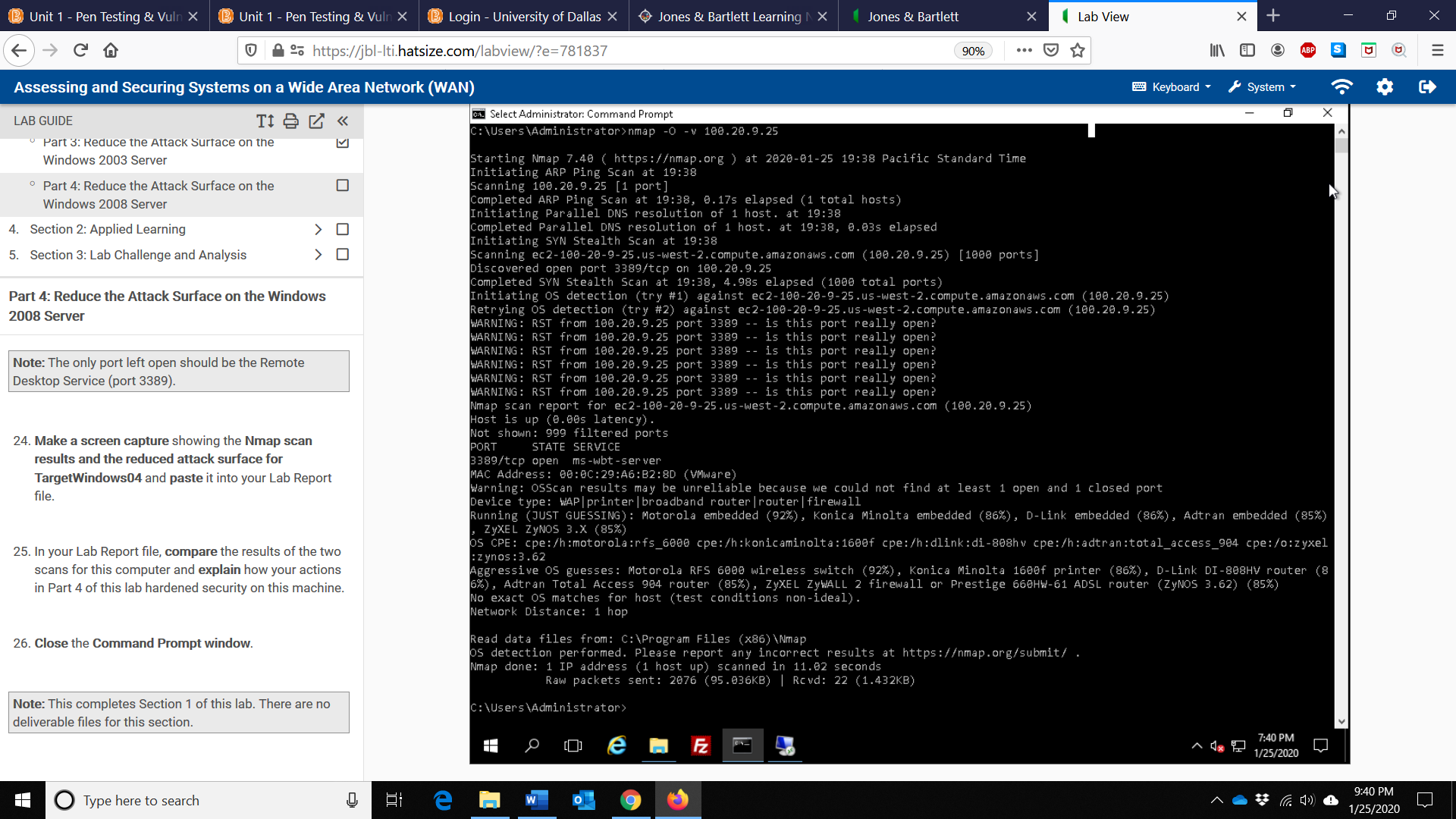
4

1. Make a screen capture showing the remaining enabled inbound Rule and paste it into your Lab Report file.



5

1. Make a screen capture showing the Nmap scan results and the reduced attack surface for TragetWindows04 and paste it into your Lab Report file.



1. In your Lab Report file, compare the results of the two scans for this computer and explain how your actions in Part 4 of this lab hardened security on this machine.

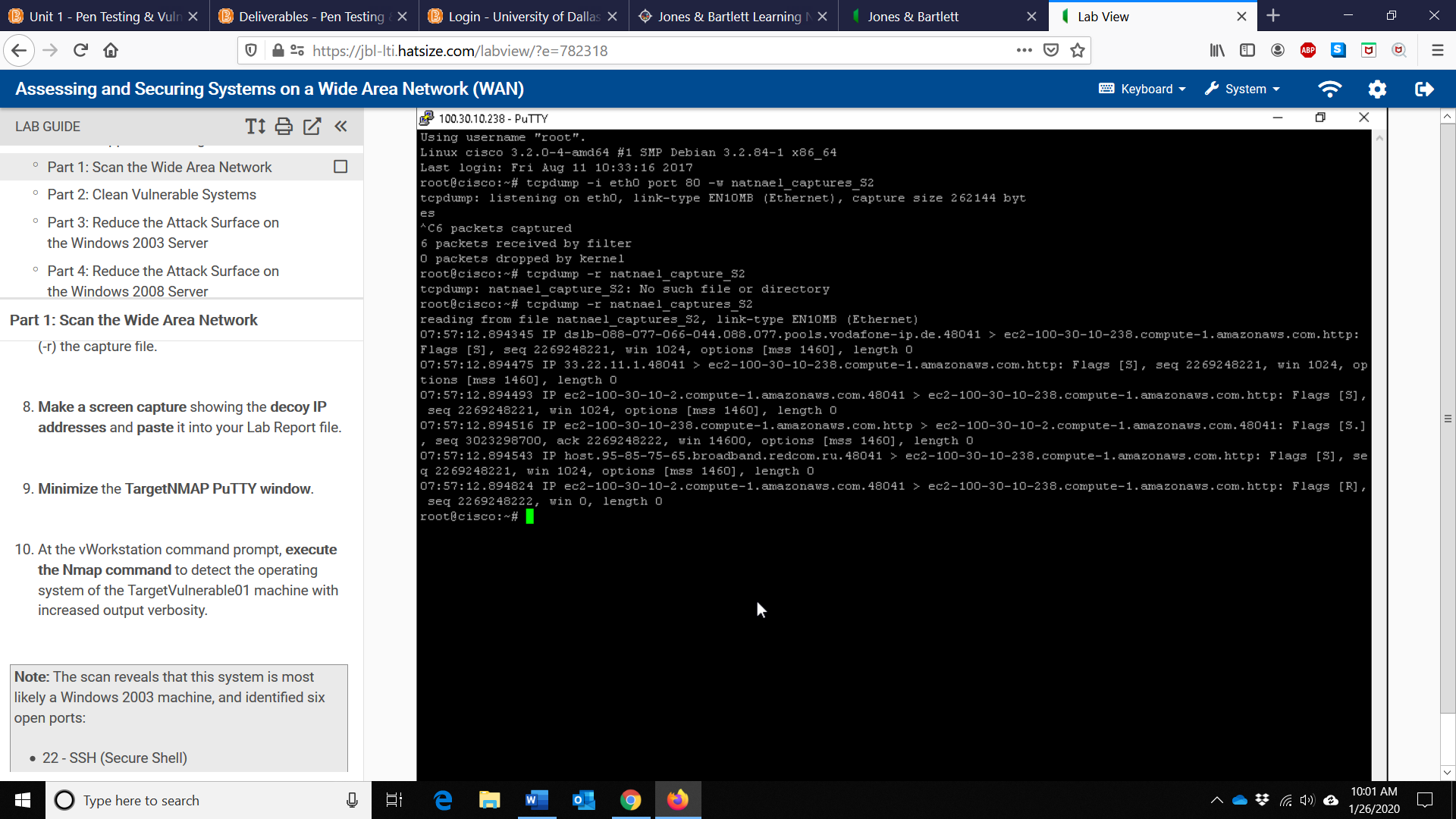
Comparing the two scans of the Windows 2008 system machine (100.20.9.25) reveals that an existing vulnerable machine with ten open ports (22-SSH, 135-Microsoft-RPC, 139-NetBIOS-SSN, 445-Microsoft-DS, 1025-NFS/IIS, 3389-RDP, 49152-Unknown, 49153-Unkown, 49154-Unkown, 49155-Unkown, 49156-Unkown, and 49157-Unkown) was later made to be less risky by minimizing the number of open ports that could be a source of any exploit.

The actions in Part 4 of this lab consisted of configuring the 2008 host-based firewall and enabling it to help reduce the attack surface (exposure) on the machine, which in-turn hardened security on this machine by eliminating the vulnerable open ports that were identified in the initial scan (leaving the Remote Desktop Service – Port 3389 open only to make remote connections in the lab).

6

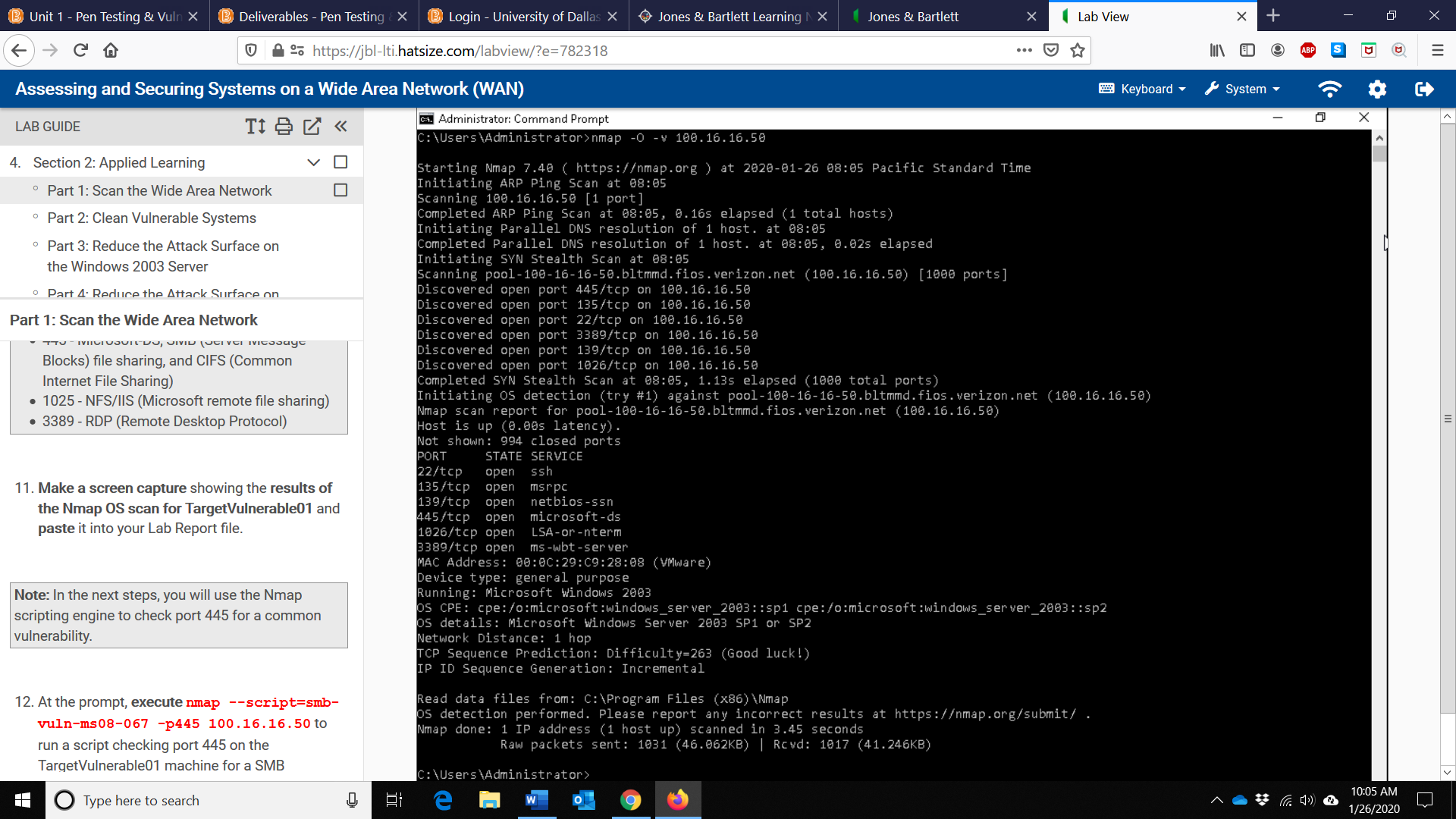
**Section 2**

1. Make a screen capture showing the decoy IP addresses and paste it in your Lab Report file.



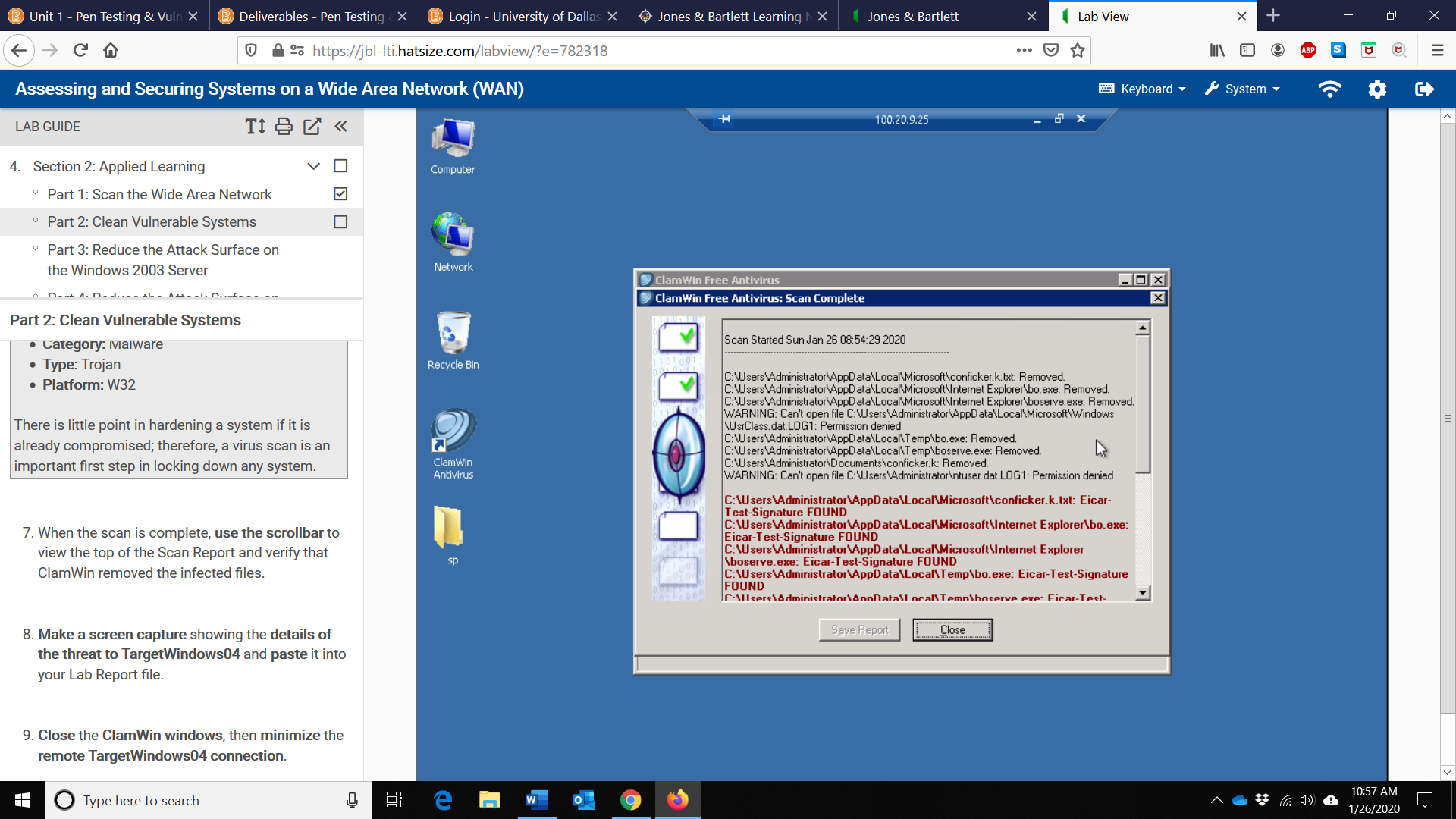
7

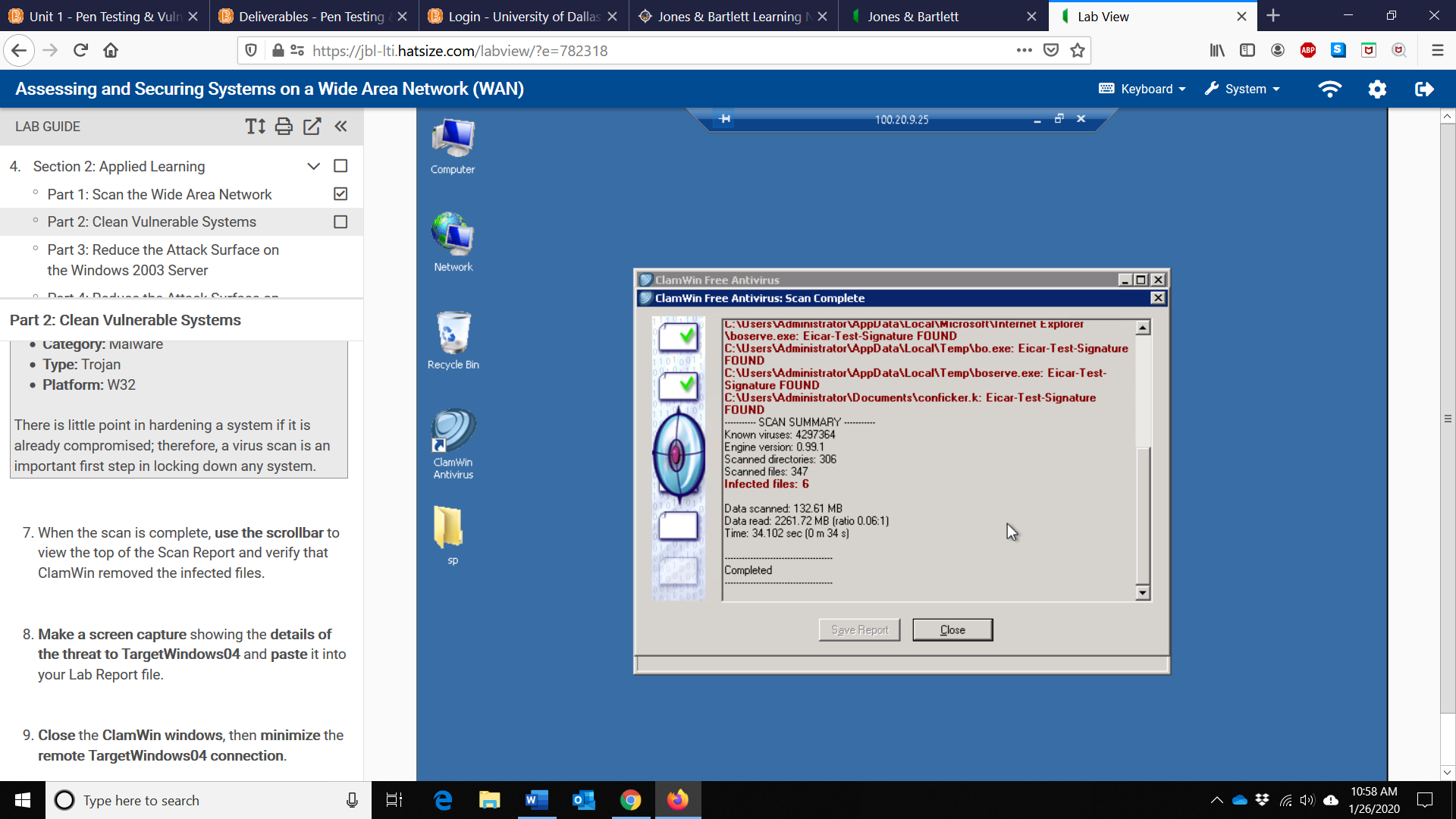
1. Make a screen capture showing the results of the Nmap OS scan for TargetVulnerable01 and paste it into your Lab Report file.



8

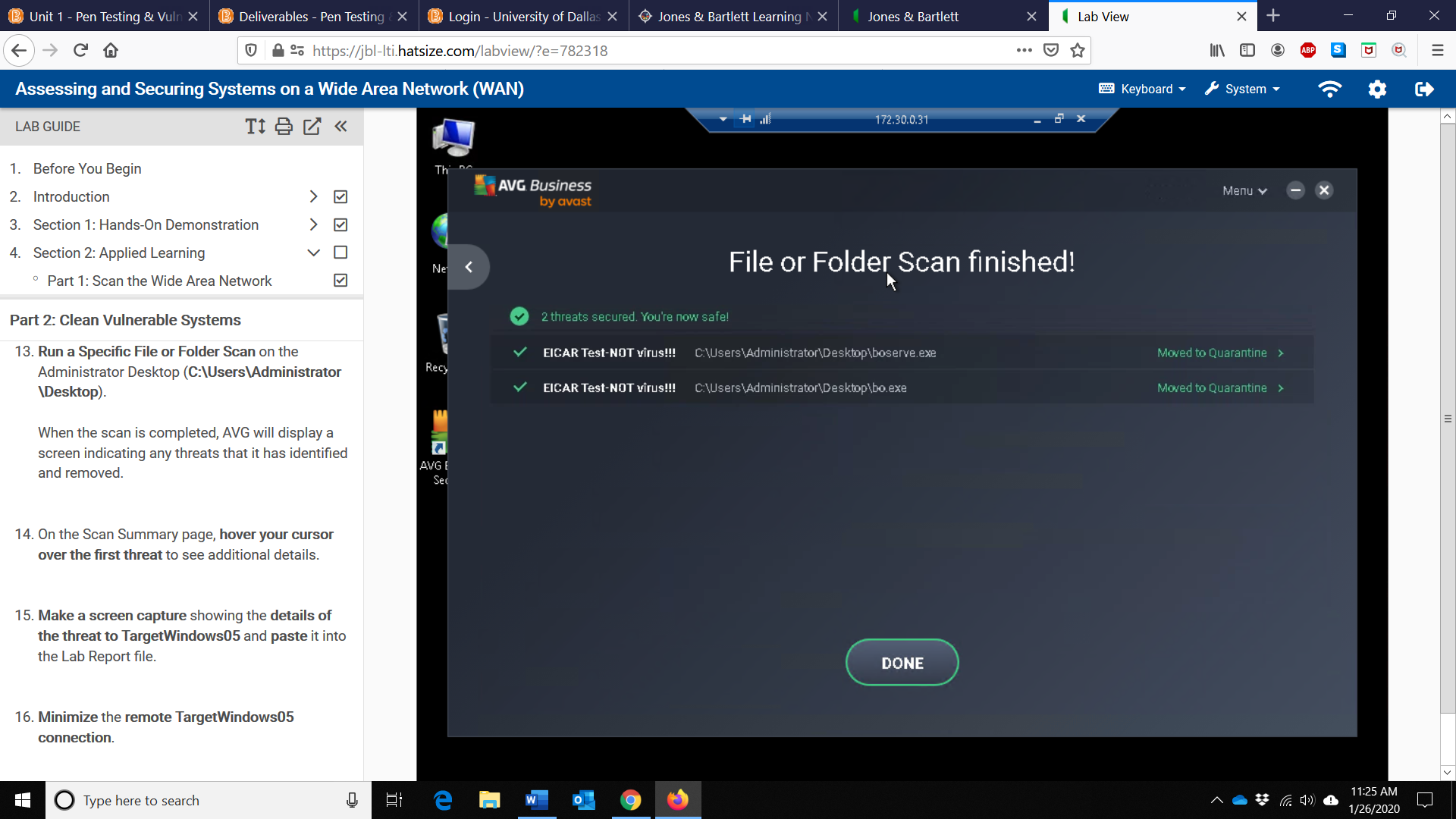
1. Make a screen capture showing the details of the threat to TargetWindows04 and paste it into your Lab Report file.

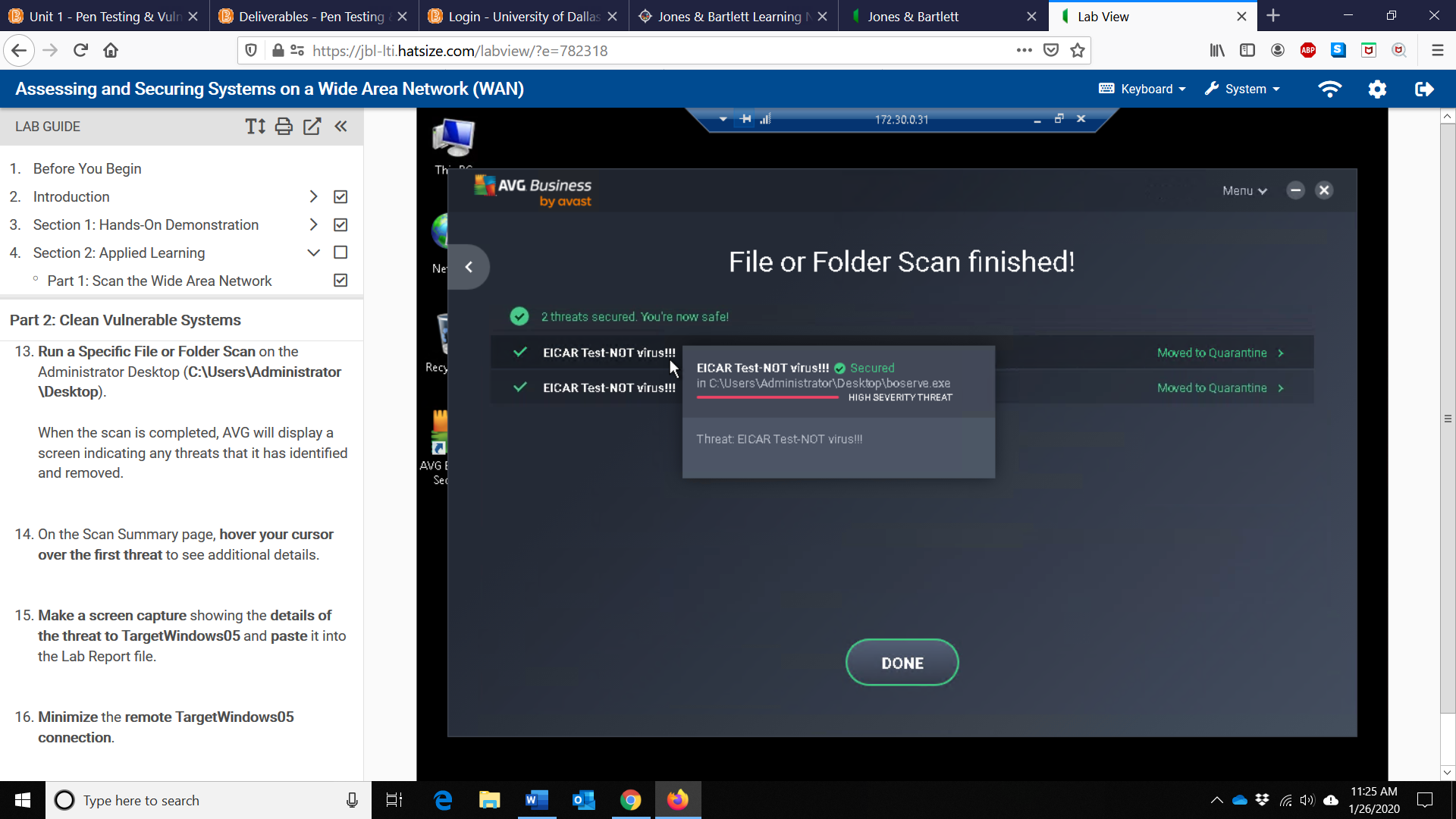




9

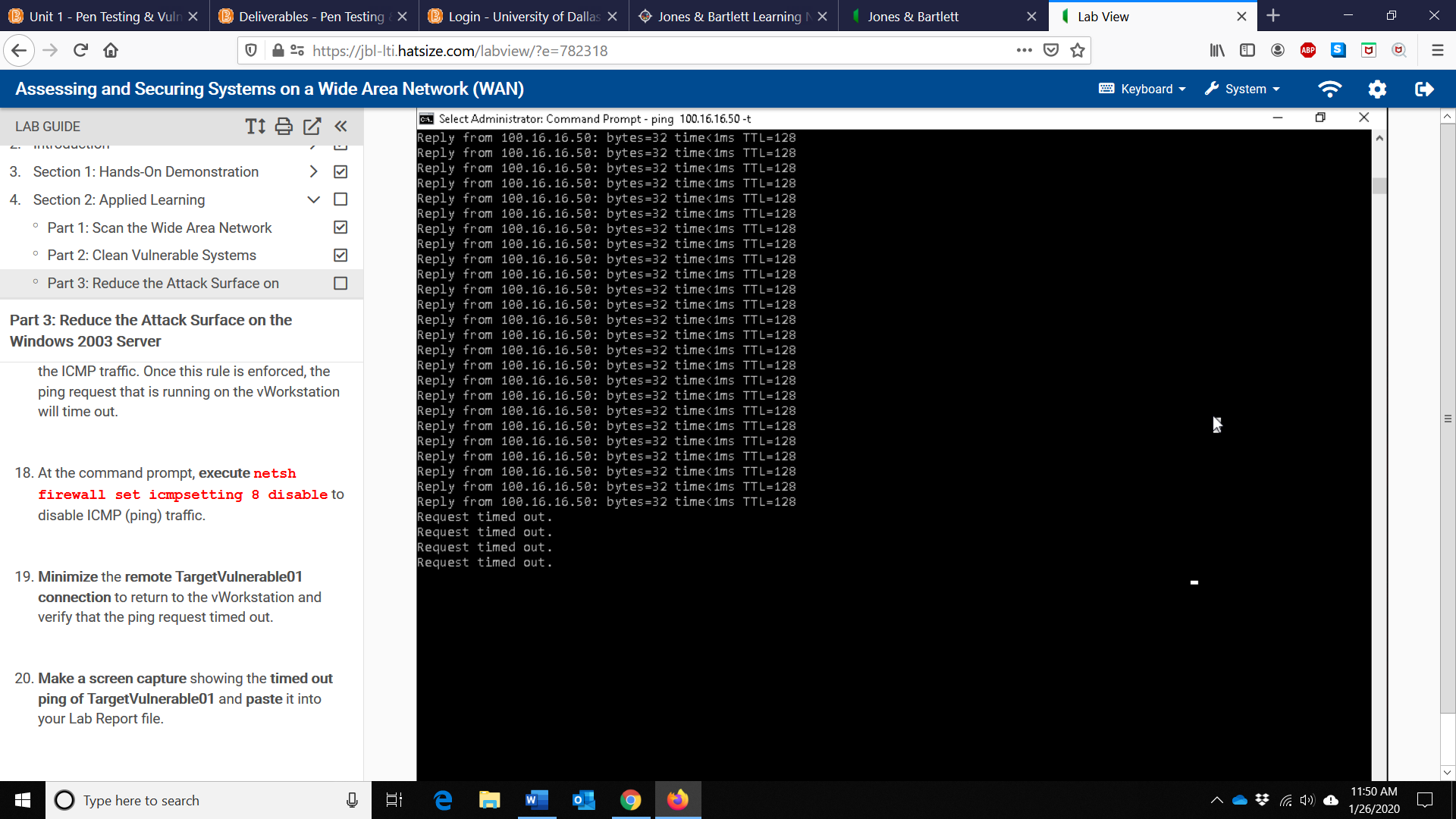
1. Make a screen capture showing the details of the threat to TargetWindows05 and paste it into your Lab Report file.





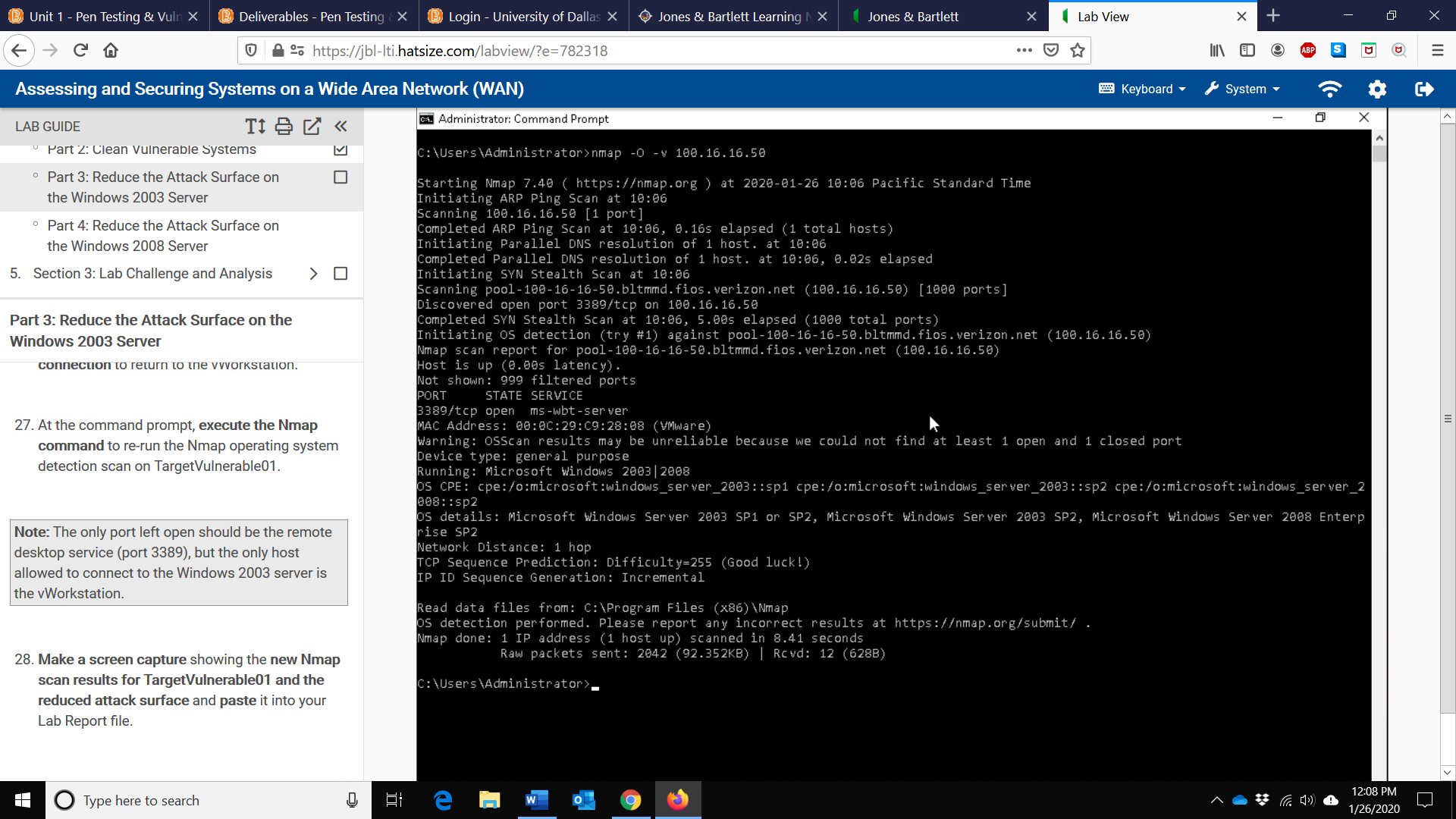
10

1. Make a screen capture showing the timed-out ping of TargetVulnerable01 and paste it into your Lab Report file.



11

1. Make a screen capture showing the new Nmap scan results for TragetVulnerable01 and the reduced attack surface and paste it into your Lab Report file.

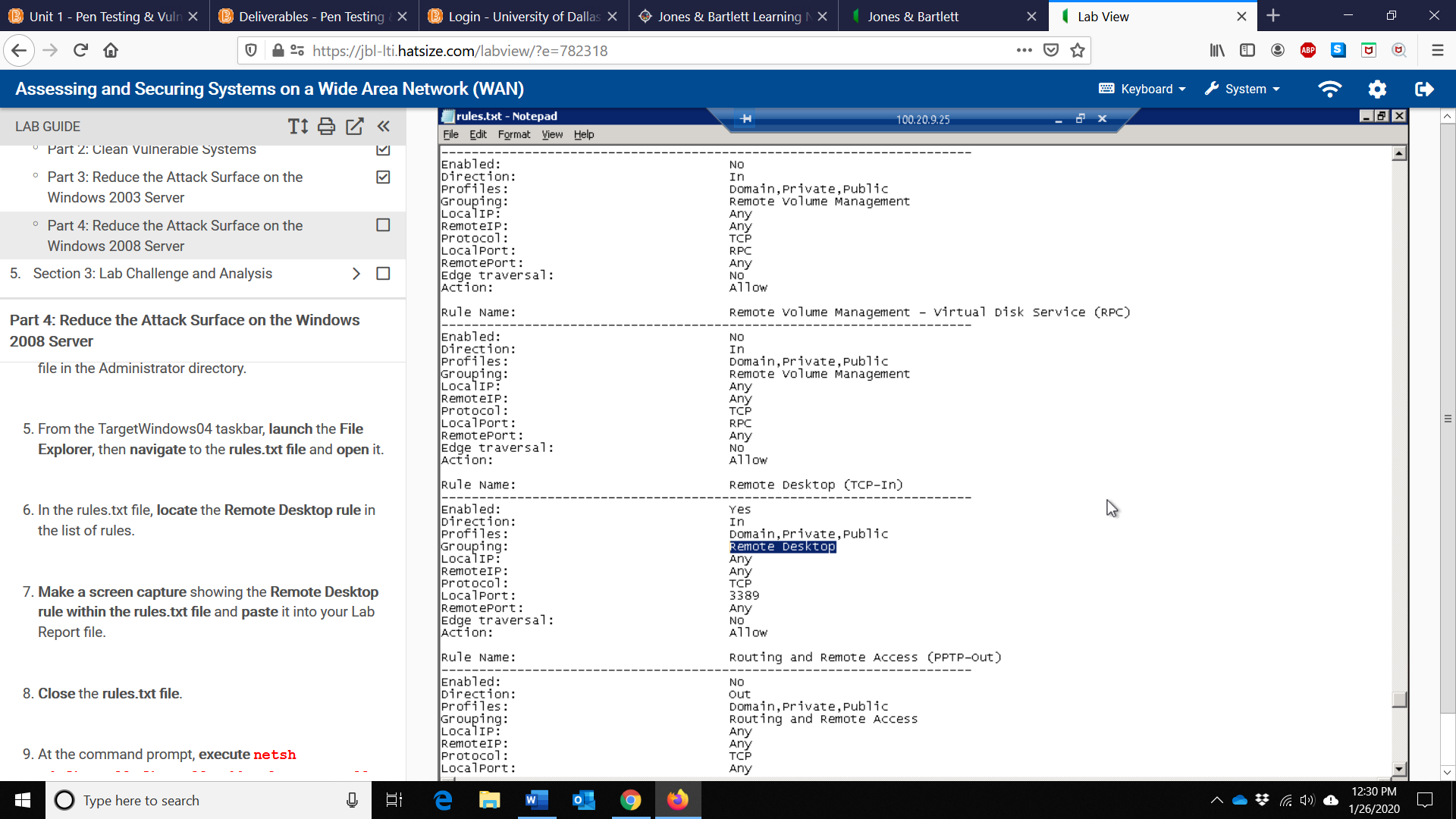


1. In your Lab Report file, compare the results of the two scans for this computer and explain how your actions in Part 3 of this lab hardened security on this machine.

Comparing the two scans of the Windows 2003 system machine (100.16.16.50) reveals that an existing vulnerable machine with six open ports (22-SSH, 135-Microsoft EPMAP, 139-NetBIOS-SSN, 445-Microsoft-DS,SMB, 1025-NFS/IIS, and 3389-RDP) was later made to be less risky by minimizing the number of open ports that could be a source of any exploit. The actions in Part 3 of this lab consisted of configuring the host-based firewall and enabling it to help reduce the attack surface (exposure) on the machine, which in-turn hardened security on this machine by eliminating the vulnerable open ports that were identified in the initial scan (leaving 3389-RDP only to make remote connections in the lab). The command netsh was used to enable the firewall rules and have the Remote Desk session remain open.

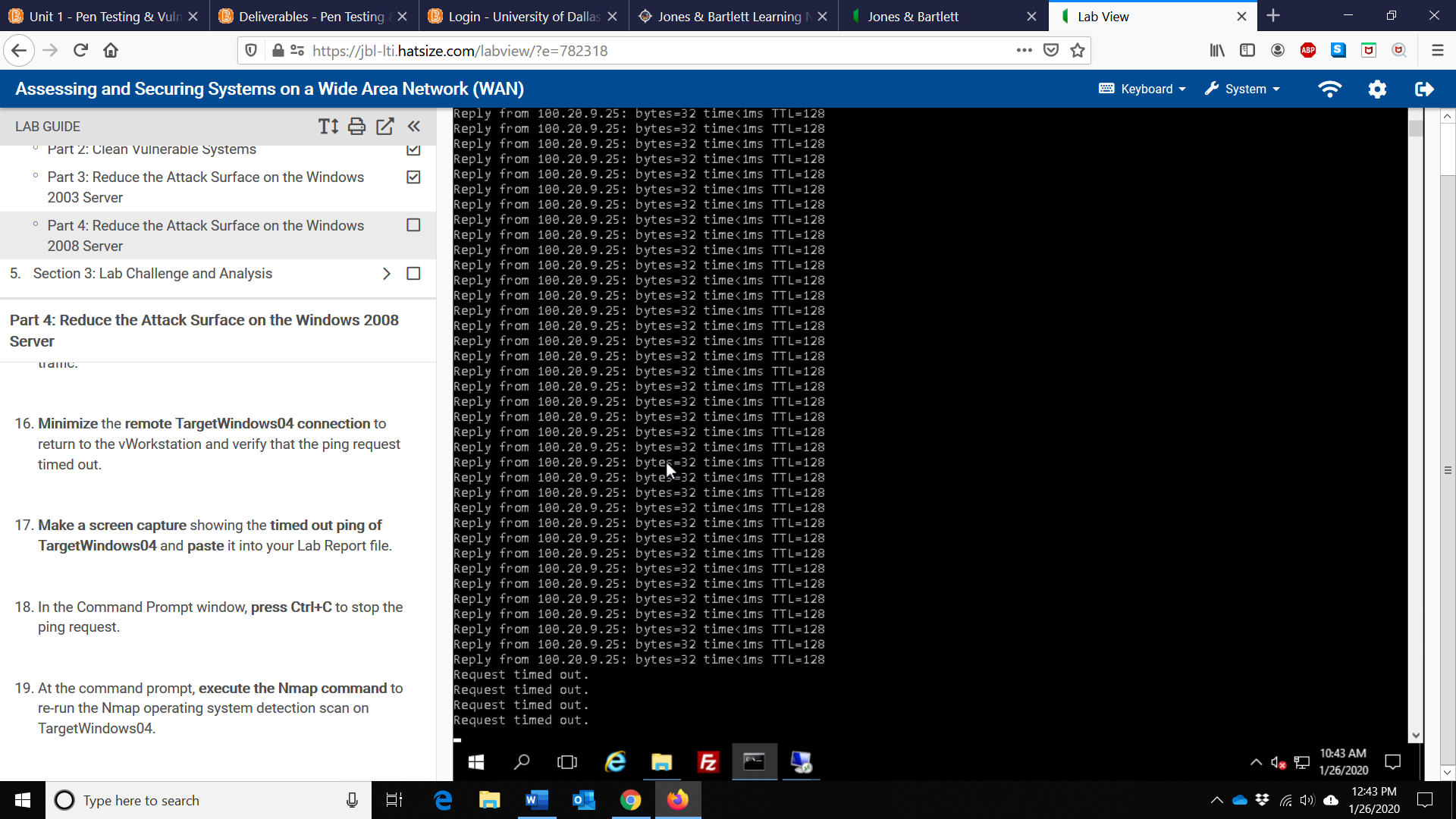
12

1. Screen capture showing the Remote Desktop rule within the rules.txt file



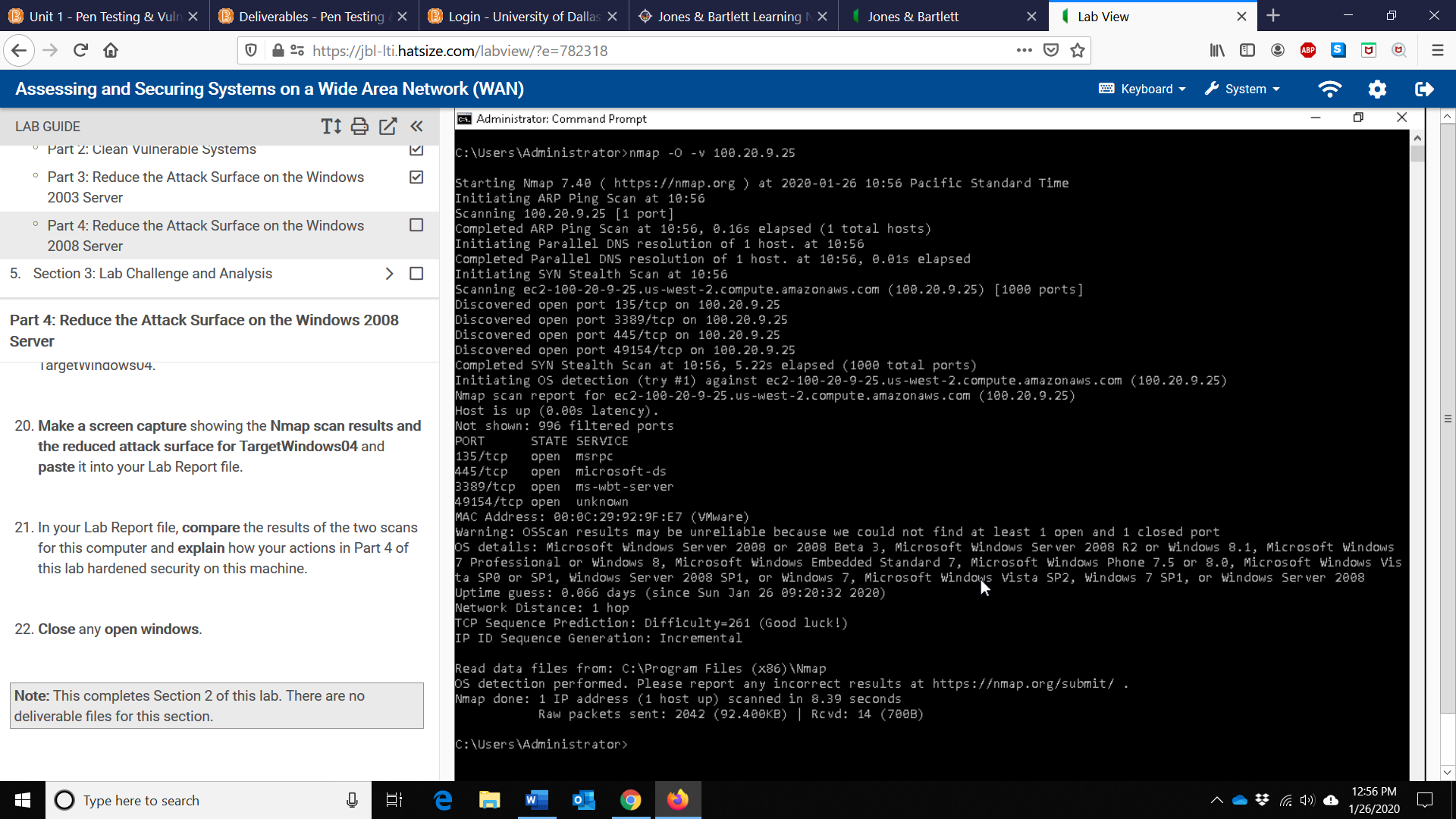
13

1. Make a screen capture showing the timed-out ping of TargetWindows04 and paste it into your Lab Report file.



14

1. Make a screen capture showing the Nmap scan results and the reduced attack surface for TragetWindows04 and paste it into your Lab Report file.



1. In your Lab Report file, compare the results of the two scans for this computer and explain how your actions in Part 4 of this lab hardened security on this machine.

Comparing the two scans of the Windows 2008 system machine (100.20.9.25) reveals that an existing vulnerable machine with ten open ports (22-SSH, 135-Microsoft-RPC, 139-NetBIOS-SSN, 445-Microsoft-DS, 1025-NFS/IIS, 3389-RDP, 49152-Unknown, 49153-Unkown, 49154-Unkown, 49155-Unkown, 49156-Unkown, and 49157-Unkown) was later made to be less risky by minimizing the number of open ports that could be a source of any exploit.

The actions in Part 4 of this lab consisted of configuring the 2008 host-based firewall and enabling it to help reduce the attack surface (exposure) on the machine, which in-turn hardened security on this machine by eliminating the vulnerable open ports that were identified in the initial scan leaving 4 ports open. These include 135-Microsoft-RPC, 445-Microsoft-DS, 49154-Unkown and the Remote Desktop Service – Port 3389 open, which is used to make remote connections in the lab). Furthermore, the command netsh wouldn’t work with Windows 2008 as it contains Advanced Firewall, a more comprehensive firewall that allows granular control of the communications between the host system and other systems on the network.

15