**Lab 6: Identifying and Removing Malware on a Windows System**

**By**

**Natnael Kebede**



**University of Dallas**

**2020**

This Paper Submitted in Partial Fulfillment of the Requirements for

CYBS 7359 – Penetration Testing and Vulnerability Assessment

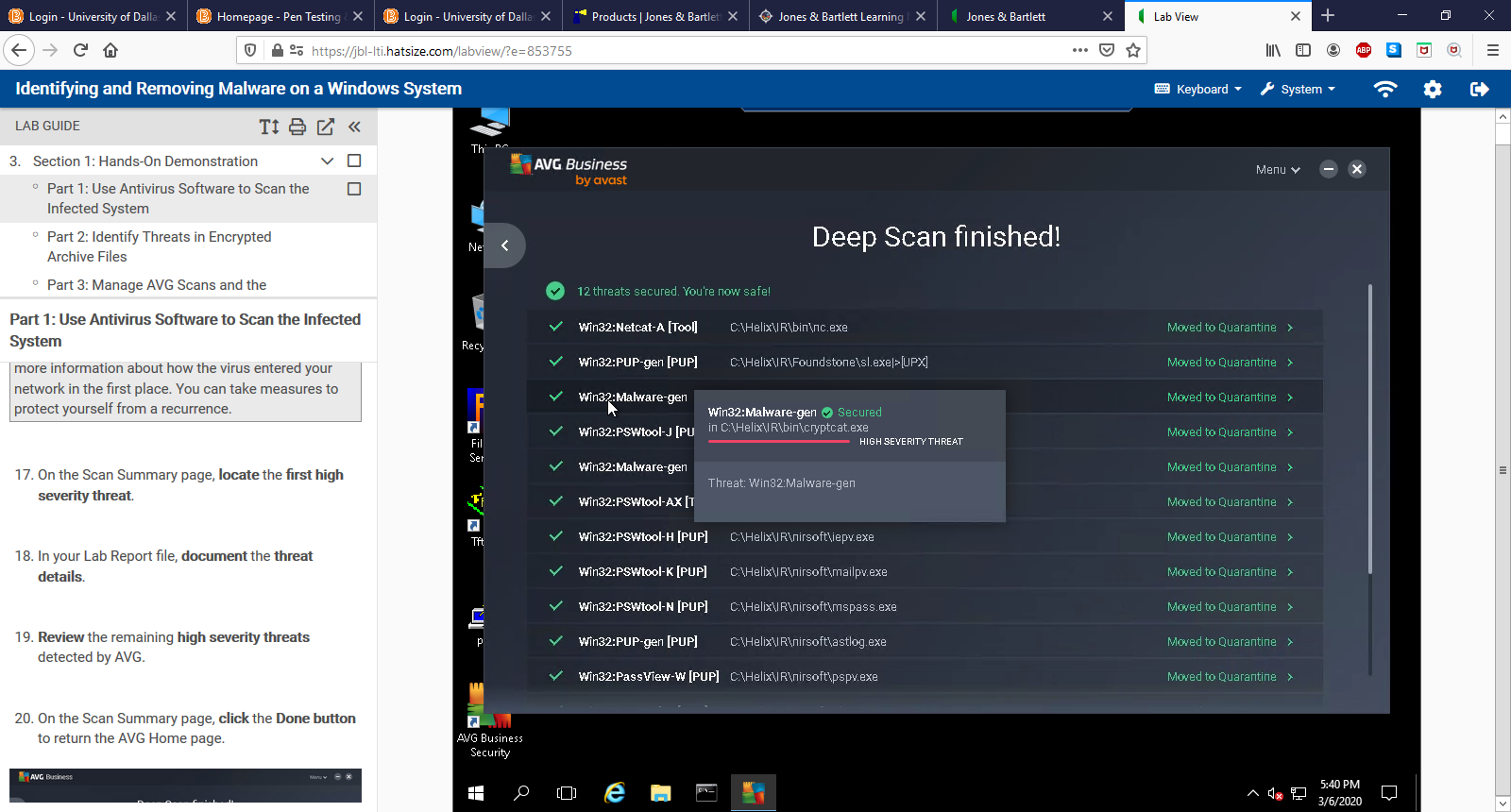
Spring 2020

Presented to Dr. Renita Murimi

**Section 1**

**Part 1**

1. On the scan summary page, locate the first high severity threat. In your Lab Report file, document the threat details.

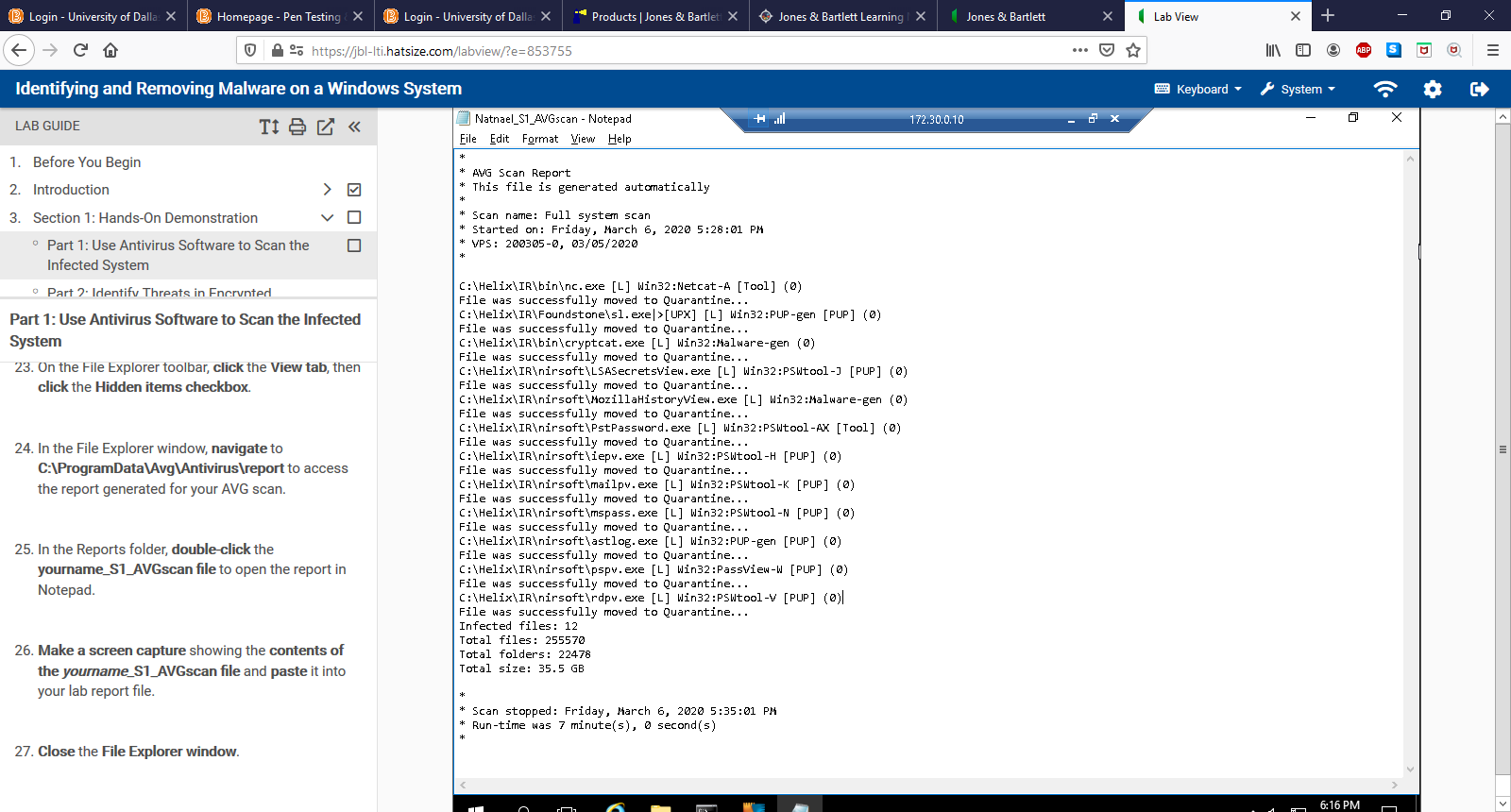


After identifying the name and details for the high severity threat, the information was then used to search AVG’s Website to get more details. Careful researching of the threat tells us that Win32:Malware-gen is a generic threat that appears malicious to AVG but does not match any of the known threats contained in AVG’s malware database. An alert from AVG warning someone that it detected Win32: Malware-Gen, indicates that a 32-bit file found on the Windows operating system should be flagged for further inspection.

Reference

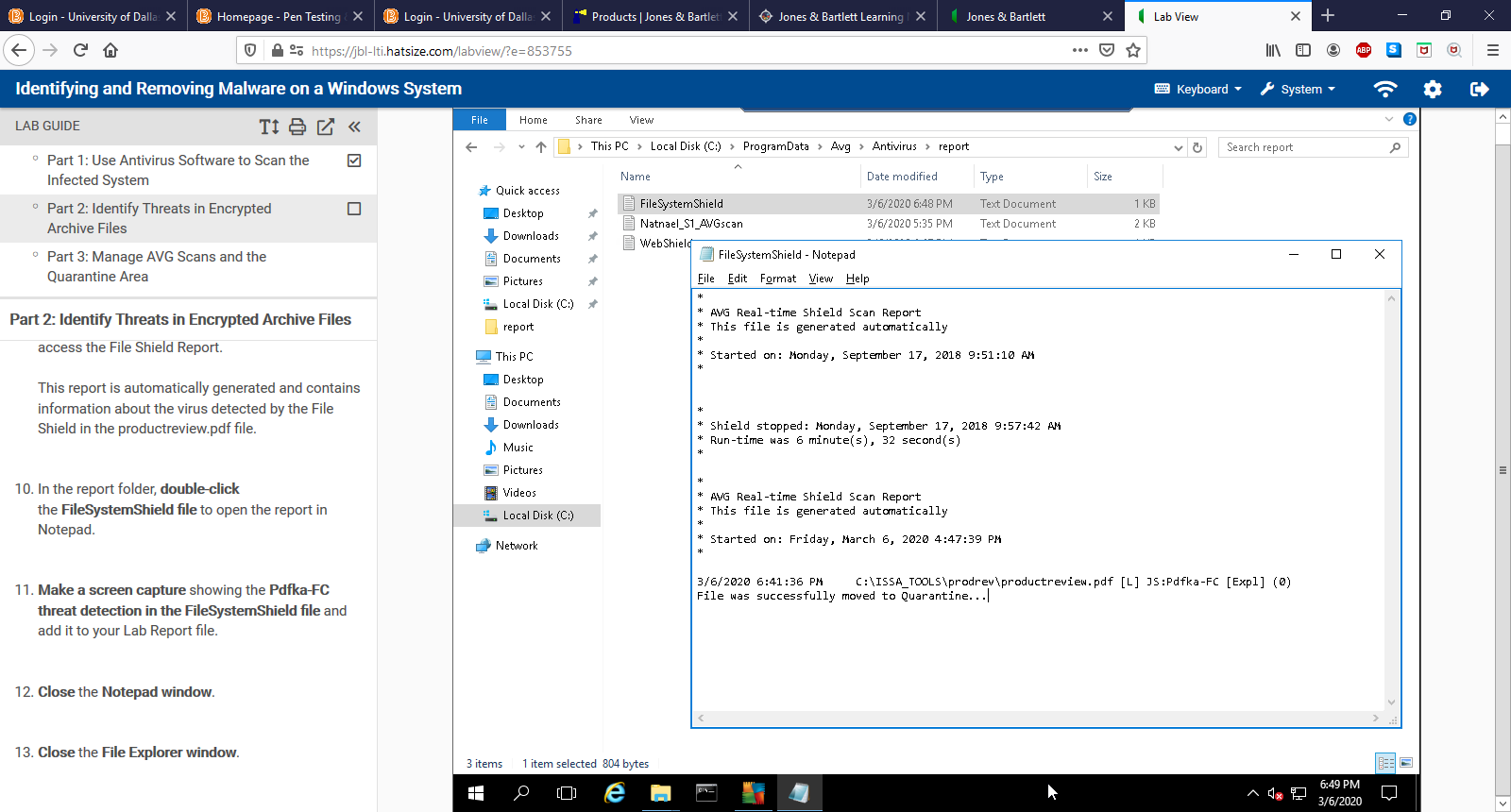
What is Win32:Malware-gen? (n.d.). AVG Home Support. Retrieved from https://support.avg.com/answers?id=9060N000000LnS4QAK

1. Make a screen capture showing the contents of Natnael\_S1\_AVGscan file and paste it into your Lab Report file.



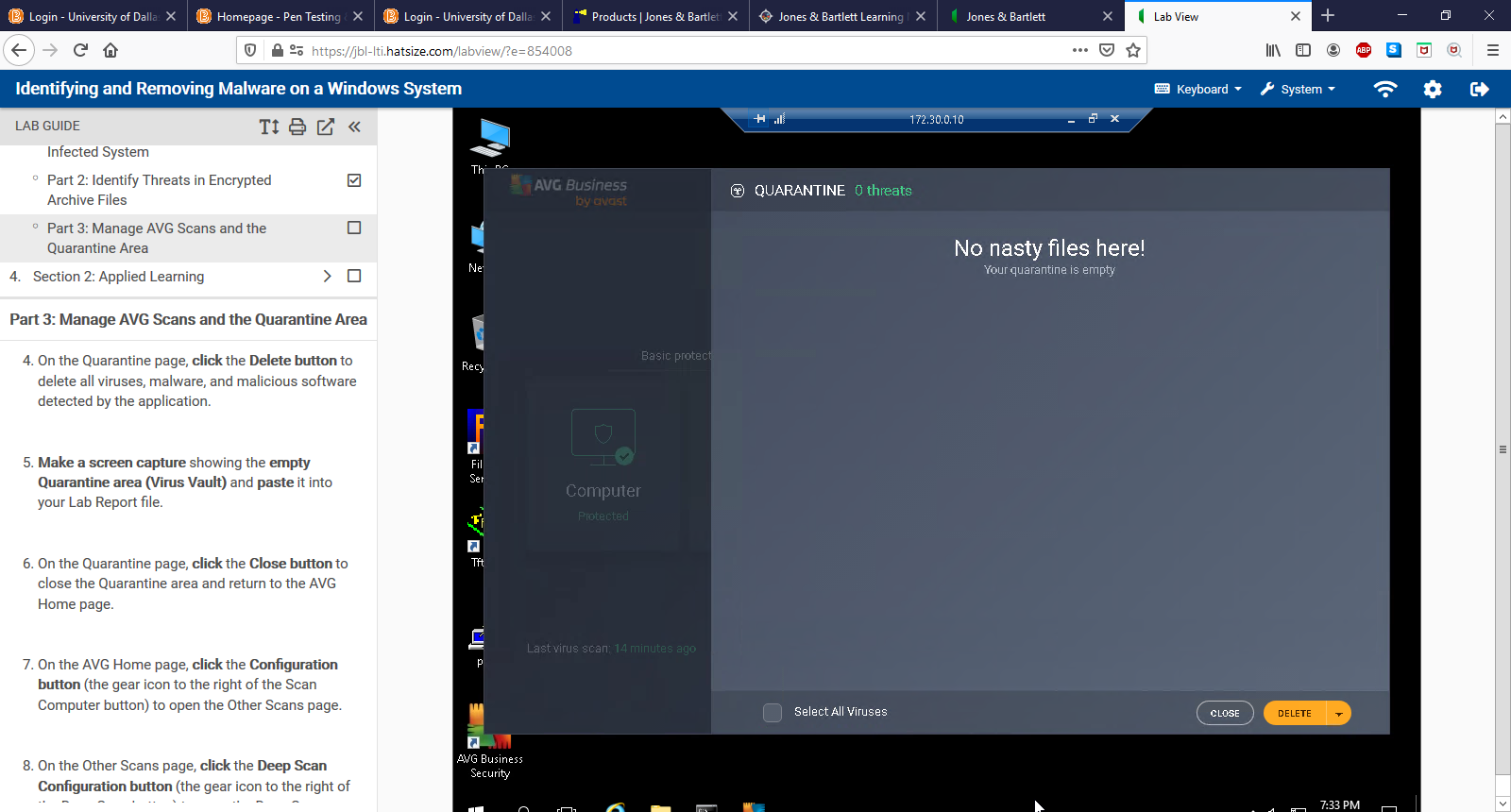
**Part 2**

1. Make a screen capture showing the Pdfka-FC threat detection in the FileSystemShield file and add it to your Lab Report file.

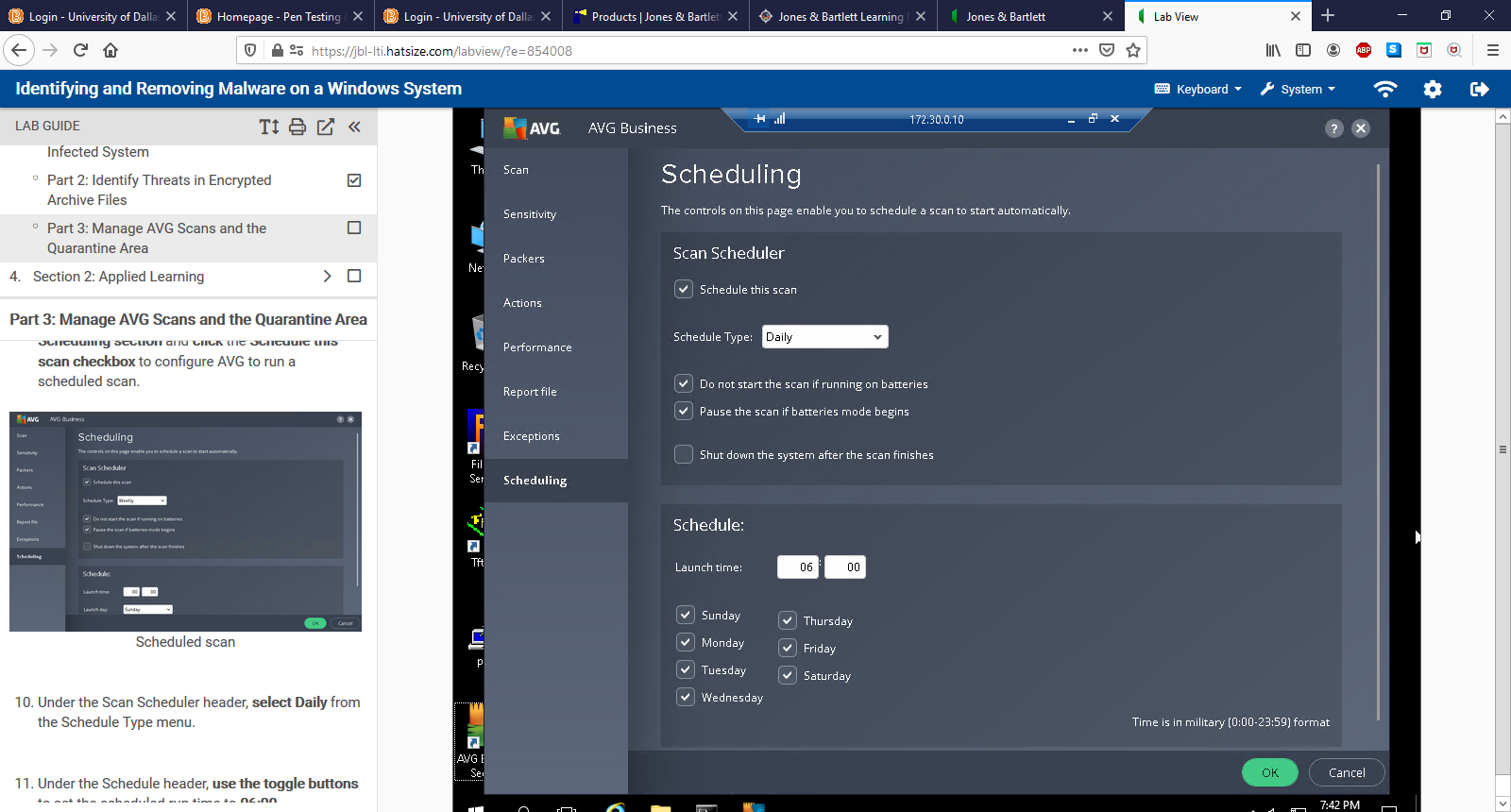


**Part 3**

1. Make a screen capture showing the empty Quarantine area (Virus Vault) and paste it into your Lab Report file.



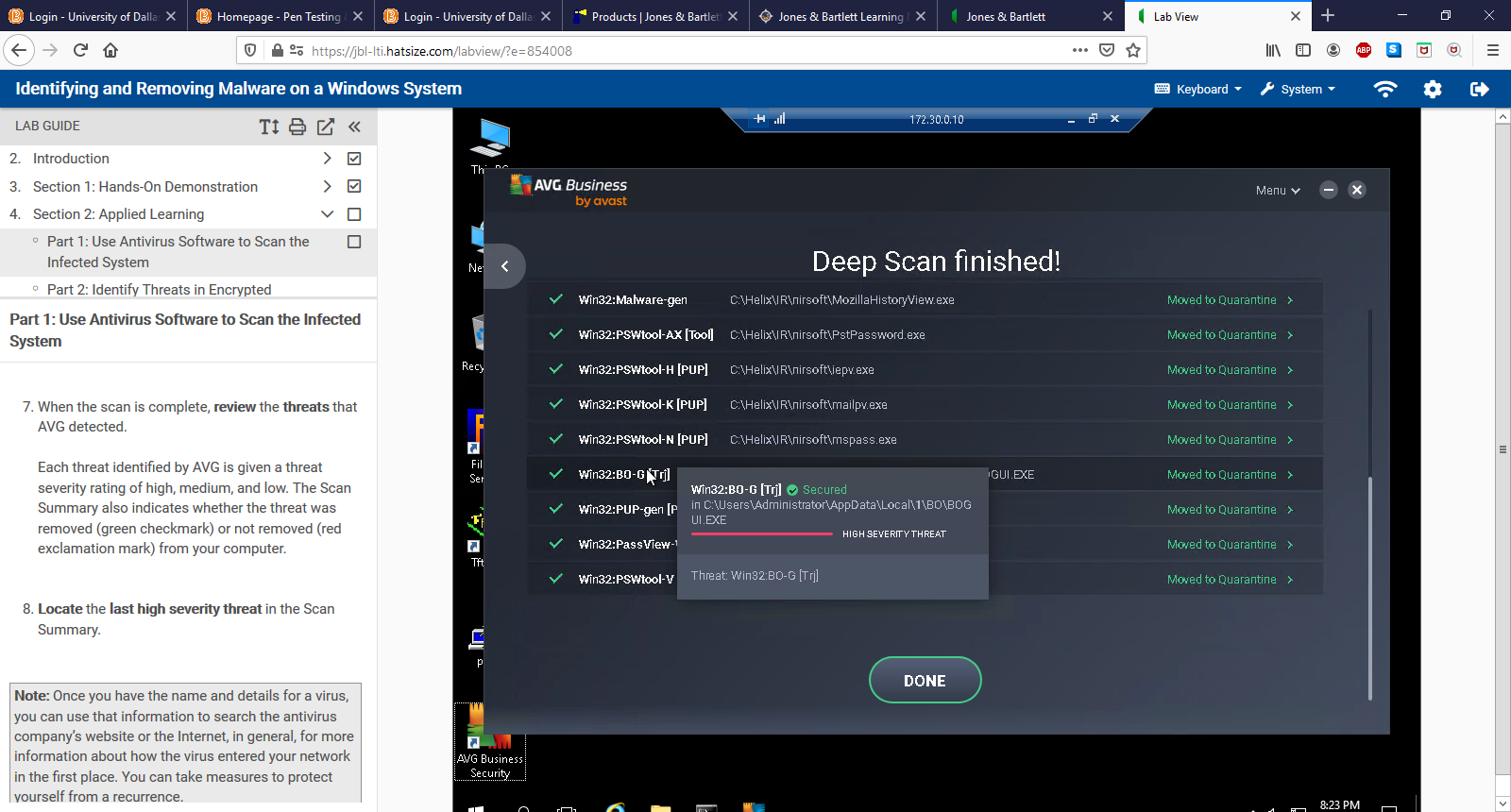
1. Make a screen capture showing the scheduled scan and paste it into your Lab Report file.



**Section 2**

**Part 1**

1. On the scan summary page, locate the last high severity threat. In your Lab Report file, document the threat details.



After identifying the name and details for the high severity threat, the information was then used to search the internet to get more details. Careful researching of the threat tells us that Win32:BO-G is a trojan that targets the core of Windows in order to complete its tasks. It functions by allowing complete remote access for the attacker. As shown above, this malicious instance is identified by Avast as a known threat contained in AVG’s malware database. An alert from AVG warning someone that it detected Win32:B0-G, indicates that a dangerous trojan has been realized on the Windows operating system and that an action was taken to forbid the threat from doing damage.

Reference

Knudsen, k. (2002). Use offense to inform defense. Find flaws before the bad guys do. SANS Penetration Testing. Retrieved from https://pen-testing.sans.org/resources/papers/gcih/tracking-orifice-trojan-university-network-101743

1. Make a screen capture showing the summary information at the top of the Natnael\_S2\_AVGscan file and paste it into your Lab Report file.

