This lab task is centered around using antivirus.

* First, scan with AVG Business to see if there is anything wrong.
* Second, quarantine the files deemed dangerous/suspicious.
* Next, examine files in a safe location.
* Then, keep or delete files accordingly.
* Finally, scan again to ensure safety of file system and automate deep scans for dates in the future.

**First Malware ID’d:**

WIN32:Malware-gen: C:\Helix\IR\bin\cryptcat.exe

**Deep scan file:**

A picture containing text, screenshot, computer, monitor

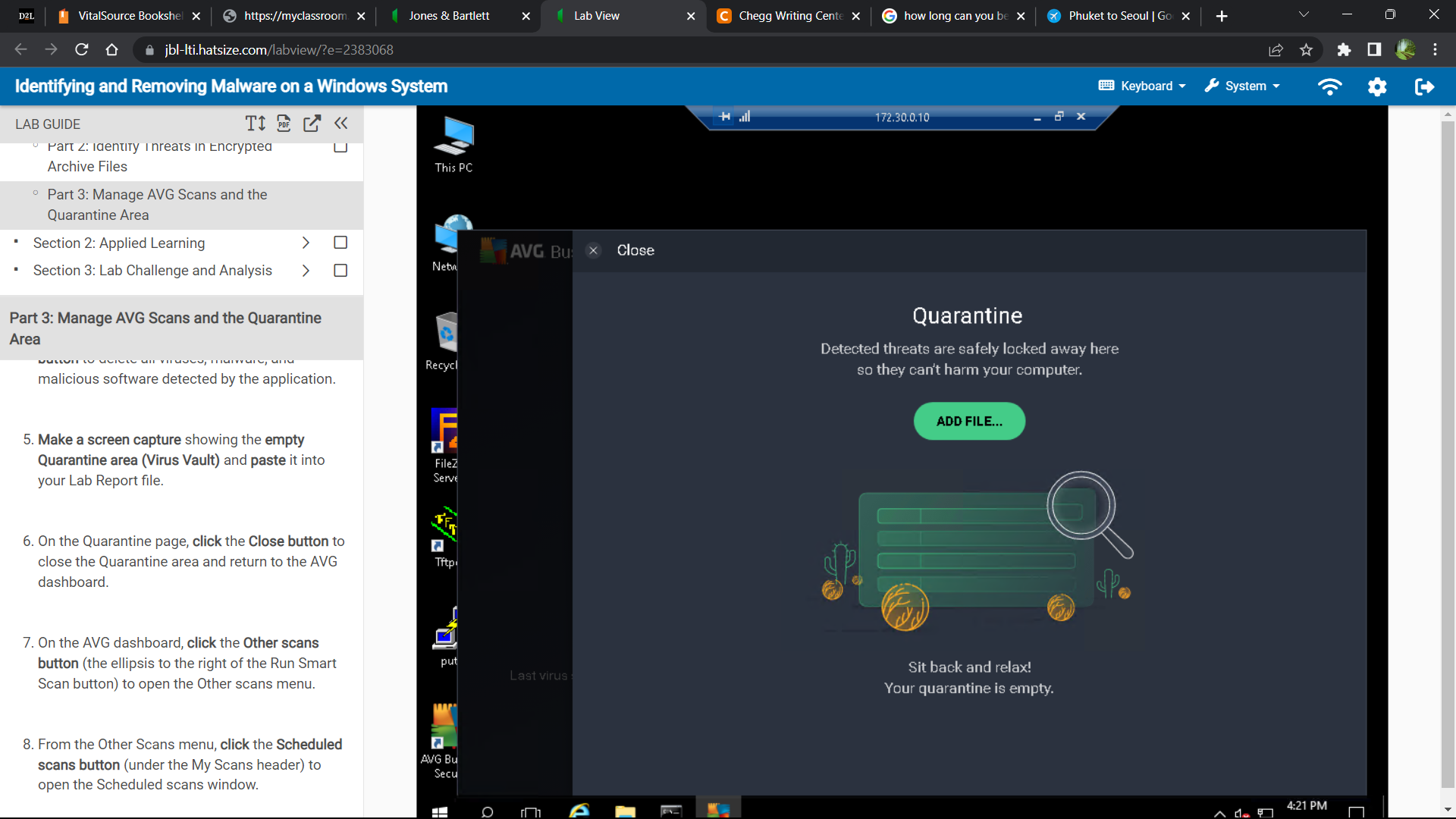
Description automatically generated

**Pdfka-FC:**

Graphical user interface, text, application, email

Description automatically generated

**Empty vault:**



**Daily scan:**

A screenshot of a computer

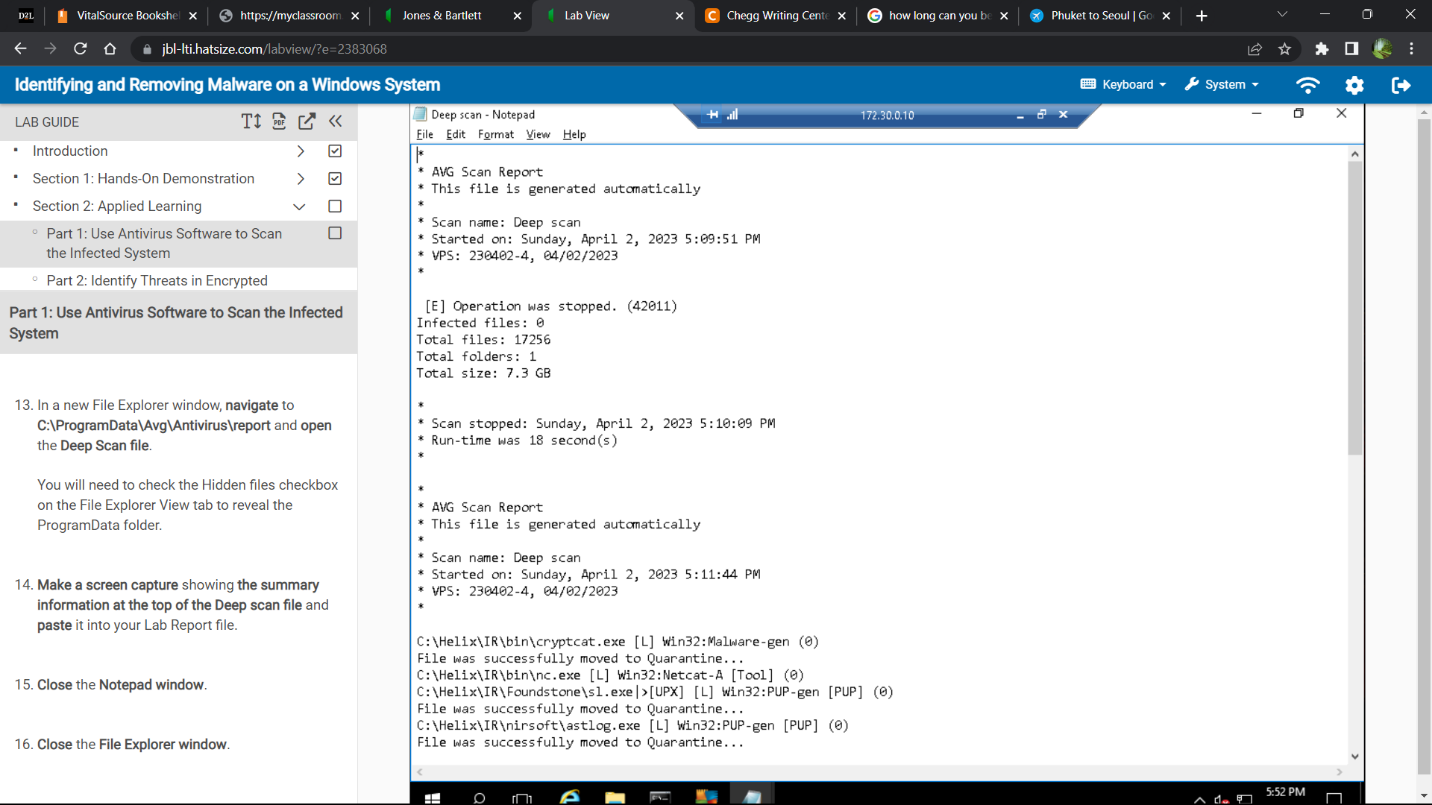
Description automatically generated

**Section 2 found threats:**

Win32: Trojan-gen Netbuster.exe

Win32:BackOrifice BOSERVER.EXE and more from Win 32

**Deep scan section 2 report:**

****

**Winuke file:**

Graphical user interface, application, website

Description automatically generated

**FileSystemSheild file:**

Graphical user interface, text, application, email

Description automatically generated

**Empty quarantine:**

Graphical user interface, website

Description automatically generated

**Daily scans:**

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated with medium confidence