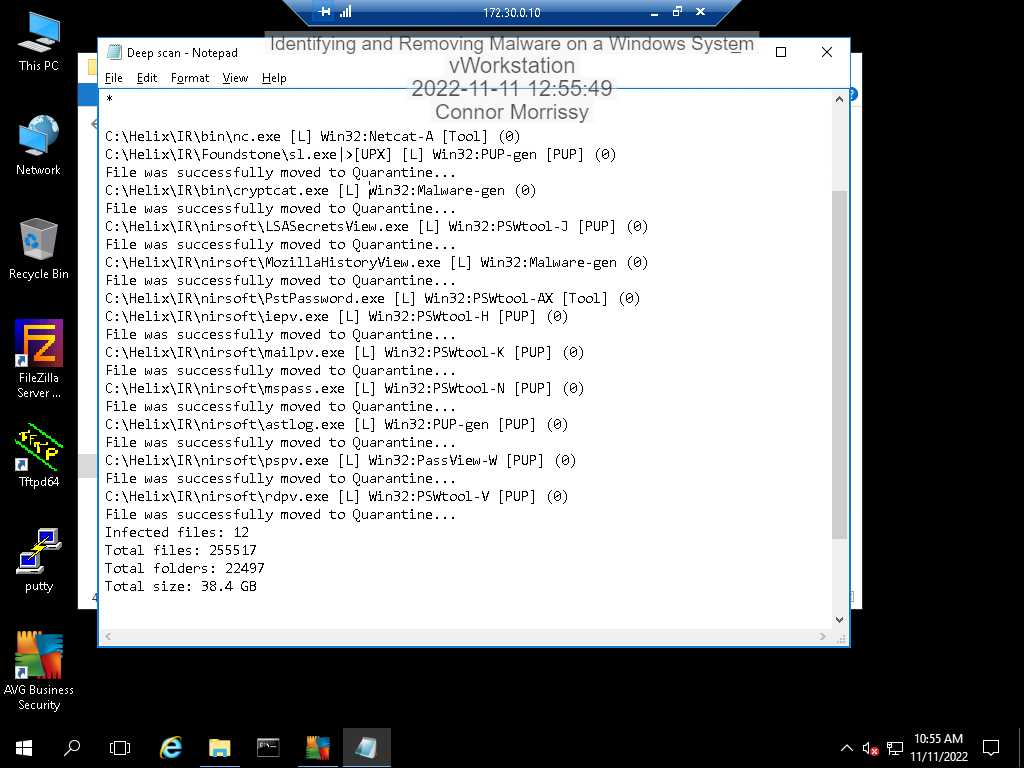
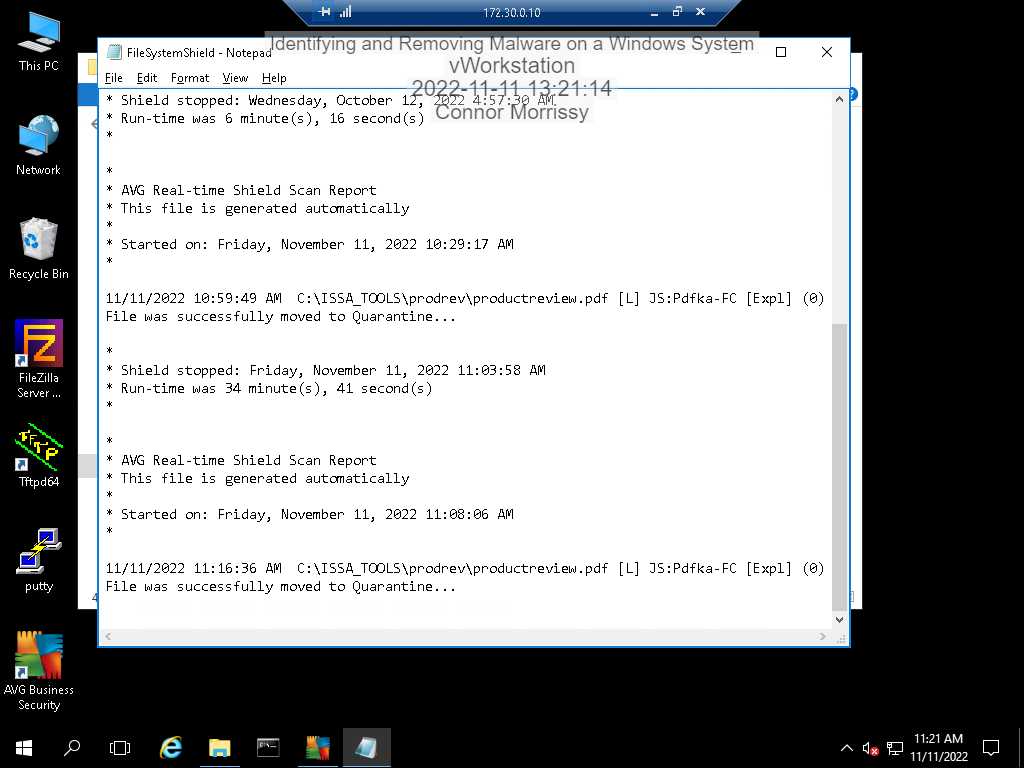
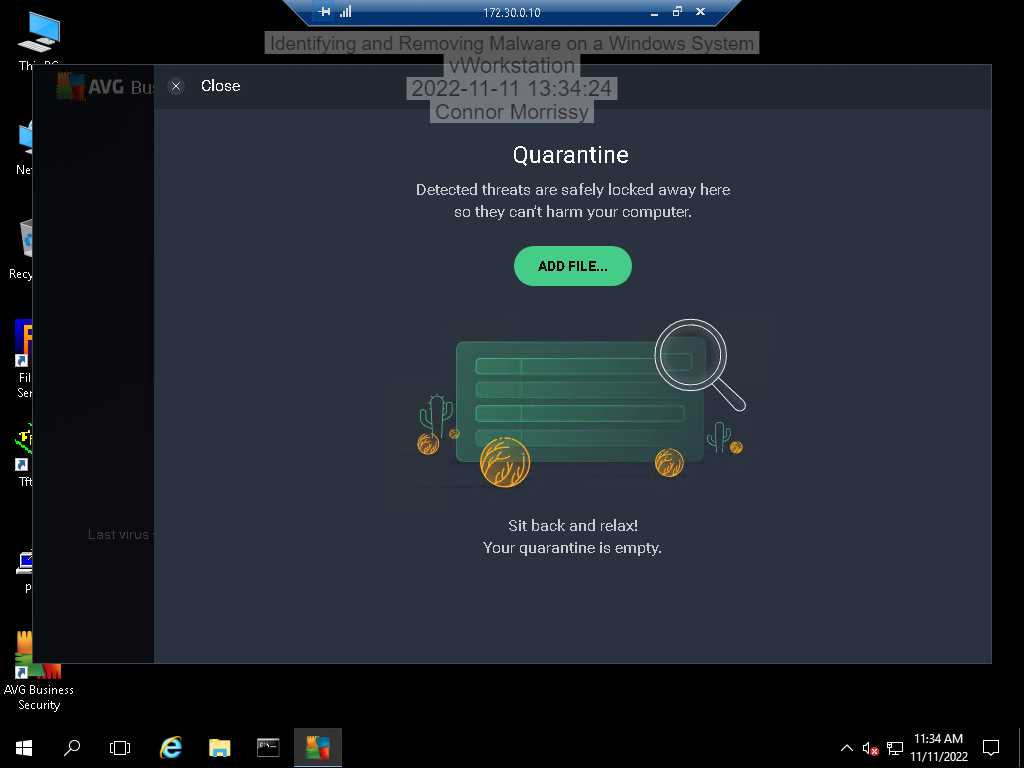
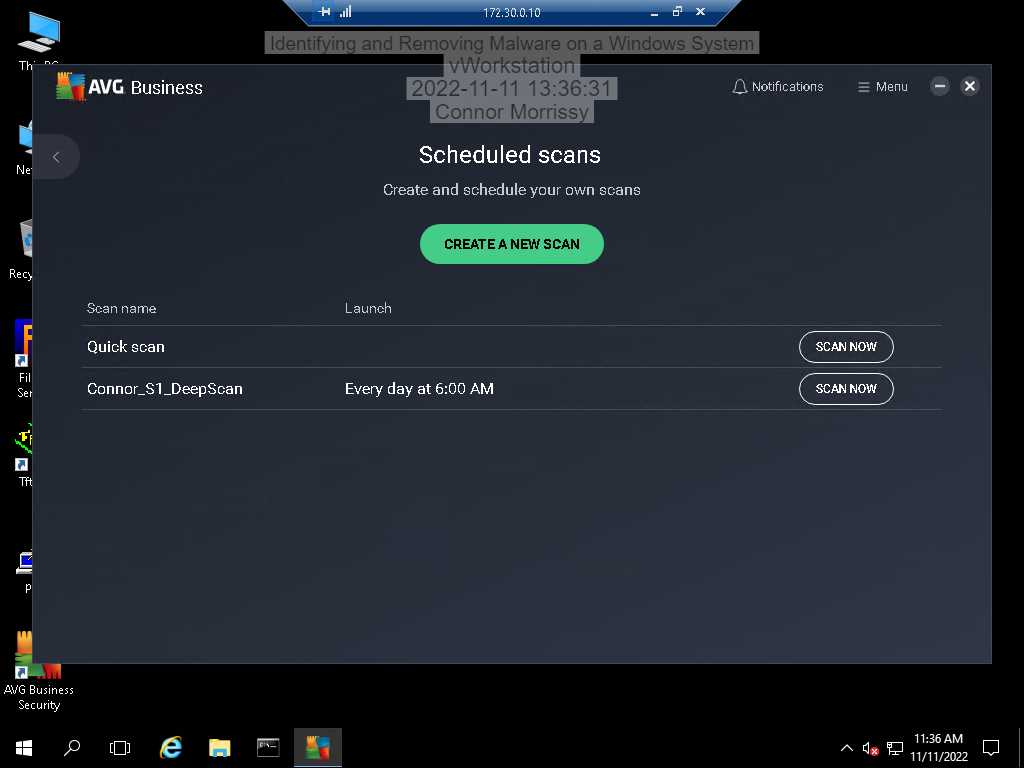
**Section 1:**

Threat: Win32:Malware-gen located in “C:\Helix\IR\bin\cryptcat.exe”



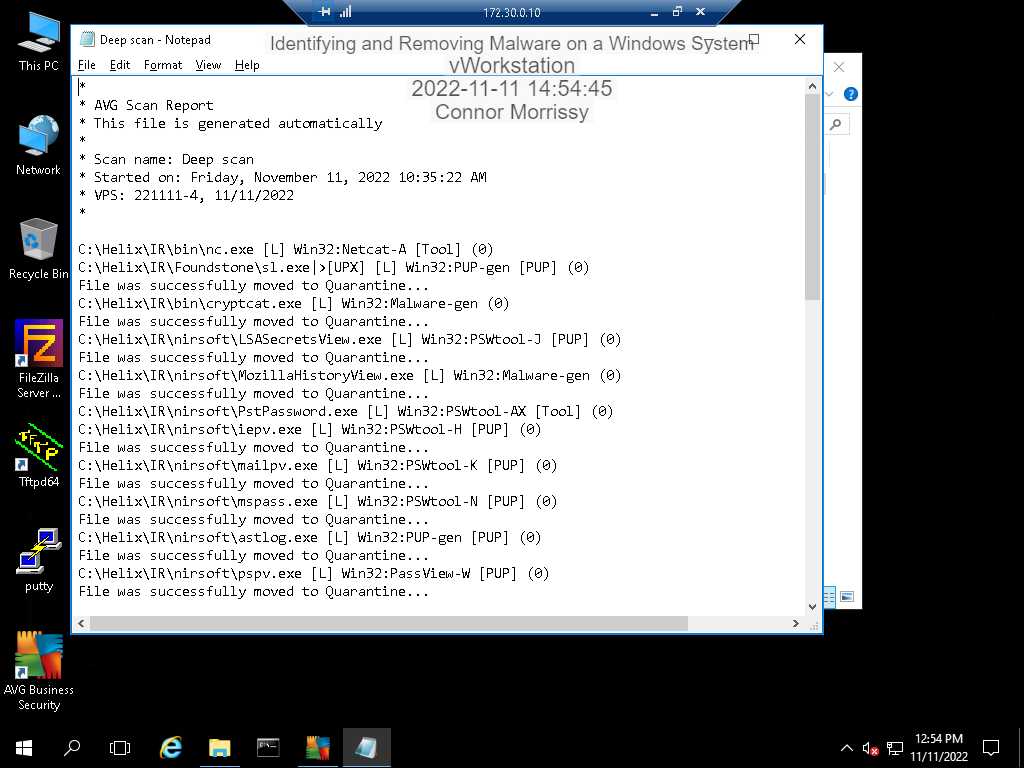


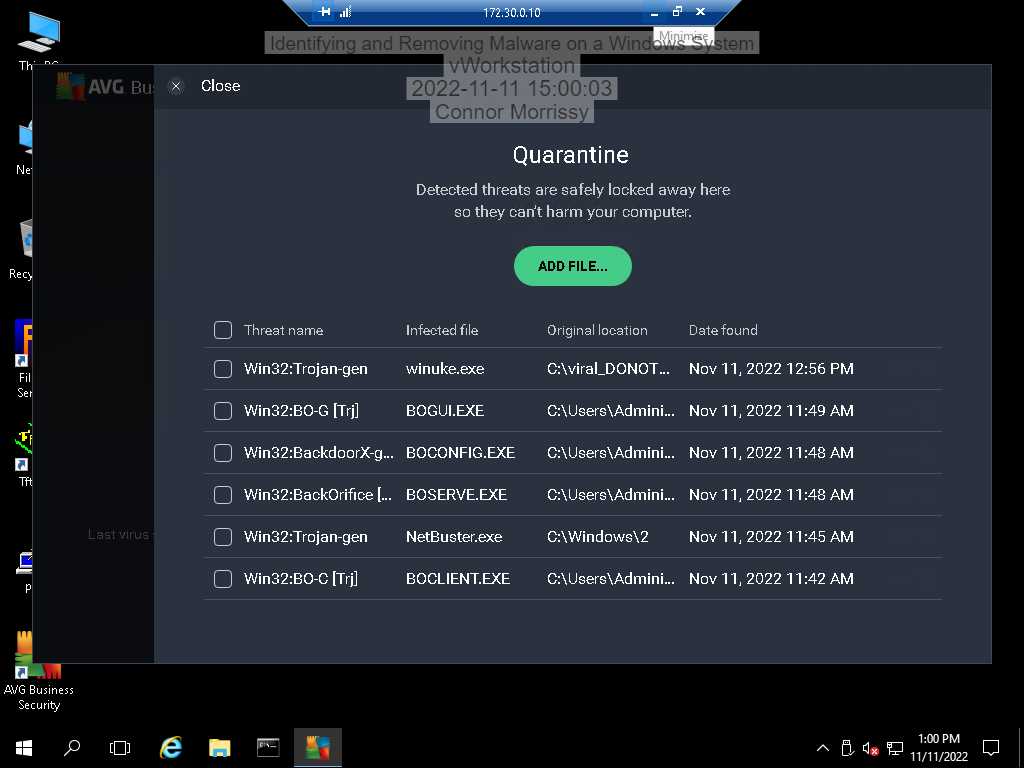


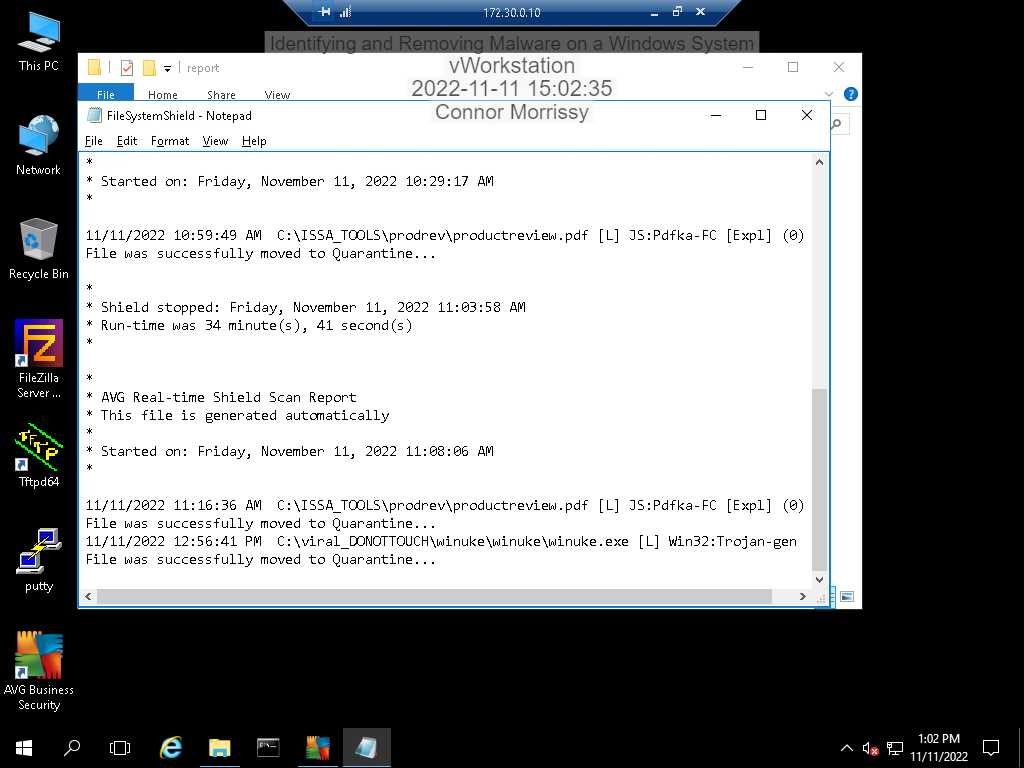


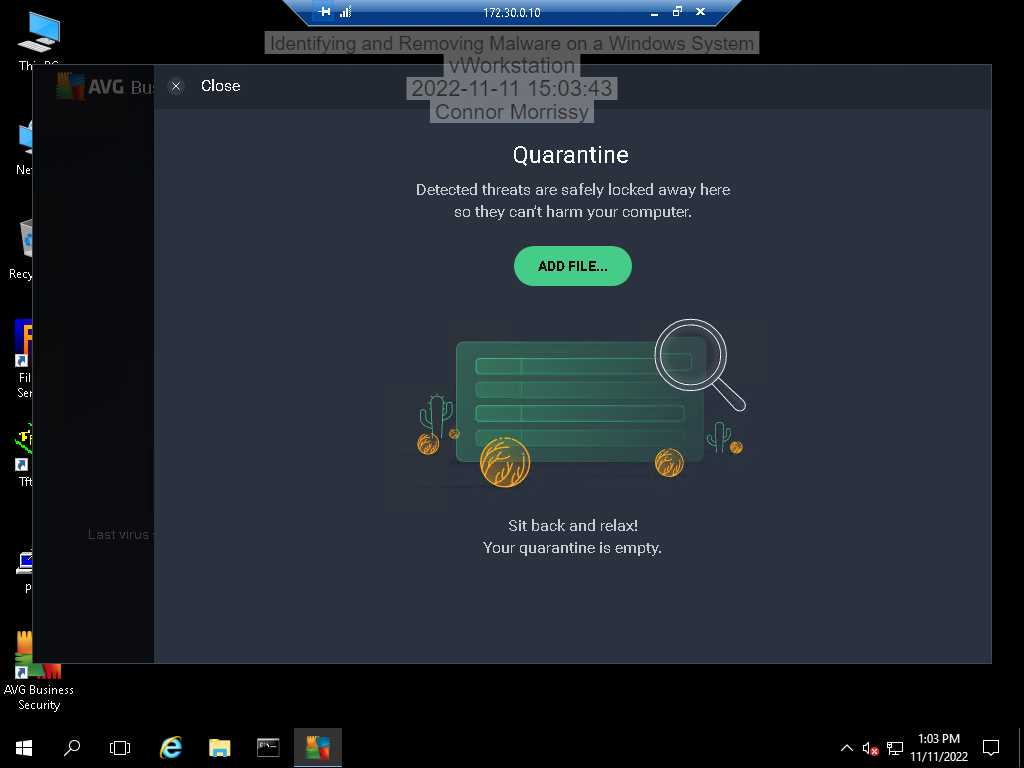
**Section 2:**

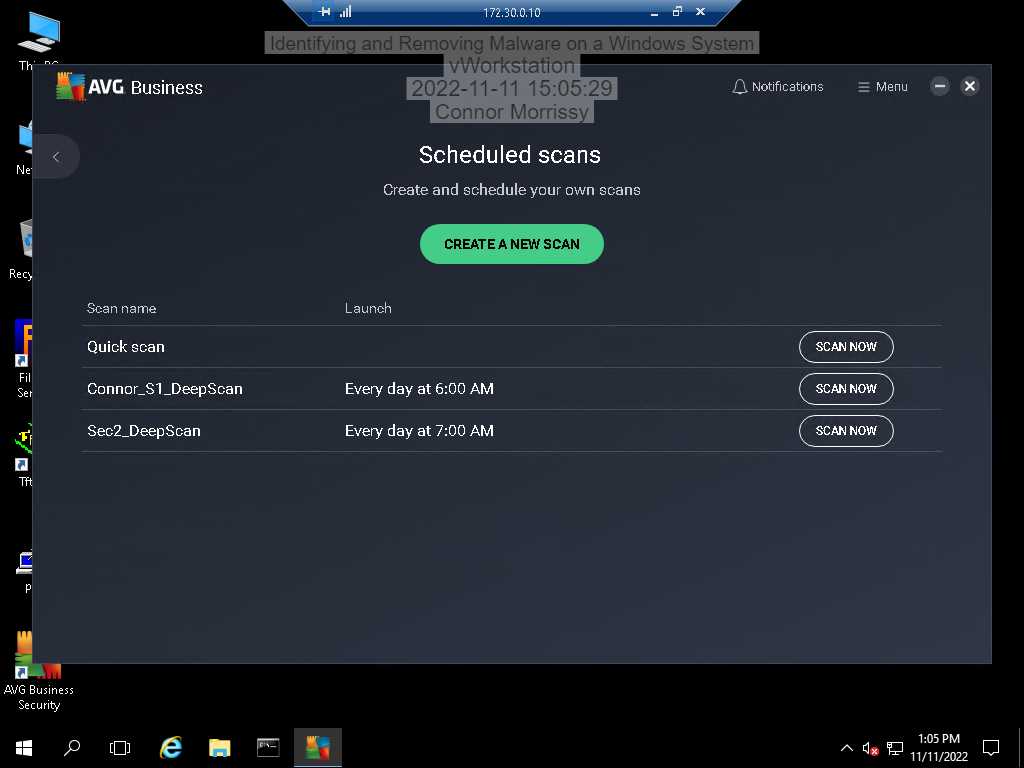
Threat: Win32:Trojan-gen located in “C:\Windows\2\NetBuster.exe”











**Section 3:**

**Part 1:**

WinNuke is a remote Denial of Service attack that was present on Windows 95, Windows NT, and Windows3.1x operating systems that crashes the system. It’s not really dangerous today as these operating systems are no longer supported or used much. It’s also not a virus and cannot spread by itself.

**Part 2:**

Three of the best/most common home-use antiviruses are Kaspersky, Bitdefender, and Norton. Kaspersky and Bitdefender both have more features and perform better than Norton. It’s a tough choice between Kaspersky and Bitdefender, but for my personal home use, I would probably pick Kaspersky mostly because there is a free version. If price didn’t matter I would probably choose Bitdefender because it seems that it has less overhead, which I think is very important for an antivirus.

**Part 3:**

I extracted the files from the C:\viral\_DONOTTOUCH folder to the Desktop (since the lab said not to extract to the same folder), and the items were successfully extracted to the Desktop, including the WinNuke folder items, which would get quarantined by the AVG antivirus if it was extracted to the C:\viral\_DONOTTOUCH folder. I’m not really sure why this is, because both the Desktop and the C:\viral\_DONOTTOUCH folder are not included in the exceptions on AVG, so I thought AVG should still scan and quarantine the malware.