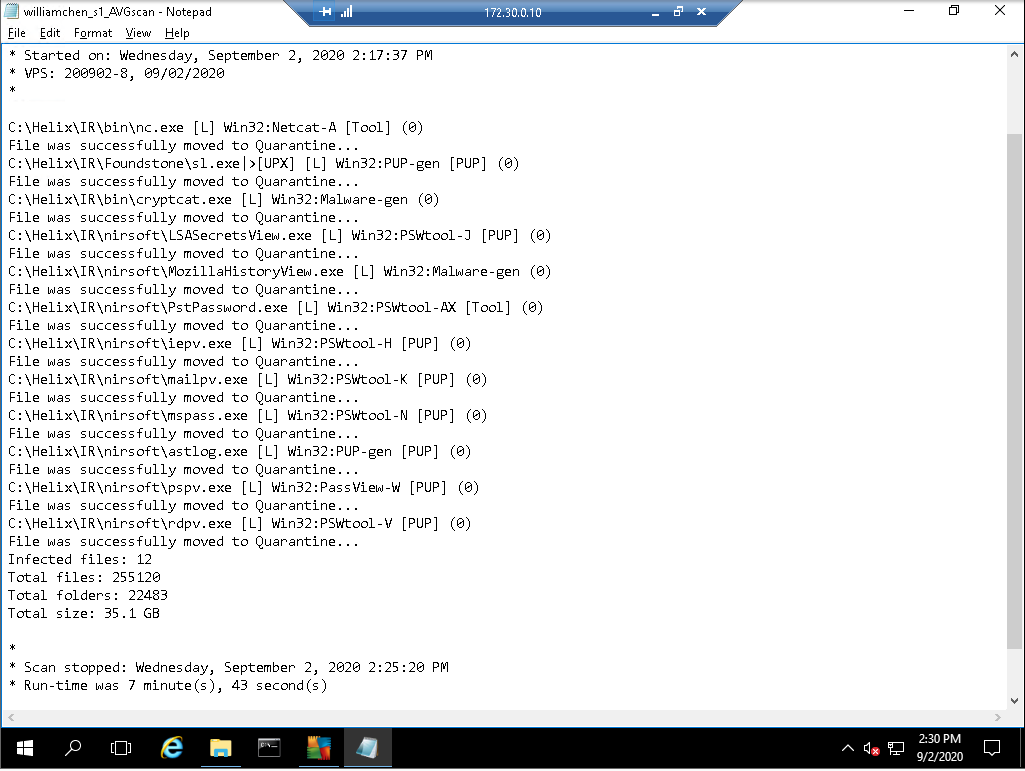
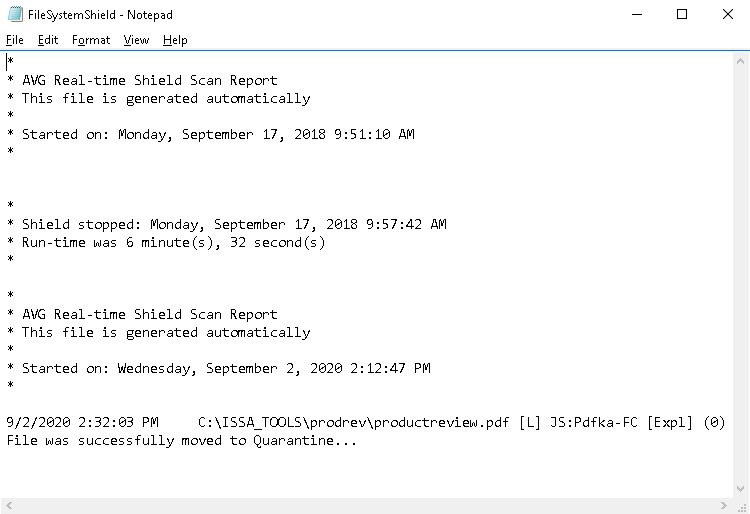
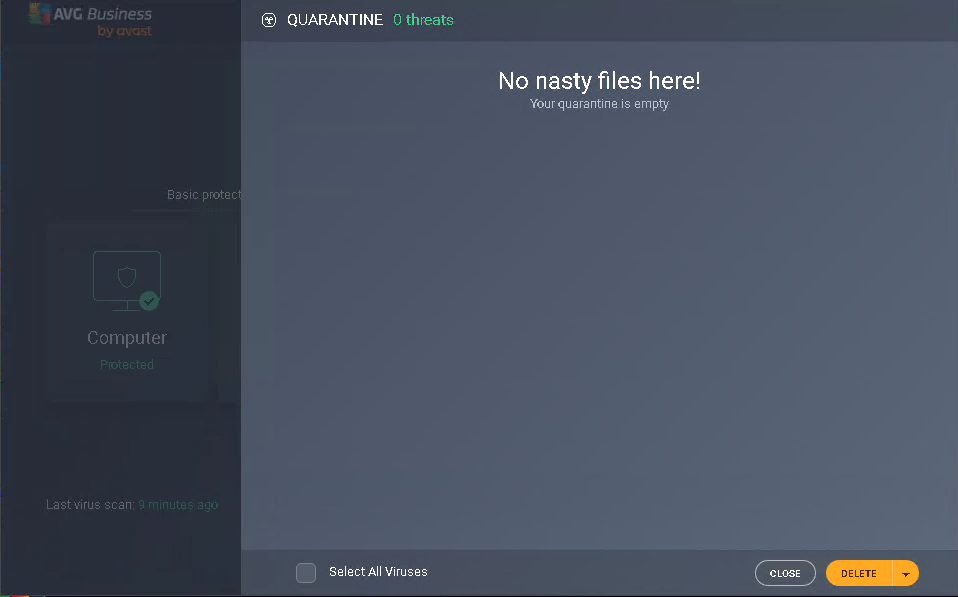
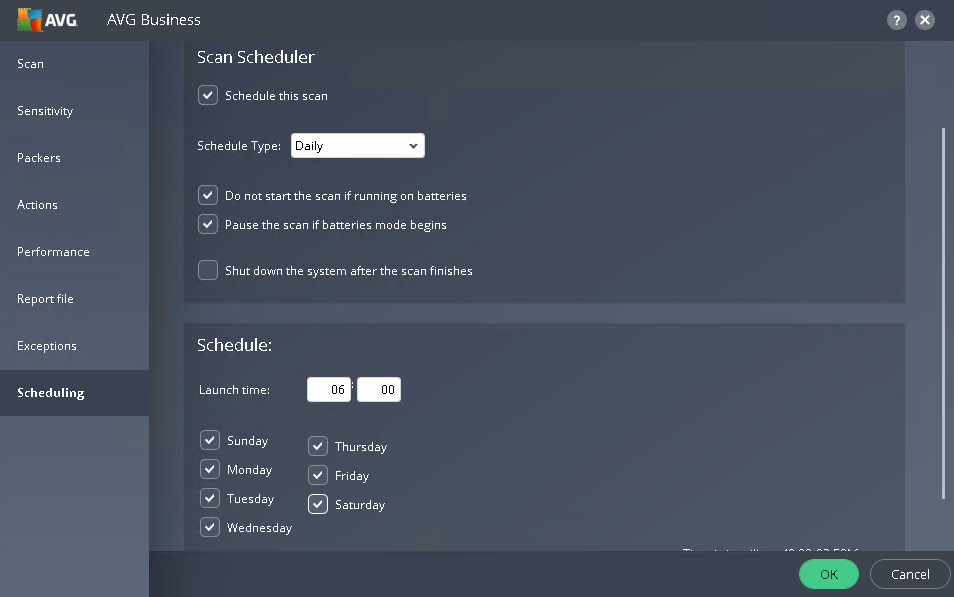
William Chen IST 323 – M002

Professor Christopher Croad 09/02/2020

**Lab #1 - Identifying and Removing Malware on a Windows System**

1. **Section 1, Part 1, Step 26: Scan report file**
2. **Section 1, Part 2, Step 11: Pdfka-FC threat detection**
3. **Section 1, Part 3, Step 5: Empty quarantine area**
4. **Section 1, Part 3, Step 12: Scheduled scan**

**Section 3, part 1:**

At the time of the release (1997), WinNuke was considered dangerous because it would crash the computer of the victim of the attack. WinNuke is a denial of service attack that affects Windows 95, Windows NT, and Windows 3.1x. The way it worked was the program would connect to port 139 of the person being attacked, and WinNuke would send junk data to that port using out-of-band data. By using out-of-band data, the computer would prioritize this data since the data would be sent directly to the receiving end, rather than going through a series of “tunnels”. WinNuke was also considered dangerous at the time because someone could constantly crash your computer and make it seem like it was a hardware fault (since it showed the blue screen of death). Luckily, Microsoft released a patch to fix this. WinNuke came back in 2002 but was quickly patched by Microsoft. WinNuke is no longer considered dangerous because of Microsoft's updated security measures, and the odds of an attack like this happening now are slim to none. An attack like this could only happen if you had a computer running one of the operating systems affected and if the OS wasn't updated to patch the attack.

**Section 3, part 2:**

The three anti-virus programs that I decided to look at are Bitdefender, Kaspersky, and AVG. Although all three of these programs have subscription options with better protection, I wouldn’t pay for an anti-virus. Comparing these three options, they all offer computer performance “enhancement,” which supposedly helps the computer run quicker and smoother. Although they all protect against viruses and malware, Kaspersky’s description of their protection is very broad. It just says that they protect against viruses, ransomware, and more. These are the only functions of the free Kaspersky program and seem very basic, just like Windows Defender, which is automatically installed on all computers running Windows 10. My second choice would be AVG since it offers browsing and download protection. Bitdefender does all of the above, along with anti-fraud and anti-phish, which is why I would pick Bitdefender as my anti-virus program. I have had multiple problems with ransomware and other random malware in the past but still don’t have any anti-virus’ installed (I have alternative protection measures). Bitdefender seems like the best option out of all three, and I could benefit from it since I like to buy stuff online a lot, and I download lots of files. Bitdefender is also more well known to have better protection, which is another reason I would choose Bitdefender over the others. Bitdefender also offers a little bit of everything, which the other programs don't.