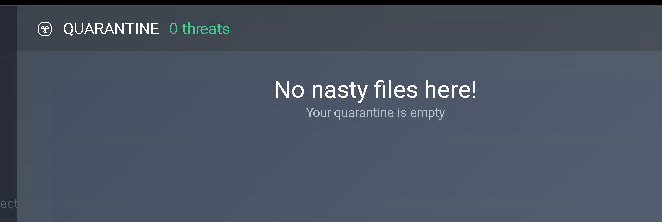
SECTION 1: Hands-On Demonstration

Part 1: Use Antivirus Software to Scan the Infected System

9. Make a screen capture showing the number of threats identified by the AVG scan

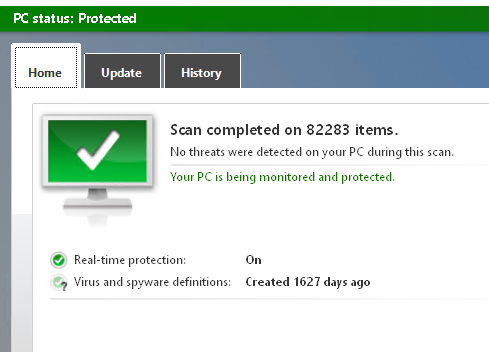


17. Make a screen capture showing the empty Quarantine (Virus Vault)

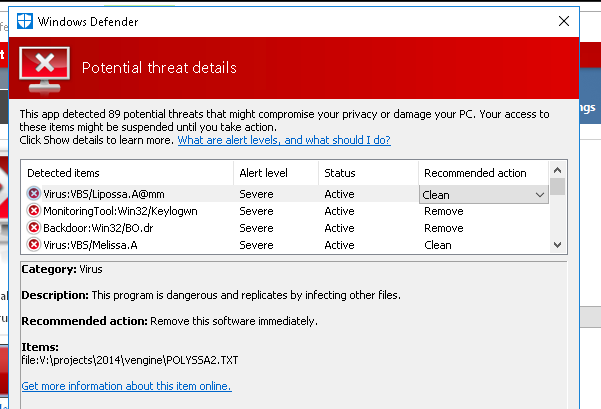


Part 2: Scan Windows Server 2016 with Windows Defender

41. Make a screen capture showing the number of potential threats identified by the scan



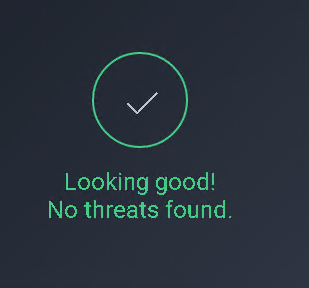
44. Make a screen capture showing the successful completion of the cleaning process



SECTION 2: Applied Learning

Part 1: Use Antivirus Software to Scan the Infected System

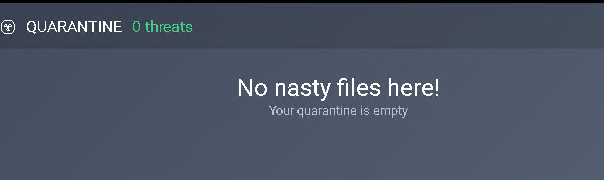
5. When the scan is complete, make a screen capture showing the number of threats identified in the AVG scan



7. Make a screen capture showing the details of the VBS:Agent-FS (Wrm) threat associated with \\172.30.0.16\viral\projects\vengine.zip|>MELISSA.txt

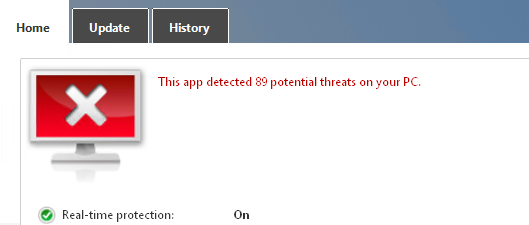
I didn’t get any threats.

11. Make a screen capture showing the emptied Quarantine area (Virus Vault)

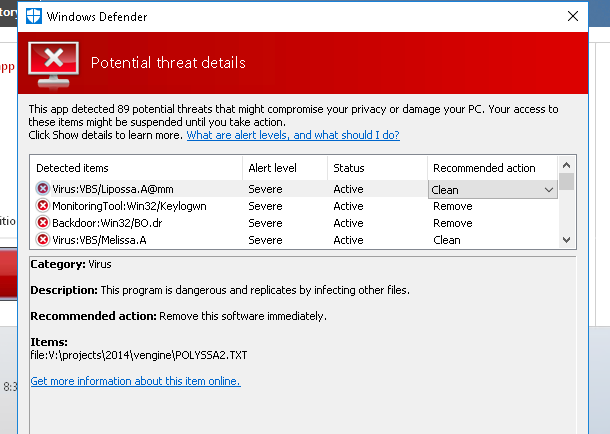


Part 2: Scan Windows Server 2016 with Windows Defender

9. Make a screen capture showing the number of threats detected by Windows Defender



12. Make a screen capture showing the threat details window



SECTION 3: Observation Summary

Part 1 of Section 1 talks about symptoms of a virus. I actually have an interesting experience with this. My laptop had a virus and I figured it out from the behaviour of my laptop fans. My laptop fans would be loud even when I am not doing anything with the computer, indicating that cpu is working hard. This is normal behaviour if it happen rarely which could indicate an update. But it happened all the time so when this weird behaviour caught my attention, I decided to open the task manager to see what task is causing cpu to work hard. Whenever I opened the task manager cpu and the fans would calm down. Sneaky. So I backed up my date and formatted the laptop. The problem went away.

**Section 1 Part 1:** We RDP into the target1 computer. We open AVG, remove a file from the exception list and start a scan. The some of the malware in the detected malware list is cryptcat, mailpv, bo, boserve. They are all executables. Which means they have been compiled down to machine code.

cryptcat.exe is an executable file that is part of Anti-Hacker Toolkit developed by McGraw-Hill Companies.

mailpv.exe is an executable file that is part of the Mail PassView program developed by NirSoft.

bo.exe is an executable file that is part of StockBase POS developed by EGA Futura.

BOSERVE.EXE is an executable file that is part of Hacker's Handbook developed by Dark Bay Ltd..

We then deleted all the files in quarantine.  
  
  
**Section 1 Part 2:** We then RDP into the second computer. We disable web shield and file shield of AVG. We restart the computer and disable AVG. We exclude C drive from windows defender. Then we do a windows defender scan. Then we scan the V drive with windows defender and found 89 threats.

**Section 2 Part 1:** We RDP into the second computer. We update the AVG. We scan V drive with AVG and find no threats.

**Section 2 Part 2:** We install windows defender, restart the computer, RDP into the second computer again, exclude C drive from windows defender, scan V drive and find 89 threats.