Name(s): Abdullah Mujahid

Lab 3.1.A: Sandboxing Malware

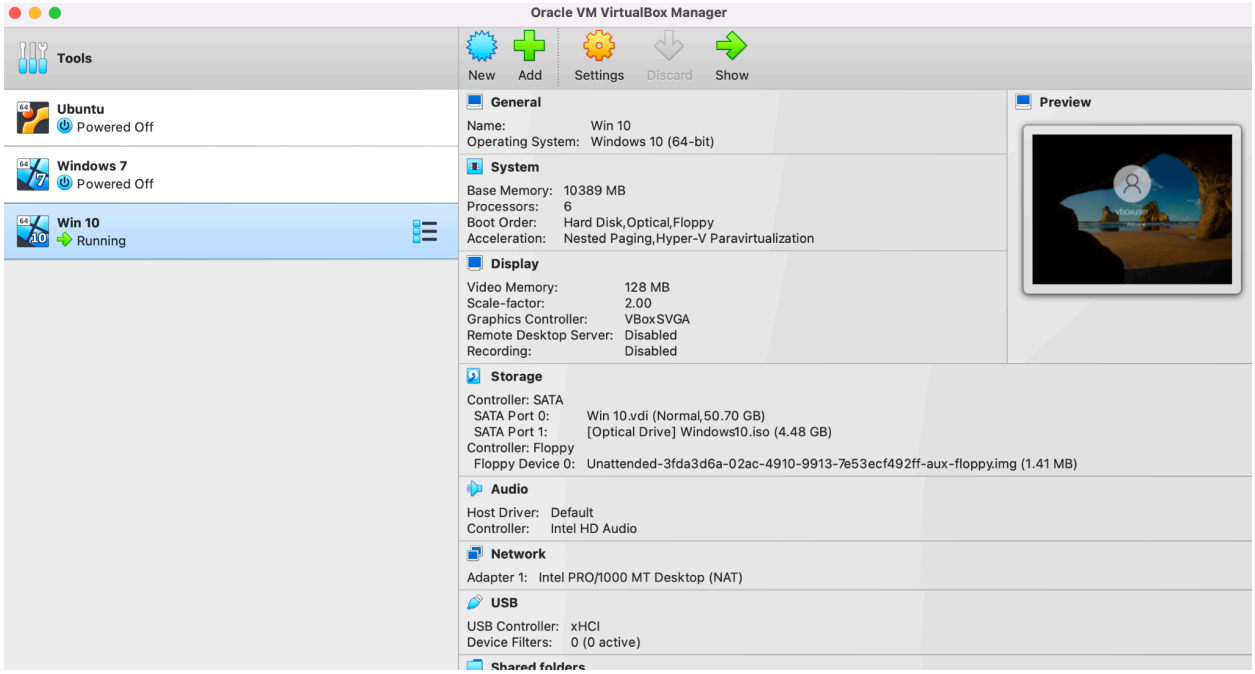
Part 1: Creating a Sandbox Environment (30 Points)

- [x] ~~Utilize the following resources to install a windows 10 virtual machine which you will be using as a "sandbox" to test malware.~~
    - Windows 10 ISO: Windows.iso
    - Reading Tutorial: How to Install Windows 10 in a Virtual Machine
    - Video Tutorial: How to Install Windows 10 on Mac using VirtualBox

      ***Note**: After Windows 10 installation is complete, log in with a "corporate account" so you can create an offline account.*

1. Screenshot of Windows 10 VM installed on your MAC: (2 Point)

   Screenshot:



2. What is sandboxing? (3 Points)

   Answer: Sandboxing is when you create a separate and safe area where you can run/test software/malware. It's used to safely test programs so your main pc system won't be affected or so your network won't be affected.

3. Why is virtualizing an effective means of sandboxing and testing malware? (4 Points)

Answer: Virtualizing Is an effective means for sandboxing/testing malware/software, since its a separated Operating System on top of your original system. So what you do on the VM does not affect your actual PC. But it takes resources away from the original device, which means it would be powerful enough to test malware, while being in an isolated environment to see its effects.

4. **Critical Thinking**: Why are we sandboxing on Win 10 as opposed to Windows 11? (4 Points)
   Answer: Windows 10 is more tailored to those who know what they are doing, while windows 11 is tailored to people who have less technical knowledge.

☑ ~~Connect your MAC to a wifi router before continuing with the malware analysis.~~

5. Why is it essential to put your sandbox on a separate network from your primary network network? (4 Points)
   Answer: If you keep the sandbox on your primary network, there's a chance that the malware you test will infect it, which is why you should put it on a separate network, just for a precaution.

6. Now that your VM is installed, use the following video and readings to complete the following steps and questions. Be sure to screenshot for each as you go through the lab:
   On your Windows 10 VM:
   - **Video**: How To Setup A Sandbox Environment For Malware Analysis
   - **Reading**: How to Build a Custom Malware Sandbox

   ☐ Install the following applications
   - ☑ ~~Extractor tool from Windows Store (Ex: Unzip, Winrar)~~
   - ☑ ~~Wireshark~~
   - ☑ ~~Download 3 Photos (be sure that they are appropriate)~~





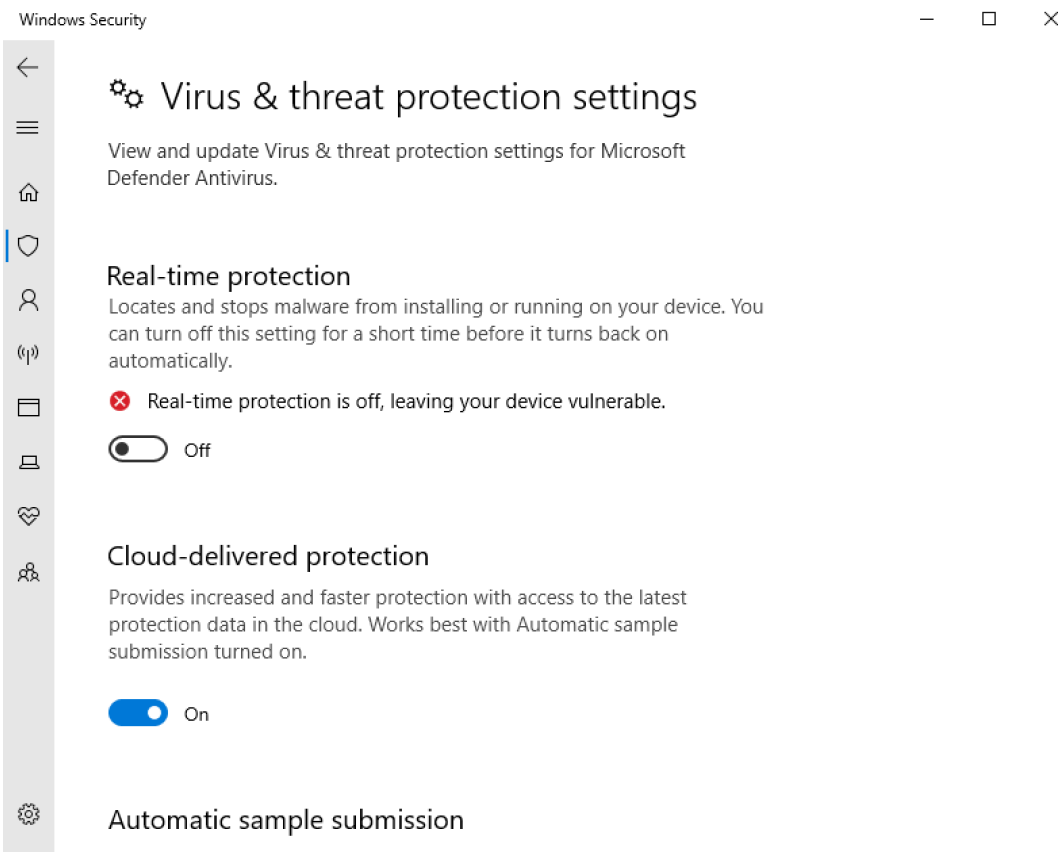


a. Why is it important to install day to day applications on a sandbox environment? (3 Points)

Answer: It is important to install day to day applications on a sandbox environment, to test software which allows people to see whether or not that application is safe or not.

☑ ~~Disable Windows security (Virus & Threat Protection Settings)~~ ~~(2 Point)~~

b. **Screenshot**:



☐ Install FakeNet from the following Website on your VM

c. What role will Fakenet play for your sandbox when you have an active malware on the system? (4 Points)

Answer:

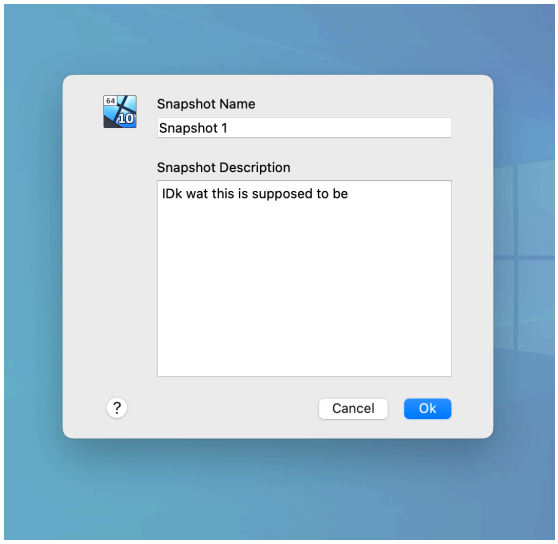
Screenshot:

☐ Take a snapshot of your VM. (4 Points)

d. Why is this an essential step?

Answer: Snapshots are essential because they serve as a "checkpoint" to revert to when something goes wrong.

Screenshot:

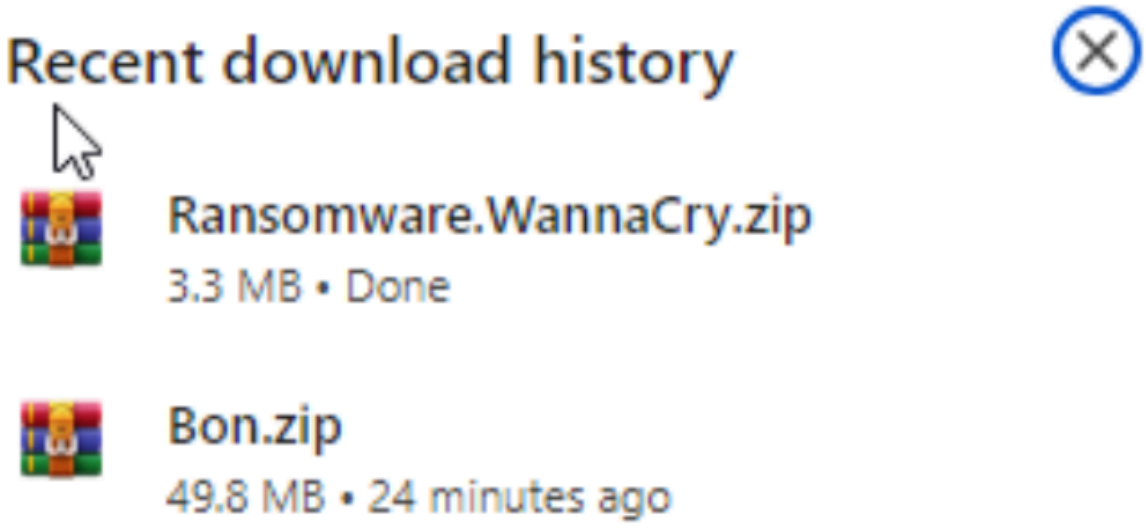


Part 2: Installing & Analyzing Malware (25 Points)

Directions: Once your Windows 10 is installed, complete the following steps. BE SURE TO FOLLOW EACH STEP CAREFULLY IN ORDER TO PROTECT YOUR HOST SYSTEM!

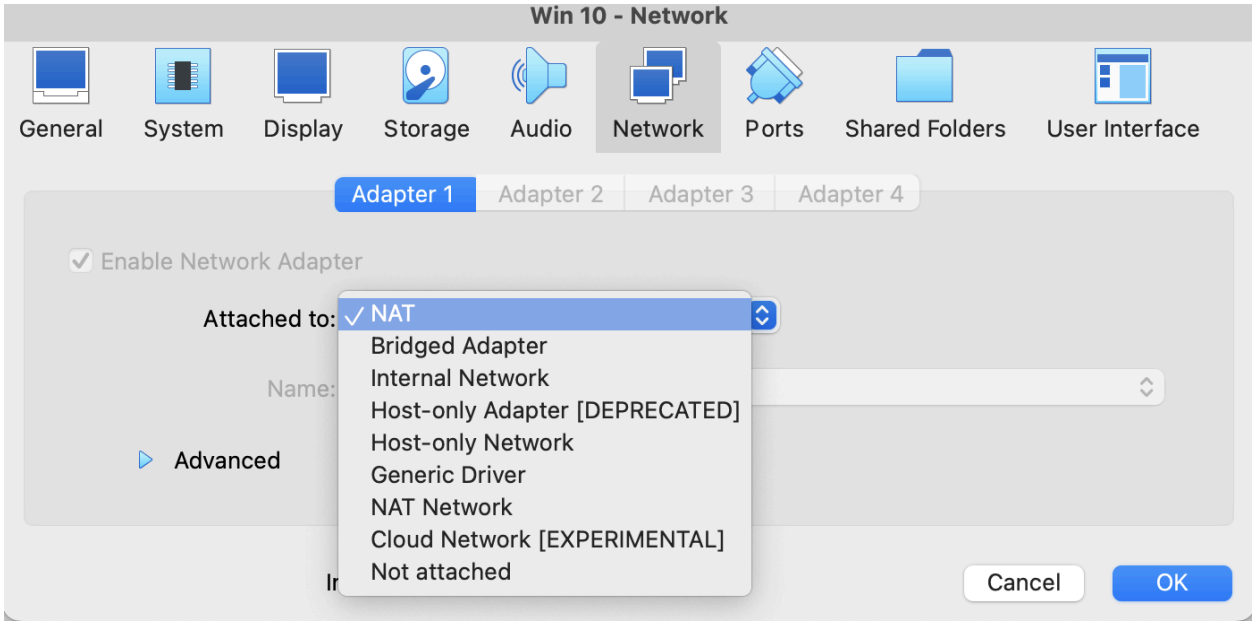
- ☑ ~~Use the following sites to download the malware~~
  - ☑ ~~"Trojan.Bonzi.Buddy"~~
  - ☑ ~~"Ransomware.Wanacry"~~

Screenshot: (2 Point)



- ☑ ~~Open up virtualbox settings for your windows 10. On the network tab, set your network adapter to "Host Only Adapter." – See image below~~
- ☑ ~~Restart your VM~~

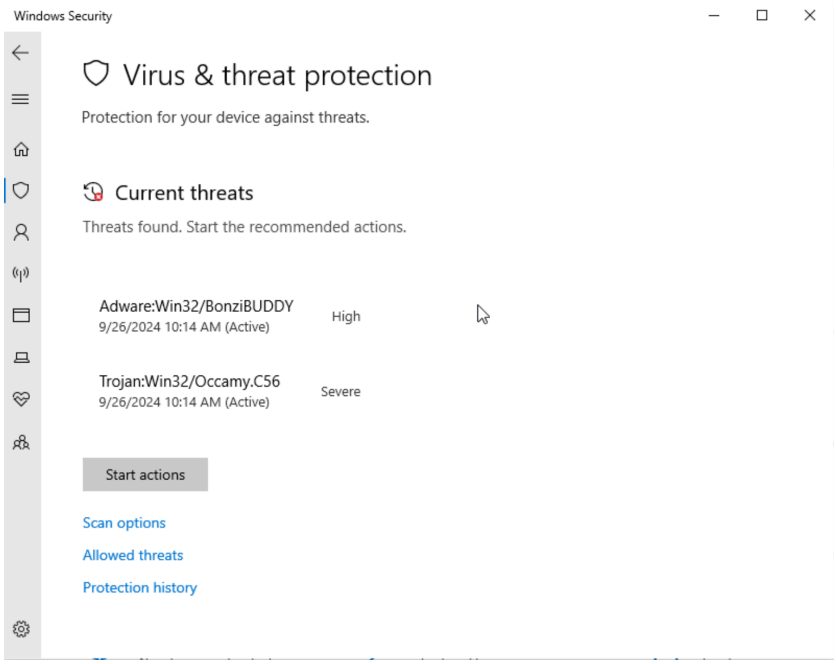
Screenshot: (2 Point)



7. **Critical Thinking**: Why is the previous step ESSENTIAL before you begin conducting experiments and analyzing malware? *(Hint: What effect does setting host-on adapter have on the host and on the VM)* (5 Point)
   Answer: This is essential because it makes sure that any malware does not travel onto your regular OS

☐ Once downloaded, extract the "Trojan.Bonzify" FILE ONLY and run it. (Password: infected)

8. **Analyze**: How is this malware a trojan? Explain and provide evidence of your claims. (Note: Use the resources below, AND you may need to observe the behavior as you continue this lab. Be sure to screenshot whenever possible) (6 Point)
   BonziBuddy Resources
   Answer: This malware is a trojan because after turning on windows defender again it says that there is a trojan on the system. Also because bonzi buddy is disguised to be a virtual assistant but it is actually stealing information and such.
   Evidence:

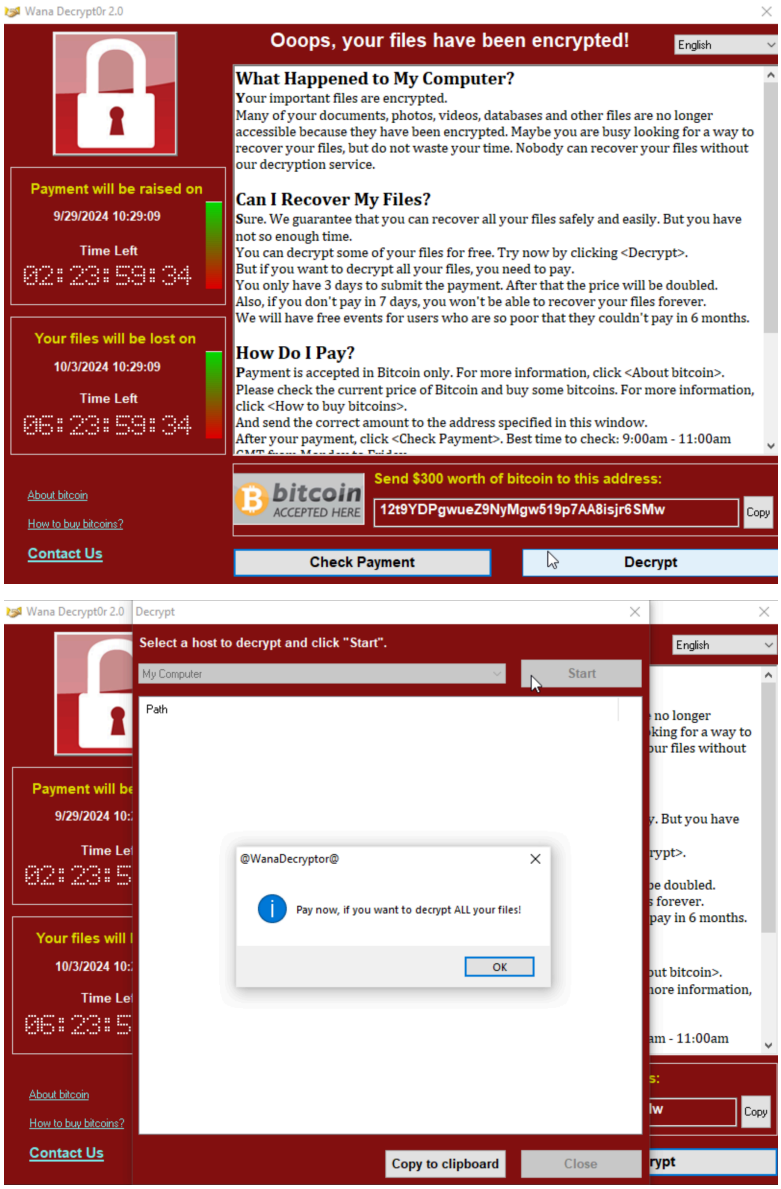


☐ Now, Extract the "Ransomware.Wannacry" files and run it.

9. **Analyze**: How is this malware a ransomware? Explain and provide evidence of your claims. (6 Points)

   Answer: This is ransomware because your files get hijacked and then you're forced to pay if you want your information back.

   Evidence:

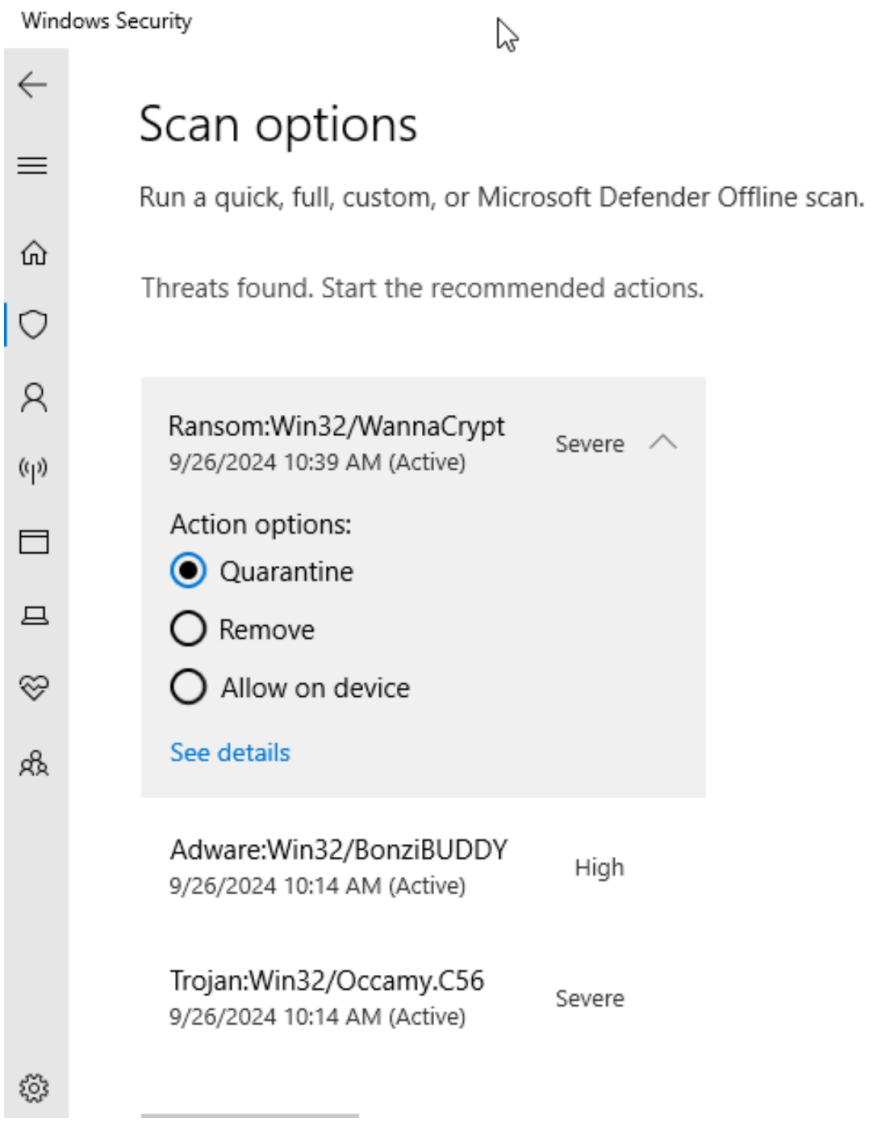


Part 3: Remediating Malware (10 Points)

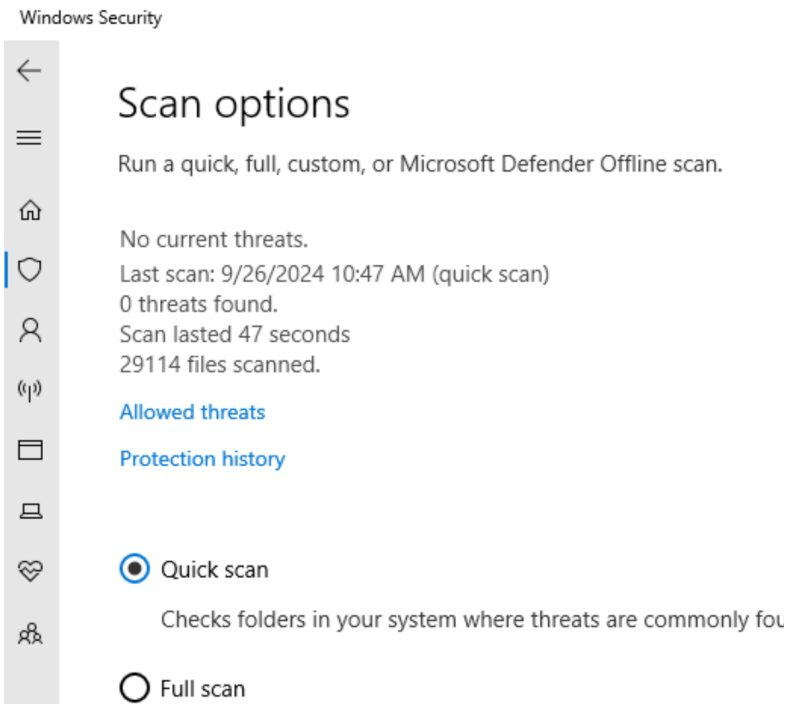
10. You are a SOC analyst tasked to resolve this infected PC for your client. Below, list the steps you take to effectively remove the malwares. Provide screenshots demonstrating the client PC is fully recovered & uninfected once completed. (6 Points)

    Steps:

    1. Go to the Virus detection setting on the windows
    2. Enable virus protection



Proof of Malware Removal:



11. **Critical Thinking**: Why is it essential to update your devices to the latest version in terms of malware protection and security? (4 Points)

    Answer: It is essential because a device that doesn't have the latest security/general updates is more prone to getting hacked since the system has been out for longer meaning bad actors have much more time learning how to crack the system. Regularly updating your software makes it harder for bad actors to try and break in because there are new security reinforcements placed for your protection.