

Goals

- Collaborate with a cybersecurity team.
- Create and implement a plan of action.
- Reflect on your cyber team experience.

Problem 1.3.1 A Dangerous Situation Rubric

Criteria	Basic	Proficient	Advanced
Risk Detection LO 5.1 Find patterns and test hypotheses about digitally processed information to gain insight and knowledge. LO9.1 Identify the components (software, hardware, protocols) that allow computers to network and communicate.	The student identified some of the security issues related to: <ul style="list-style-type: none"> • processes • downloaded files • other suspicious files • firewall rules 	The student identified most of the security issues related to: <ul style="list-style-type: none"> • processes • downloaded files • other suspicious files • firewall rules 	The student identified all of the security issues related to: <ul style="list-style-type: none"> • processes • downloaded files • other suspicious files • firewall rules
Risk Response LO 10.3: Design the correct level of protection by implementing the appropriate safeguards.	The student addressed no more than a few of: <ul style="list-style-type: none"> • suspicious processes and related application files • suspicious downloads • other suspicious files 	The student addressed most of: <ul style="list-style-type: none"> • suspicious processes and related application files • suspicious downloads • other suspicious files 	The student addressed all of: <ul style="list-style-type: none"> • suspicious processes and related application files • suspicious downloads • other suspicious files
Risk Protection LO 8.1 Describe the modular components of a computer's hardware and software. LO 8.2 Identify user actions that strengthen the security of information stored on a computer.	The student identified no more than a few of the security configuration settings for: <ul style="list-style-type: none"> • firewall rules • out-of-date software • computer settings 	The student identified most of the security configuration settings for: <ul style="list-style-type: none"> • firewall rules • out-of-date software • computer settings 	The student secured all of the security configuration settings for: <ul style="list-style-type: none"> • firewall rules • out-of-date software • computer settings
Risk Recovery LO 8.2 Identify user actions that strengthen the security of information stored on a computer.	NA	NA	The student recovered deleted data.

Documentation LO 15.2: Recognize documentation as an indispensable part of the security process.	The student created minimal to no documentation explaining why the content poses risks and how it has been rectified.	The student created adequate documentation explaining why the content poses risks and how it has been rectified.	The student created thorough documentation explaining why the content poses risks and how it has been rectified.
Collaboration LO 14.2: Collaborate effectively as part of a team. LO 14.3 Apply project management strategies effectively as part of a team.	The student is inconsistently engaged and inadequately contributes to the team's work.	The student is consistently engaged and adequately contributes to the team's work.	The student is consistently engaged and substantially contributes to the team's work.
	The student rarely provides constructive feedback to others and does not encourage or incorporate input from others.	The student occasionally provides constructive feedback to others and consistently encourages and incorporates input from others.	The student consistently provides constructive feedback to others and consistently encourages and incorporates input from others.
Presentation (Optional) LO 2.2 Engage stakeholder in a problem and use their perspectives to shape the course of your development. LO 15.1: Communicate ideas, processes, and products to optimize audience perception and understanding	The student rarely participates in the presentation.	The student occasionally participates in the presentation.	The student substantially participates in the presentation.
	The presenter is unclear, presents some of the necessary information, and does not stay on topic.	The presenter is clear, presents most or all of the necessary information, but does not stay on topic.	The presenter is clear, presents all of the necessary information, and stays on topic.
	The presenter rarely uses appropriate body language, voice modulation, and eye contact.	The presenter occasionally uses appropriate body language, voice modulation, and eye contact.	The presenter consistently uses appropriate body language, voice modulation, and eye contact.

#7 Notebook- Plan

Detect:

When and by which user did a suspicious file get to your desktop?

Could there be other potentially malicious data on your computer? How can you find it?

What applications and/or services could have been used to get these files there?

Are there any files missing from the computer?

A suspicious file could get onto the desktop by someone getting on your computer if you left it open in a public place, or if you downloaded something that contained malicious files or software. The data could have gotten there through a download, or copied from a USB drive. Double check the recycling bin to make sure nothing important has been deleted.

Respond:

What actions should you take to resolve the security threats?

You should scan the computer to see if there are any malicious files, and if so, completely delete them.

Recover:

How do you recover any missing data?

You can recover missing data by using backups saved in a secure location.

Identify

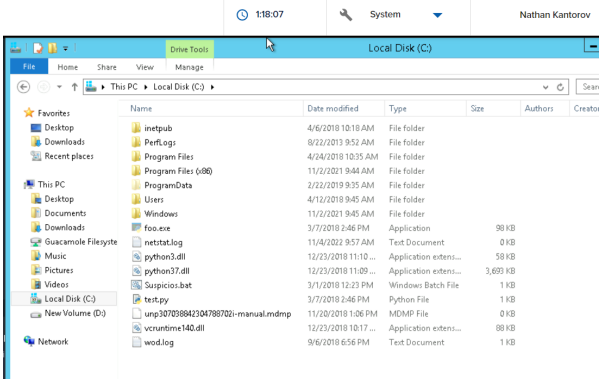
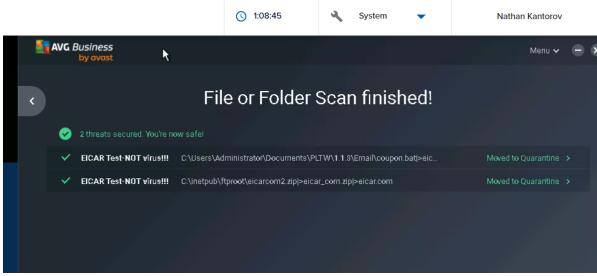
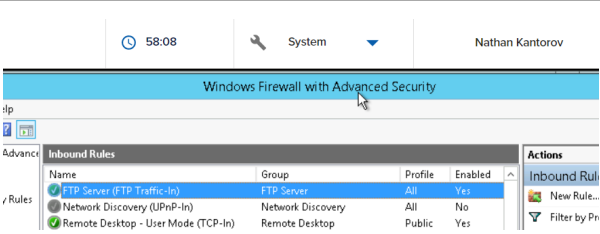
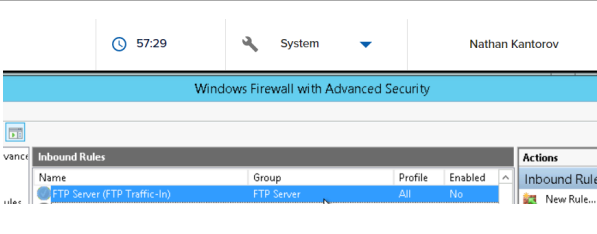
The asset is your computer and its data.

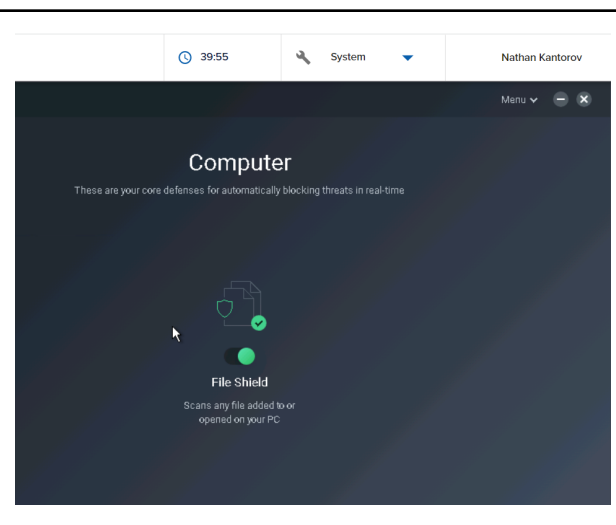
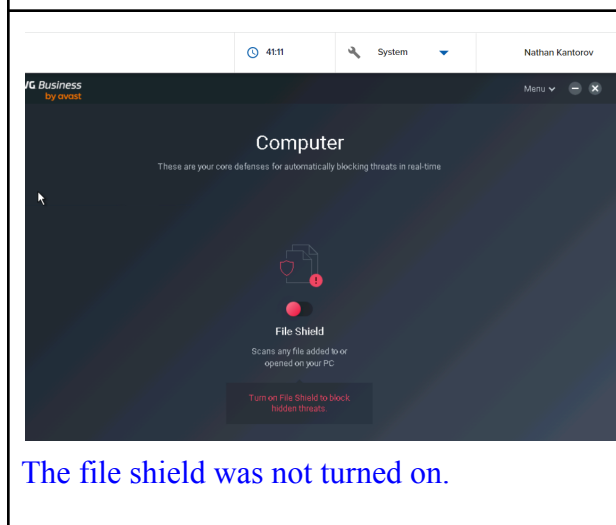
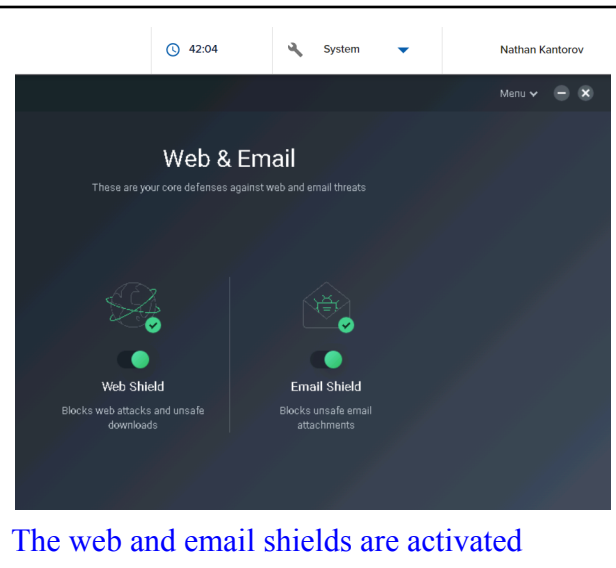
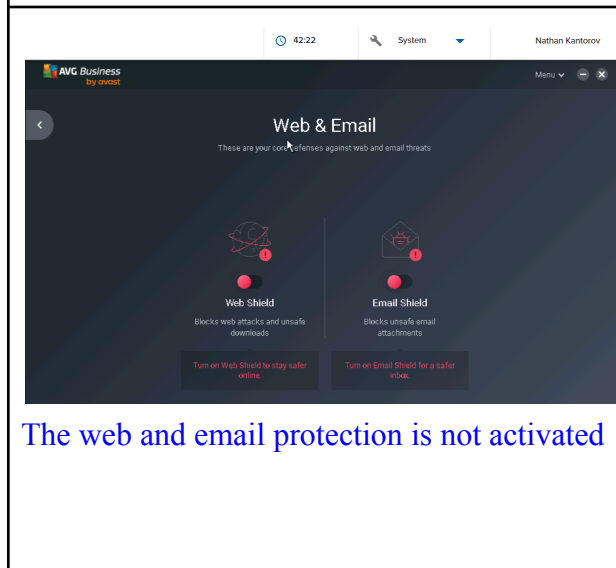
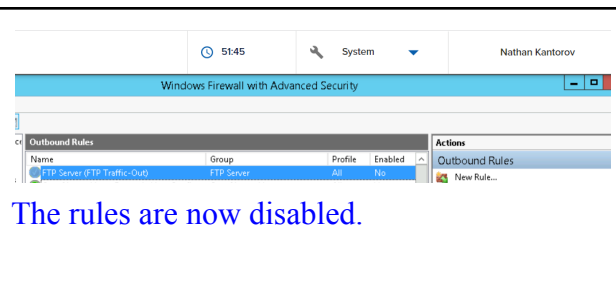
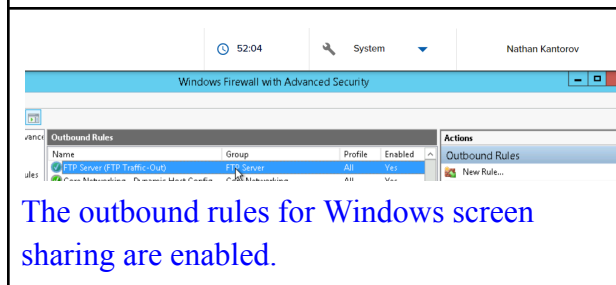
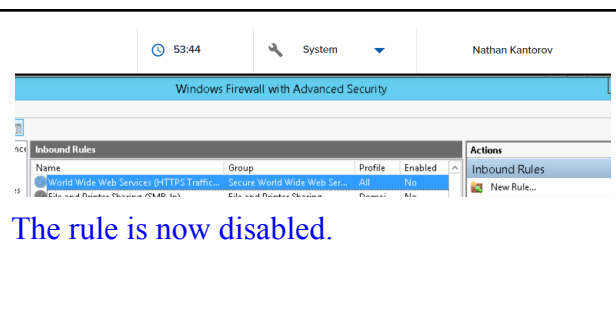
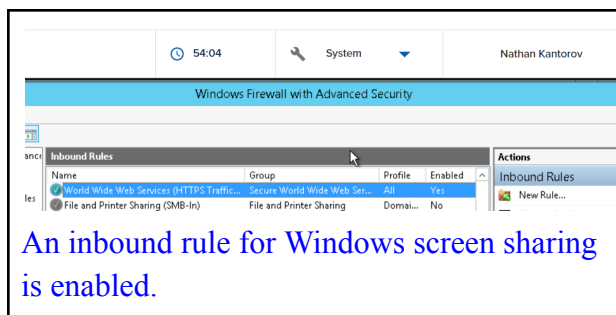
Protect:

What are the security measures you should take to secure your computer and ensure this does not happen again?

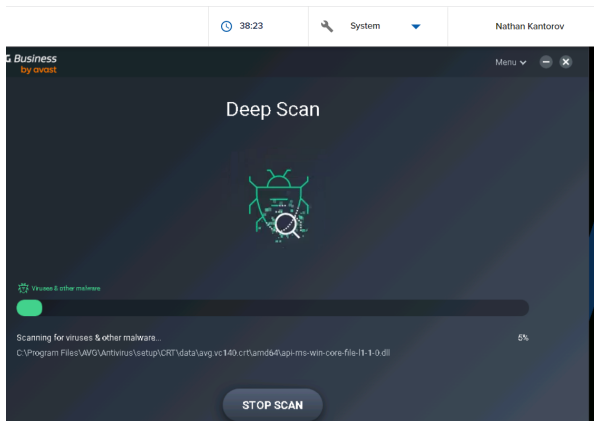
You should make sure that windows file sharing is disabled, that you change your password(s) every 90 days, and you never leave your computer signed in and unattended.

#9 Notebook

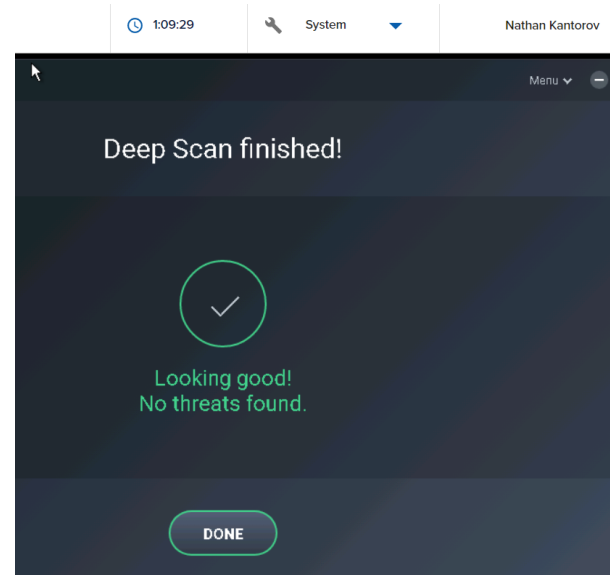
Before	Before
 <p>There were suspicious files on the Computer</p>	 <p>The suspicious files were moved to the quarantine.</p>
 <p>An inbound rule for Windows screen sharing is enabled.</p>	 <p>The rule is now disabled.</p>



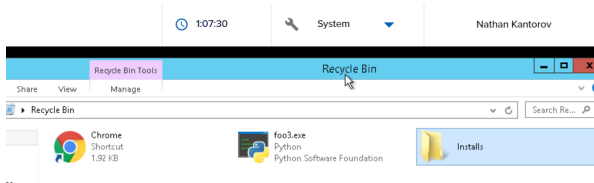
The file shield is now turned on.



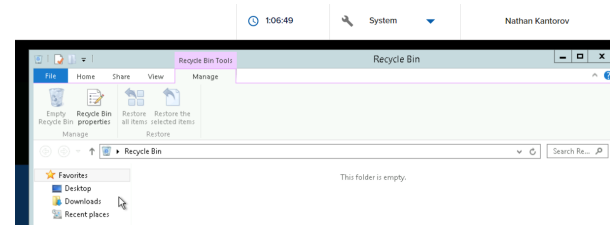
The computer has not received a deep scan.



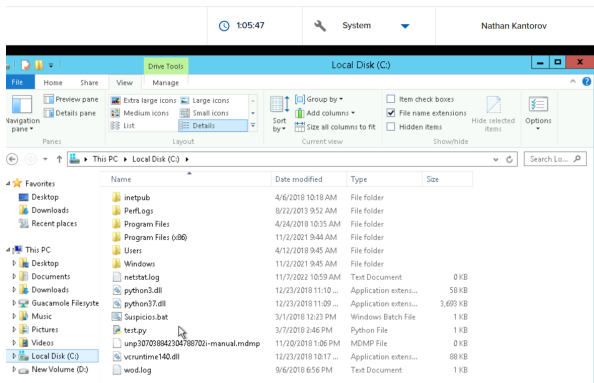
No threats, such as viruses or other types of malware, were found.



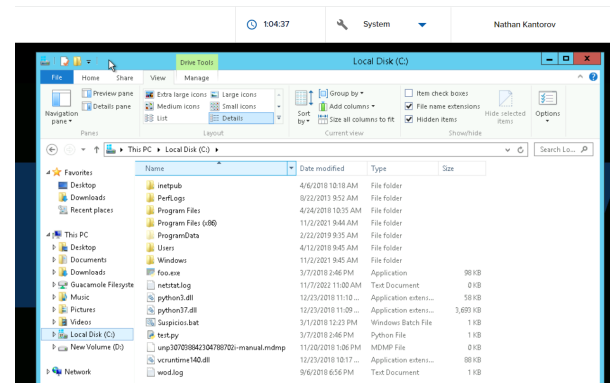
The recycling bin was not fully emptied.



The recycling bin is not completely emptied, so everything is fully deleted.



There might be some hidden malicious files that you cannot see.



You can now see and scan the hidden files for malicious content.

There are a lot of suspicious tasks going on in the background.

The suspicious tasks were ended

#13 Notebook: Reflect on your collaborative experience with your cyber team.

Describe what each team member contributed.

Each team member contributed ideas as to what the possible problems could be, and ways to solve them.

Describe one moment during teamwork when your team:

Worked well together

We all worked well together when we were communicating what steps to take to fix something when someone in our group got stuck.

Could improve on collaboration

We could probably improve a bit on organization, as we would sometimes accidentally overlap while trying to help each other.

Security Incident Response Report (for coffee shop from 1.1.1 d)

1. Contact Information for this Incident	
Name(s):	Bella Murillo and Nathan Kantorov
Date of Report:	11/4/2022
2. Detection	

Provide a brief description of what was detected and the security threat, vulnerability, or breach identified: There is a suspicious file on the computer that was not there beforehand, and something that you did not install.

3. Response

Provide a brief description of the actions you took to contain and eradicate the security threat, vulnerability, or breach:

First you scan the computer to make sure that there is no other malware and such on the computer. Then you check the location of the suspicious file and make sure there are no hidden items, and that the file extension names match. Then open the file as a text file (either with the open with, or by changing the file extension to .txt) and review its contents, to understand what it does and how best to remove it. Then delete the file, making sure to go to the recycling bin and completely emptying it. Finally, do one more scan of the computer, and review all the settings just to be safe.

4. Recovery

Provide a brief description of the actions you took to recover any affected data:

To recover any affected data, you use backup versions that were saved in a secure location. When saving it back onto the computer making sure to delete/save over the original file on the computer.

5. Identify

Provide a brief description of any assets you identified that need to be protected:

Assets that would need to be protected would be any personal information relating to health or family, bank information, credit card information, social security number, and so on.

6. Protect

Provide a brief description of the actions you took to protect your assets from future threats:

To protect the assets from future threats, I updated the Windows File sharing settings so that it is disabled, and updated everything to its most current version.

7. Lessons Learned

Please describe two lessons your team learned while solving this problem.

1. Be extremely thorough when checking the firewall rules to make sure everything is correctly set.
2. When going through the task manager details tab, make sure to pay extra attention to the owner of that task, as it makes it easier to spot suspicious ongoing tasks.

8. Other Information

Please provide any additional information you feel is important.

1. It is extremely important backup your files in a secure location, change your password every 90 or so days, and to never leave your computer logged in and unattended.

Conclusion Questions

- What are the reasons that someone might want to access your computer or device without your consent? Even if it's a friend playing a joke on you, does that make it acceptable?

There are two possible reasons why someone would want to access your computer without your consent. The first would be to steal your information or to use it for mining bitcoin. The other reason would be your friends trying to play a joke on you. Even though it is a joke, it is unacceptable because they could accidentally mess up one of your settings, opening up your computer to attacks, or actually download some malicious software without realizing it.

- How does what you have learned in this unit apply on a larger scale to businesses and large organizations?

This applies on a larger scale to businesses and large organizations because it provides them with good cybersecurity habits, and if necessary, the means to recover and fix data and issue due to a cyberattack or malicious software.