Group Project - Part 1: Assets, Vulnerabilities, and Threats …

Goal: As a group, combine your process maps and create one system that you are going to analyze for this project. Identify assets, classify them, and then run a network scan on a 'vulnerable' hypothetical network in your system and document findings.

Group: You do not have to work in a group, you can work on this individually. Max of 4 in a group, please show who is responsible for what work.

Tools:
I would recommend downloading and getting familiar with the following:

1. **OWASP Threat Dragon** https://owasp.org/www-project-threat-dragon/
2. **Microsoft Threat Modeling Tool** https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool
3. **Threat Composer** https://awslabs.github.io/threat-composer/workspaces/default/dashboard
4. Network vulnerability scanner
    a. YOU ARE ONLY DOING THIS IN A TEST ENVIRONMENT
    b. {scanner} **OpenVAS**: https://greenbone.github.io/docs/latest/22.4/kali/index.html
    c. {vulnerable system} **Metasploitable**: https://docs.rapid7.com/metasploit/setting-up-a-vulnerable-target/

Tasks:

1. Combine and build out your system and/or process map for HealthNetwork. This is based on your own research as well as the background that I have given you in the previous homework assignment.
    a. I will be posting the tabletop exercise we are working on; you can use that information as well.
2. Build an asset inventory for the organization
    a. Map the assets using Threat Dragon
3. Classify those assets using any of the tools we discussed in class
    a. Document this using both the Microsoft threat modeling tool and Threat Composer
    b. Compare and document the advantages and limitations of each
4. Run a vulnerability scan with OpenVAS or nmap, whichever tool you choose.
    a. Run the scan on Metasploitable or an existing VM. [YOU ARE RUNNING THIS IN A TEST ENVIRONMENT ONLY]
    b. Unauthorized vulnerability scanning is ILLEGAL and UNETHICAL!
    c. If the network is not yours, DON'T TOUCH.

5. Put together your documentation:
    a. Start laying out the frameworks and components that you are going to include in your risk assessment.
        i. Make sure to include GDPR, HIPAA, and references to NIST, ISO, etc.
    b. System/process map(s)
    c. Asset inventory with initial classifications
    d. Vulnerability scan output of a network (hypothetical vulnerable network in your system)