Lab 7 – GVM: OpenVAS

*Some of these responses do not require screenshots. Only include a screenshot if requested. Otherwise provide the desired response.*

**Hint**: It can be helpful to allocate more RAM and CPU if you are able to do so. Power down the OS, go into configuration and then hardware.

**1. OpenVAS Scan**

*Make sure you are watching the lectures, as they provide information you may need to complete this task. The following may contain some hints, but they are not instructions on how to install it. Refer to the lecture. You are responsible for providing screenshots where indicated by the appropriate icon.* ***Your name*** *must be seen somewhere in the background for each. A small terminal screen open is fine. Please be sure to* ***crop screenshots appropriately*** *and produce readable screenshots that can be read without zooming in; other screenshots that do not meet this requirement* ***will not receive points****.*

* Install OpenVAS scan in Kali Linux 2020. OpenVAS is part of GVM, and they have underwent some changes. You will need to install GVM and follow the sequence of commands shown in the lecture. The method of installing has changed from the past.
* Show screenshot showing OpenVAS/GVM is installed in terminal in Kali.
* Start GVM from terminal.
* Go to web interface
* Do a scan on Metasploitable 2.
  + Make sure it is on the same subnet as your Kali.
* Show a screenshot of vulnerabilities found. Make sure date is visible (more than one screenshot is fine).
* Show one vulnerability with CVSS of 8, 9, & 10. Speculate whether this would be good to use. Why or why not?!

**Deliverables**

These MUST be contained all in one PDF or DOC/DOCX.

You may select **two questions** to skip if you so desire.