Title: Using GVM/OpenVAS Tool for Vulnerability Assessment

Learning Objectives: This exercise is based on Vulnerability management which is all about identifying, evaluating, treating, and reporting security vulnerabilities in systems and software and it is important for organizations to prioritize potential threats and reduce the **'attack surface'**. In this exercise, you will learn about the GVM earlier known as OpenVAS scanner which is a vulnerability assessment tool and c**an detect security issues in all manner of servers and network devices.**

Description: GVM is a full-featured vulnerability scanner. It is capable of performing unauthenticated /authenticated vulnerability testing. The scanner is developed and maintained by Green Bone Networks since 2009. The works are contributed as Open Source to the community under the GNU General Public License (GNU GPL). In this exercise, you will learn about OpenVAS, which is a suite of tools that work together to run tests against target computers using a database of known exploits and weaknesses. The report that OpenVAS creates, tells you of potential vulnerabilities in the system you scanned.

Instructions to follow before executing the Exercise:

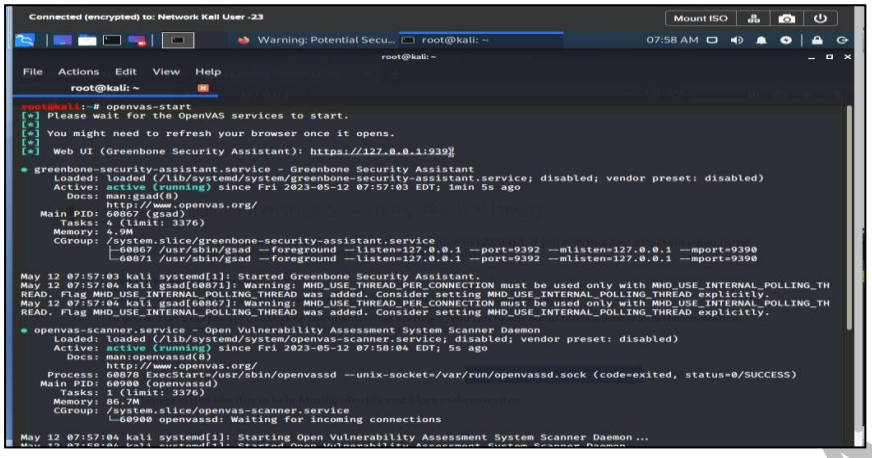
1. Start by creating your lab by clicking on CREATE LAB button on this exercise home page.
2. Watch the exercise video.
3. Read the Exercise document containing a step-by-step procedure to execute it.
4. Execute the Exercise, as per the steps given in the document.
5. after executing the exercise take the screenshot prepare a pdf file and submit the file using submit file link on the home page, click on the MARK COMPETE button on this Exercise Home Page. This will update the completion status of your course. REMEMBER: After clicking on the MARK COMPLETE button, all the VMS in this exercise lab will be deleted and you will lose, all your work related to the exercise.

About the Exercise lab infrastructure:

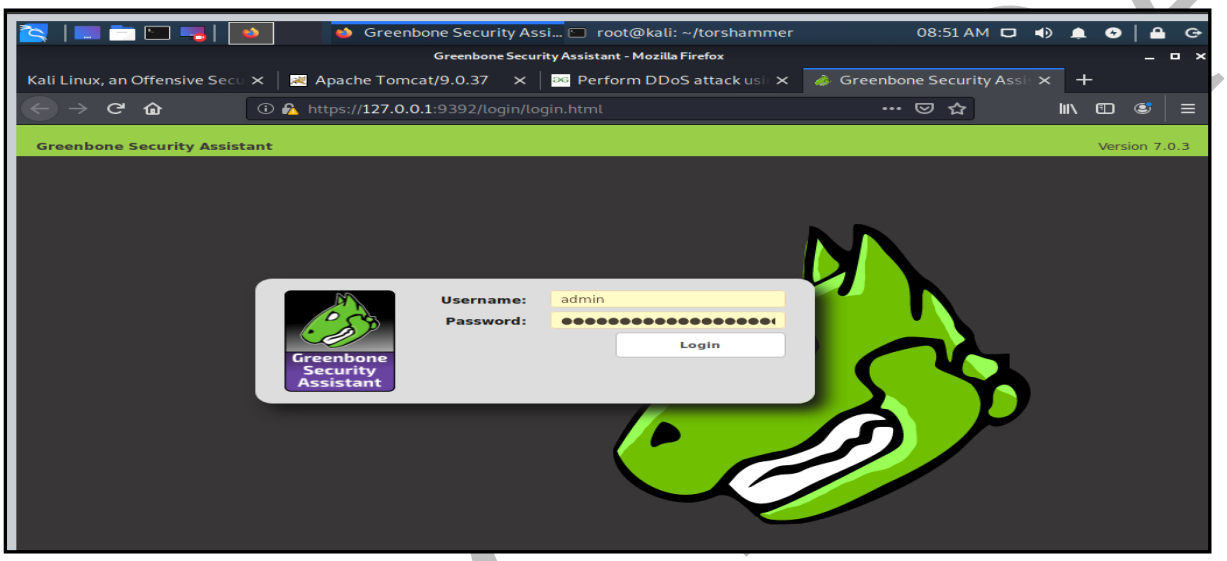
For this exercise, we require two virtual machines one is Kali as a scanner machine having username "root" and password "toor" and the other is a Windows 10 machine (target) having password "qwerty".

For Vulnerability Scanning using OpenVAS:

Open a terminal in Kali Linux and type: **gvm-start**



The OpenVAS tool will be started in a browser.



For more details, please go through the step-by-step guide provided in the "Lab Manual-Using OpenVAS tool for Vulnerability Assessment" manual.