CSC436 Lab 05

Take only the screenshots of your work as indicated below and save them to a single Word or PDF document.

**Note: You may need internet access for some components of this lab. Switch the network adapter for your Kali VM in the IA Lab to the Internet network, and get a new lease from DHCP like we did in class. Before you run any scans, make sure you switch the adapter back to the CSC436 network.

MBSA

- Install the Microsoft Baseline Security Analyzer on a Windows host. This can be something in the IA Lab, a local VM, or your local physical machine. Anything works.
- Perform a scan against the host where MBSA is installed.
- Take a screenshot of the scan results.

Nessus

- Install Nessus on your Kali VM in the IA Lab. Register for a Home feed.
- Configure a custom scan policy based off the Basic Network Scan policy that Nessus comes with. The scan policy title should contain your name (cmwelu_Basic_Scan).
- Scan the systems you found on the 10.10.30.0/24 network in the previous lab.
- Launch the scan, and take a screenshot of the hosts summary in the web interface. The screenshot should show the title of the scan including your name, the types of vulnerabilities found, and the hosts scanned.

OpenVAS

- Create a new scan target, and make sure the title contains your name (cmwelu Target)
    - Include the systems you found on the 10.10.30.0/24 network in the previous lab in the list of hosts.
    - Take a screenshot of this configuration.
- Create a new scan task, and make sure the title contains your name (cmwelu Scan)
    - Set the target to the target you created in the previous step.
    - Change the Scan config to Full and fast ultimate
    - Set the order for targets to Random
    - Take a screenshot of this config.
- Execute the scan, and let it complete.

- Take a screenshot of the status page with the running scan, including your scan name in the screenshot.
- After the scan is finished, open the PDF version of the report. Take a screenshot of the Result Overview section.