Lab 6 – Nessus

**Part I. Nessus Scan**

*Make sure you are watching the lectures, as they provide information you may need to complete this task. Please Provide the screenshots indicated.* ***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 Nessus scan in Linux.
* Show screenshot showing Nessus is installed in Kali. **
* Obtain community key to register Nessus as home user.
* Show screenshot showing it has been activated. **
* Start Nessus from terminal:
  + /etc/init.d/nessusd start
* Navigate to Nessus <https://kali:8834/> --note the s!
* Create credentials and login.
* Allow all the plugins to download. This may take a significant period of time.
* Do a scan on Metasploitable 2.◦ Make sure they are on the same subnet.
* Show screenshots of the following:
  + Creating policy **
    - Metasploitable 2 is a Linux machine. You decide on an appropriate policy.
* The Report, showing the number of vulnerabilities found. **

**Part II. Understanding Vulnerabilities**

Answer the following questions:

1. Select one of the critical severity vulnerabilities reported by Nessus and enter all of the items in the list above. For item 4, other vulnerability identifiers, only list CVE identifiers if available; otherwise, list only the first other identifier reported.
2. Select one that is not critical severity that you think could be promising. Enter all of the items in the list above. For item 4, other vulnerability identifiers, only list CVE identifiers if available; otherwise, list only the first other identifier reported.

Click on the first vulnerability of critical severity to see the details Nessus reported about the vulnerability. Each vulnerability has multiple attributes, the most important of which are the following:

1. Nessus plugin ID number: Identifies the plugin that reported the vulnerability.
2. Nessus plugin name: The name of the plugin that reported the vulnerability.
3. CVE (Common Vulnerabilities and Exposures) vulnerability identifier: Some vulnerabilities will not have this identifier, but vulnerabilities that do are recorded in the National Vulnerability Database (nvd.nist.gov) and can be looked up there or at www.cvedetails.com. A single Nessus vulnerability may correspond to multiple CVE identifiers. These identifiers are of the form CVE-YEAR-####.
4. Other vulnerability identifiers: Many vendors, such as Microsoft (MS-## format) and the Mozilla Foundation (MFSA-YEAR-####) record vulnerabilities in their own databases, which may provide more information than Nessus shows or that can be found in CVE databases. Other identifiers include OSVDB numbers for the Open Source Vulnerability Database and BID numbers for the Bugtraq database at securityfocus.com.
5. CVSS base score: The Common Vulnerability Scoring System (CVSS) provides a numerical indication of vulnerability severity raning from 0 to 10. Critical vulnerabilities will have CVSS scores near 10. The current CVSS version is 2.0. More details can be found at https://nvd.nist.gov/cvss.cfm.
6. Exploit available: Indicates whether or not an open source (like Metasploit) or commercial (like Canvas or Core Impact) exploit framework has an exploit for this vulnerability. Even if no exploit exists for a vulnerability in a popular framework, individual exploit scripts may be found on sites like Exploit DB (www.exploit-db.com).
7. Exploitable with: Names which frameworks have exploits for this vulnerability.

**Deliverables**

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

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