Lab 01: Vulnerabilities

Goals

- Review a vulnerability scan and assess results
- Determine CVSS for a described system and defend your answer

Vulnerability Scan Report

Use the Nessus report linked here to answer the following questions:

1. How many critical level vulnerabilities were found on the computer at 192.168.1.55?
2. Expand the details for 192.168.1.113. One of the Critical vulnerabilities is MS17-010. What is the first CVE this bulletin covers?
3. MS17-010 also covers CVE-2017-0144. What is the CVSS Base Score for that CVE based on the CVSS v3.0 Severity and Metrics? Also provide a severity level.
4. List the following metrics for CVE-2017-0144
    a. Attack Vector:
    b. Attack Complexity:
    c. Scope:
    d. Availability
5. The second to last listed critical vulnerability for the system at 192.168.1.79 refers to the cumulative update from September 2017 for Windows 8.1 and Server 2012 R2. Included in this update is a patch for CVE-2017-0161. Which application is affected by this vulnerability?
6. What type of vulnerability is CVE-2017-0100? Please provide a specific CWE number as well.
7. What is the technical impact of CVE-2017-0297? This is visible as part of the associated CWE.
8. Which vulnerability reported by Nessus would you prioritize on the system at 192.168.1.114? Why?

CVSS

Fill in the score metrics for the following vulnerability and describe why you chose the values you did in the space below.

A web order form is incorrectly configured such that an unauthenticated user can discover items in authenticated users' carts by changing a URL parameter for user ID. This configuration issue results in the web application returning a HTTP 500 when a user doesn't exist and the contents of their cart when the user exists.

Attack Vector	
Attack Complexity	
Privileges Required	
User Interaction	
Scope	
Confidentiality Impact	
Integrity Impact	
Availability Impact	
Total Base Score(v3)	

Explain: