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?

   4 crits
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?

   It's linked to several CVE's :

   CVE-2017-0143

   CVE-2017-0144

   CVE-2017-0145

   CVE-2017-0146

   CVE-2017-0147

   CVE-2017-0148
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.

   Base Score: 8.1

   Severity: High
4. List the following metrics for CVE-2017-0144
   a. Attack Vector: Network
   b. Attack Complexity: high
   c. Scope: Unchanged
   d. Availability: High
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?

   Windows NetBT / Netbios over TCP
6. What type of vulnerability is CVE-2017-0100? Please provide a specific CWE number as well.

   Improper Authentication (CWE-287) allows privilege escalation
7. What is the technical impact of CVE-2017-0297? This is visible as part of the associated CWE.

   Comrpomise of Confidentiality / Information Disclosure
8. Which vulnerability reported by Nessus would you prioritize on the system at 192.168.1.114? Why?

   MS17-010 – It's Wannacry and squad – stands out among all the remote execution and elevation vulns.

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	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality Impact	High
Integrity Impact	High
Availability Impact	None
Total Base Score(v3)	9.1

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N&version=3.1

Explain:

Attack Vector	This is a web based shopping application, so I'm assuming it's accessible from the internet
Attack Complexity	No technical expertise or even tools required to exploit this vulnerability
Privileges Required	pretty self-explanatory. Since the error issue is a bypass of the URL-based authentication system
User Interaction	None
Scope	On this one I'm not 100% confident what to choose. The exploit doesn't afford me any higher privileges on the system, but it does change what I can view and access. So the scope isn't really changing, but the frame is...
Confidentiality Impact	High I can see the cart which may or may not contain sensitive information... depends on the store, the contents, and the customer
Integrity Impact	High This is based on the assumption that any functionality from the cart-page will allow me to modify the contents (say remove items, or increase / decrease quantities of items)
Availability Impact	None