Lab 5 - Vulnerability Analysis

Objectives

Perform a vulernability scan against your lab network.

Review a vulnerability scan report to analyze vulnerabilities.

1. Vulnerability Scanning with Nessus

* Completing the Installation of Tenable Nessus
* Ensure the Nessus service is running in the Kali VM by running: service nessusd restart
* After successful installation, pull up a web browser inside Kali and navigate to https://localhost:8834. (Ignore any SSL Certificate errors)
* Follow the "wizard" to configure the Nessus engine. It should default to Nessus Essentials. Simply click continue.
* You will need an activation code so you'll be prompted to register through the wizard, or optionally you can manually do it by opening a separate tab in your web browser Go to the website: https://www.tenable.com/products/nessus/nessus-essentials
* Enter valid information in the form. Check your email and you will have an activation code. Enter in the validation code you were sent and select Next.
* Next, create the username (admin) with a password that you'll remember (Password1234!)
* Select Download Plugins
* This can take a while (up to an hour). Class will begin at this point.
* Using Nessus to perform a Vulnerability scan
* Below is a general list of steps however new versions of Nessus may change the order of these steps.
* Login to the web console with the username and password created.
* Go to Policies - Select New Policy - Select Basic Network Scan
* Enter a policy name of "Non-Credentialed Scan"
* Iterate through the options on the side menu to complete the configuration. When in doubt, select "Default" in the drop down menu.
* Go to Scans - Select New Scan - Give the scan a name of “non-credentialed scan”
* For Policy Select Non-Credentialed Scan
* For the Target, select your IP range for your systems (i.e. 192.168.100.1-192.168.100.255)
* Select Launch; When the scan is finished, double click on it

1. Reviewing a Nessus Vulnerability report

* What ports were found open in the scan?

Ans: A screenshot of a computer

Description automatically generated

I can see six hosts detected my Nessus including windows 7, XP and Kali VMs. It also shows Host Windows 11 System.

* How many High vulnerabilities were found?

Ans: A total of 87 Vulnerabilities were found across 6 systems, which included 11 Critical, 10 High, 17 Medium, 2 Low vulnerabilites and rest were informative findings.

* Select a vulnerability listed and view the details Nessus provides

Ans: A screenshot of a computer

Description automatically generated

It is a critical vulnerabilitywith CVSS score of 10. It shows that the support for Windows XP has been ended in 2014.

* What CVE is associated with the finding?

Ans: There are a lot of CVEs associated with this vulnerability as it is legacy operating system.

A screenshot of a computer

Description automatically generated

The CPE associated with this vulnerability is cpe:/o:microsoft:windows\_xp.

* What solution does Nessus propose?

Ans: Upgrade to a version of Windows that is currently supported.