Jordan Schalter

IT419 SCHIPPERS

LAB3

08/01/2023

19. **Compare the scan results on the Windows XP machine to the scan results to Nessus. To complete the lab, answer the following questions, utilize screenshots from both scanners:**

* 1. **How many vulnerabilities did Nessus find on the target?**

According to my screenshot Nessus found 27 vulnerabilities.

* 1. **How many vulnerabilities did OpenVAS find on the target?**

According to my screenshot OpenVAS found 35, 10 of them being the most severe.

* 1. **If you’re looking to identify vulnerabilities, what has this exercise illustrated?**

This lab has illustrated that there are many valuable tools that can be utilized in terms of scanning for vulnerabilities.

* 1. **Provide a screenshot of Nessus Scans and OpenVAS scans.**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

30.

A computer screen shot of a black screen

Description automatically generated

33. A computer screen shot of a black screen

Description automatically generated

39. A computer screen shot of a black screen

Description automatically generated

40. After the command finishes, you may have some surprising results. Some documents will have Zone.Identifier appended as an ADS on the primary file. Perform a Google search (break out your GoogleFu) and provide a reason ADS files have been built on your machine. Be sure to cite your source for credit.

According to <https://blog.foldersecurityviewer.com/ntfs-alternate-data-streams-the-good-and-the-bad/> some of the benefits of ADS are as follows:  
  
 Windows Resource Manager leverages ADS to identify high risk files that shouldn’t be accessed.

The Windows operating system uses ADS to encrypt and store files in a secure manner.

The Windows Attachment Manager uses ADS as a file scanner. This explains why sometimes you receive warnings when you open a file downloaded from the Internet.

The SQL Database server uses ADS to maintain database integrity.

Citrix’s virtual memory uses ADS to boost DLL loading speed.

Anti-virus applications, such as Kaspersky, uses ADS to enhance the scanning of files.

All of these reasons seem valid to me, especially the database integrity and resource management effectiveness.

## Criteria for Completion

1. Please pick 3 different tools that you can use to perform scanning based on what you learned in the course books or via research online. Then use those tools to perform scans on the systems in the lab. Write about what you did, tools you picked, and the results and what you learned.
2. The first one that I used is the scanning tool Qualys, and it checks the network or the relevant network devices to see whether they comply with the compliance standards. The finest thing about Qualys is that it provides a precise scanning report and informs the user of the type of action that must be performed to address the vulnerability. It can also carry out a policy scan, which verifies details like whether the server has been hardened. Qualys is well-known because it offers a complete solution for scanning the network, online applications, and policies. This program searches the network for vulnerabilities and recommends the patch needed to fix such issues. It provides the ability to scan for vulnerabilities in web applications in addition to network vulnerabilities. The scans are really carried out by a cloud-based vulnerability scanner, which also keeps the report on the cloud solely.
3. The second command-line-based network scanning tool that I used is called Nikto. Nikto is typically included in Linux distributions like Kali Linux. When the requirement is to run server type-specific tests, it is recommended. In certain Linux distributions, it is included by default, whereas in others, it must be installed. It searches the network in a manner that is quite like those of other technologies however, it lacks the availability to run the scan in a customized manner. It is worth mentioning that since Nikto is a command-line tool, the user’s whim is familiar with the command line interface, finds it easy to work with it, and many users still prefer to work with a graphical user interface. Even though Nikto is thought to be classified as a tool that frequently causes false alarms, it is still open-source and is often used for network scanning. Like other tools, it also scans the network for vulnerabilities and notifies us of them so that they may be corrected before an attacker leverages them.
4. The last program I tried is Zenmap, which is a graphical user interface for the Nmap network security scanner. Because it is also open-source, this network scanning application is well-liked by users that prefer working with a graphical user interface. This program's most important feature, which also makes it quite useful, is that it can perform any task that Nmap can. Another way to describe it is as a GUI-based network scanning program that runs Nmap commands in the background to carry out the scan. This tool's environment has an input box that is only meant to take Nmap commands. The output area below that input box displays the results of running the Nmap application.

I tested the tools that I found on this website: https://www.educba.com/network-scanning-tools/