Lab – Investigate Vulnerability Assessment Tools

Objectives

Part 1: Exploring Kali Linux

Part 2: Investigating Nmap and Zenmap

Part 3: Using Wireshark to Open and Analyze a pcap File

Background / Scenario

Kali Linux is a Debian-based Linux distribution that contains tools for advanced penetration testing and security auditing. Kali contains several hundred tools which are used for a wide variety of information technology security tasks. In this lab, you will explore some of the tools available in Kali Linux.

Note: Only use Kali tools on networks on which you are authorized to do so.

Required Resources

- PC with at least 1 GB of RAM and 15 GB of free disk space with IoTSec Kali VM

Part 1: Exploring Kali Linux

Step 1: Start the Kali VM.

a. On your PC, open Oracle VirtualBox. Select the IoTSec Kali VM that was installed in a previous lab.

b. Click the green Start arrow in the menu bar. After a brief delay, you should see a new window open that displays a username field.

c. Enter the username **root** and click the Next button. Use **toor** for the password and click **Sign in**. If you have typed the username incorrectly, click **Cancel** to input the correct username.

Step 2: Explore Kali Linux.

Kali Linux contains a number of tools for various information security tasks. To make it easier to use the tools, they have been organized into different categories.

a. Explore the Kali menus. How many categories of tools are there in Kali Linux?

_____

b. Find each of the tools in the table below in the Kali Applications menu. Investigate each and fill in the table below. You may need to run the tools to determine the type of interface that is used.

Note: Using any of these tools on actual networks could violate the ethical hacking policy for this course and may break the law.

Tool	Category	Interface (GUI or Command line)
Nmap		
Zenmap		
SQLmap		
Skipfish		
Wireshark		

Part 2: Investigating Nmap and Zenmap

Use the "Kali Linux Tools Listing" web page accessible at the link https://tools.kali.org/tools-listing to research the answers to the following questions:

Step 1: Learning about Nmap

a. Find the Kali Tools page for Nmap. In what two categories is Nmap listed?

_____

_____

b. What is Nmap primarily used for?

_____

_____

c. Nmap has many options. How does a penetration tester tell Nmap which options to use? (You can see some of the options the in the Nmap Usage Example entry on the Nmap Kali Tools page.)

_____

_____

We will use Nmap later in the course.

Step 2: Learning about Zenmap

Zenmap is a network scanning tool that allows you to discover network hosts and resources, including services, ports, operating systems, and other information. Zenmap should not be used to scan networks without prior permission. The act of network scanning can be considered a form of network attack.

a. What is the relationship between Zenmap and Nmap?

_____

_____

b. How many default scan profiles are available in Zenmap?

_____

_____

c. When we change the profile, we see also see changes in the Command field. What does the Command field contain?

_____

_____

Part 3: Using Wireshark to Open and Analyze a pcap File

Wireshark is a software protocol analyzer, or "packet sniffer" application. Wireshark captures traffic on a network segment and provides features that simplify analysis of the traffic. Wireshark can be used for learning about networking, monitoring and troubleshooting networks, and network software development. Wireshark captures each frame transmitted on the network and provides access to details about the upper levels of the protocol stack at the internet, transport, and application layers of the TCP/IP model.

a. Open **Wireshark** in the IoTSec Kali VM by either finding it in the application menu or typing **wireshark** at a terminal prompt.

b. Ignore any errors that might appear and go to the Wireshark file menu. Open the file **/root/lab_support_files/PCAP_files/PlainText.pcap**.

The pcap file contains a protocol capture of a Telnet session between the client 192.168.0.2 and a Telnet server. The client is attempting to open a terminal on the server in order to execute commands on it. Use Wireshark to answer the following questions.

c. What is the IP address of the Telnet server?

_____

d. What protocols are used in the captured data conversation?

_____

_____

e. Go to the **Analyze** menu and select **Follow** > **TCP Stream**. A window appears that shows the data exchanged between the client and server. The color coding identifies which host is the source of the data. If you click any part of the conversation, the corresponding frame will be selected in the capture window.

What is the username and password used for authentication of the session?

_____

_____

What operating system is running on the server?

_____

Which commands were sent from the client to be executed on the server??

_____

_____

How did the server respond?

_____

_____

This packet capture illustrates an important security vulnerability that exists in the Telnet protocol. What is this vulnerability?

_____

_____