Wireshark Watching

Introduction and/or Background

What do the words “dragon”, “maggie”, and “cowboy” have in common? They all appear on the 500 worst passwords list.

Objectives

In this project/lab the student will:

- Gain familiarity with Wireshark

Equipment/Supplies Needed

- As specified in Lab 0.0.1.
- Linux Installation File: Metasploitable

Procedure

Perform the steps in this lab in the order they are presented to you. Answer all questions and record the requested information. Use the Linux Virtual Machine to perform lab activities as directed. Unless otherwise stated, all tasks done as a non-root user. If root access is needed use the sudo command.

Assignment

nMap Noise

1. Setup
    a. Power on Metasploitable VM and record its IPv4 address.

    b. Power on the Kali VM and open the following programs:
        i. Wireshark
            1. Applications -> 09 –> Sniffing & Spoofing -> wireshark
            2. Double-click the eth0 interface.

    c. ZenMap: Applications -> 01 – Information Gathering -> zenmap

2. Scanning
    a. Wireshark: Start a new capture (or reset the current one).

    b. nMap Command: nmap –sn <Metasploitable’s IPv4 Network Address>/24

c. Wait for the scan to complete.

d. Wireshark: Stop and save the capture to a file titled arpscan (the pcapng extension should be added automatically).

3. Searching
    a. Open the arpscan.pcapng file in Wireshark.

    b. Apply the **arp** filter and **take a screenshot**.

    c. Examine the packets listed paying close attention to the Time and Info categories.

Reflection Questions

1. How can arp packets be used to identify a network scan?
2. Why might this knowledge be valuable to a network administrator?
3. What can be done to limit the scope of this type of attack?

Hydra Hacking

1. Setup
    a. Open a Terminal window.

    b. Common Passwords List
        i. Change to the Documents directory.
        ii. Download the password list: wget https://wiki.skullsecurity.org/images/c/ca/500-worst-passwords.txt
        iii. Open the password list and **take a screenshot**.

2. Scanning
    a. Wireshark: Start a new capture.
    b. Terminal Command: hydra –l sys –P 500-worst-passwords.txt <Metasploitable's IPv4 Address> telnet
    c. Wait for the scan to complete.
    d. Wireshark: Stop and save the capture to a file titled telcap

3. Searching
    a. Apply the **telnet** filter.
    b. TCP Stream Examination
        i. Right-click a packet and select TCP Stream from the Follow menu.
        ii. Increase the window's size.
        iii. Examine the TCP stream's content.
        iv. Click the drop-down menu that says Entire conversation and examine both parts of the stream.
        v. Increase the number in the Stream up-down menu by one.
        vi. Repeat steps 3-5 to view all of the streams.

vii. Scroll to the end of the last stream and **take a screenshot**.

Reflection Questions

1. What is a TCP stream?
2. What do the different text colors in wireshark's TCP stream window mean?
3. What username and password combination successfully authenticated to Metasploitable's TCP server?
4. How might a program be better able to analyze these types of packets?

Lab Submissions Proof: Provide screenshots as indicated in the lab; upload your proof to Moodle for grading.

Rubric

Checklist/Single Point Mastery

Concerns Working Towards Proficiency	Criteria Standards for This Competency	Accomplished Evidence of Mastering Competency
	Criteria #1: Screenshot of ARP filter applied to Wireshark capture (15 points)	
	Criteria #2: Screenshot of last TCP stream (15 points)	
	Criteria #3: Answer to reflection question 1 in nMap noise section (10 points)	
	Criteria #4: Answer to reflection question 2 in nMap noise section (10 points)	
	Criteria #5: Answer to reflection question 3 in nMap noise section (10 points)	
	Criteria #6: Answer to reflection question 1 in Hydra section (10 points)	
	Criteria #7: Answer to reflection question 2 in Hydra section (10 points)	
	Criteria #8: Answer to reflection question 3 in Hydra section (10 points)	
	Criteria #9: Answer to reflection question 4 in Hydra section (10 points)	