Lab Activity 3

CSE 420: Ethical Hacking

**Marks: 2.5**

**Group Activity: (Group of 2 students)**

**Submissions**:

1. Fill the answers for given questions after performing practical and submit the Word file
2. Record a video on MS teams to explain the practical parts done to get answers for given questions (Video and screen must be available in the video). No marks for video without voice and video.
3. In recording of the video, explain the followings:
4. Overall objective of the lab.
5. For each objective, explain the overview of that objective.
6. Then perform the steps to show how did you reach to the answer. You can keep Word file open to perform the task but you have to explain what is the purpose of the command and explain the output of the command as well.

Incomplete Lab - Packet Crafting with Scapy

**Lab - Packet Crafting with Scapy**

Spring 2023-24

Date: 21th March 2024

by: Mohammed – 1082759

Question 1:

How does the author describe the capabilities of Scapy in the first paragraph of the page?

Answer :

In the first paragraph, the author describes Scapy as a Python program that allows users to send, sniff, dissect, and forge network packets. This enables the construction of tools for probing, scanning, or attacking networks

Question 2:

How many types of TFTP packet formats are listed?

Answer

TFTP\_ACK: TFTP Acknowledgment

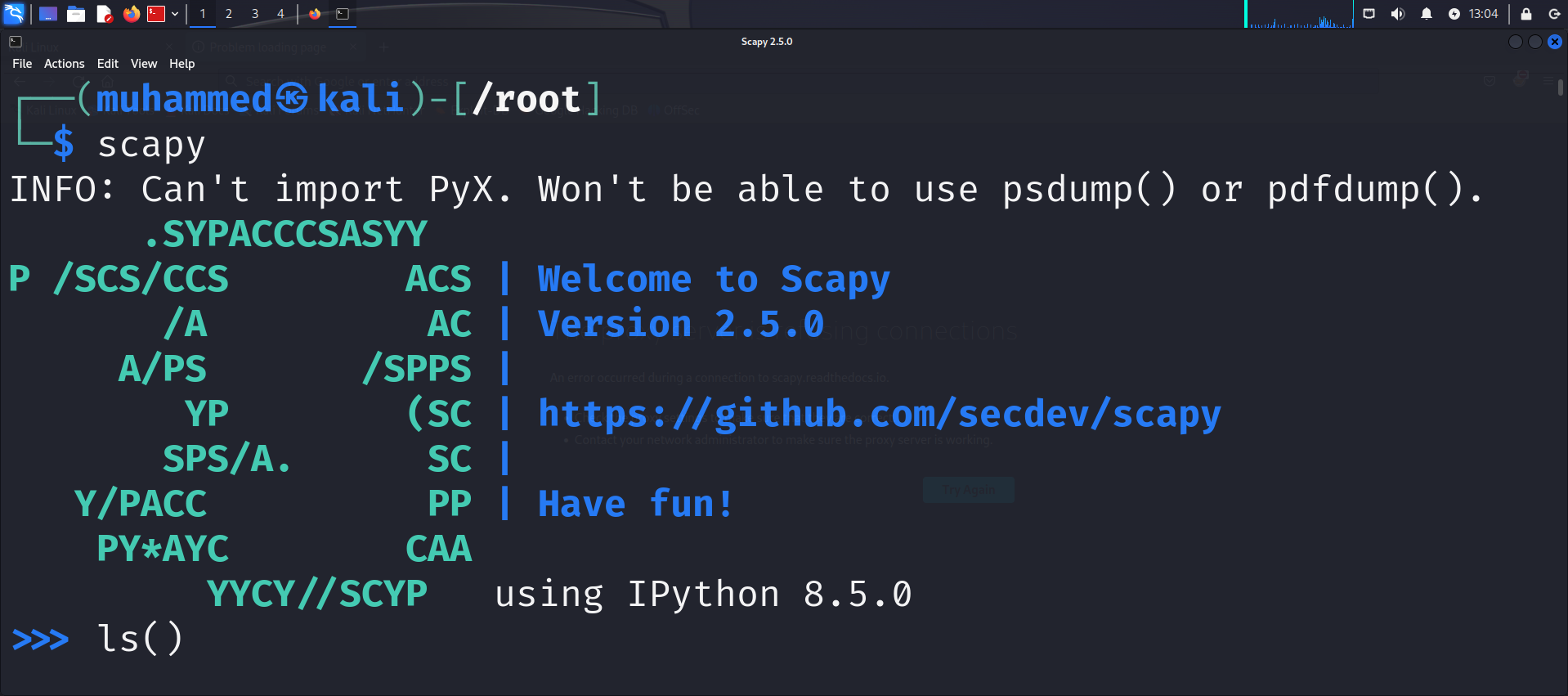
TFTP\_DATA: TFTP Data

TFTP\_ERROR: TFTP Error

TFTP\_OACK: TFTP Option Acknowledgment

TFTP\_RRQ: TFTP Read Request

TFTP\_WRQ: TFTP Write Request



Question 3:

Compare the fields in the IP detail on Scapy with the packet header described in Step 3a. Are there any differences between the two?

Answer

The fields listed in the Scapy ls(IP) output match the described IPv4 packet header fields, with the main difference being the representation of the Differentiated Services field (tos) and the presence of the options field in Scapy, which is shown as an empty list.



Question 4:

Which field do you think you would change to create a packet that would generate a

reply to a target machine, rather than the machine that actually sent the packet?

Answer

To create a packet that would generate a reply to a target machine, rather than the machine that actually sent the packet, you would typically change the Destination IPv4 Address (dst) field in the packet header. By setting the dst field to the IP address of the target machine, the reply would be sent to that target machine instead of the original sender.

Question 5

What traffic is displayed in the output of the nsummary() function?

Answer

The output of the nsummary() function displays ICMP traffic that was captured using the filter filter = "icmp" and a count of 10 packets.

Question 6:

Why are there two sets of source and destination fields?

Answer

There are two sets of source and destination fields because the packet capture includes both the request and response packets for the ICMP ping operation. The first set of source and destination fields corresponds to the request packet sent by your machine (source) to the target machine (destination). The second set of source and destination fields corresponds to the response packet sent by the target machine (source) back to your machine (destination) in response to the ICMP ping.

Question 7:

What type of packets are shown in the summary output?

Answer

The summary output shows ICMP packets, as indicated by the "ICMP" protocol designation

Question 8:

What is different between the original ICMP packet conversation and the custom ICMP packet conversation?

Answer

The original ICMP packet conversation likely consists of standard ICMP Echo-request and Echo-reply packets, which are used for basic network testing (like pinging). These packets would have typical ICMP headers and payloads.

In contrast, the custom ICMP packet conversation involves sending a modified ICMP packet with a different payload, such as "This is a test." This custom packet is not part of a standard network diagnostic exchange and is used here to demonstrate crafting and sending custom packets.

Question 9

What does the SA flag indicate in the packet returned from 10.6.6.23?

Answer

The SA (SYN-ACK) flag indicates that the TCP packet returned from 10.6.6.23 is a TCP SYN-ACK packet. This type of packet is sent in response to a TCP SYN packet when a server is listening on the specified port and is ready to establish a TCP connection.

# Reflection Questions

1. How can crafting various TCP SYN packets be used to perform passive reconnaissance on a target host.?

Answer

Crafting TCP SYN packets helps to passively gather information about a target host's open ports and services. By analyzing the responses, one can identify potential vulnerabilities without directly engaging the target.

2. How could creating an ICMP echo-request packet with a spoofed source address create a denial of service attack on against a target host?

Answer

Creating an ICMP echo-request packet with a spoofed source address can lead to a denial of service (DoS) attack by flooding the target host with ICMP echo-request packets. The target host, believing the packets are legitimate, responds to the spoofed source address, which may overwhelm the actual owner of that address with responses. This can consume network resources and potentially render the target host unreachable.