Lab 4 - Packet Sniffing and Spoofing

Submission

You need to write a report which includes:

1. A concise description of your findings for each task.
2. Answers to all questions given in the tasks.
3. The Python scripts you write to accomplish the tasks (if any).
4. **Screen captures** to support your findings.

Submission requirement

1. Use Markdown to write your report; a report template will be provided by the instructor.
2. You can use your favorite Markdown editor. However, if you never used Markdown before, there are two recommended ones:
    1. https://marxi.co/ - A browser app
    2. https://typora.io/ - A cross-platform desktop MD editor
3. In your report, all codes should be placed in code blocks/fences. For example:

```
def somefunc(param1='', param2=0):
    '''A docstring'''
    if param1 > param2: # interesting
        print 'Greater'
    return (param2 - param1 + 1) or None
```

4. Do not submit the MD file; instead, export as **pdf** for submission.

Overview

Packet sniffing and spoofing are two important concepts in network security. They are two major threats in network communication. Being able to understand these two threats is essential for understanding security measures in networking. There are many packet sniffing and spoofing tools, such as Wireshark, Tcpdump, Netwox, etc. Some of these tools are widely used by security experts, as well as by attackers. Being able to use these tools is important for students, but what is more important for students in a network security course is to understand how these tools work, i.e., how packet sniffing and spoofing are implemented in software.

Objective

The objective of this lab is to master the technologies underlying most of the sniffing and spoofing tools. Students will play with some simple sniffer and spoofing programs, read their source code, modify them, and eventually gain an in-depth understanding of the technical aspects of these programs. At the end of this lab, students should be able to write their own sniffing and spoofing programs.

Lab Environment

- This lab has to be done in Linux. You may use the Kali Linux to accomplish the tasks.

Drills

Task 1 - Packet Sniffing Program

1. Understanding the python implementation of a network packet sniffer. Use the link: http://www.binarytides.com/python-packet-sniffer-code-linux/, and try the three examples provided. **Screenshots** are required in the lab report.
    - When trying the examples, pay attention to the grammar. The examples use Python 2 grammar, e.g., `print`. Change it for Python 3.
2. **Writing filters**. Please implement the following: 1) Capture the ICMP packets between two specific hosts. 2) Capture the TCP packets that have a destination port range from to port 10 - 100. Your filter expression will be put into an external file `filter.txt`, which should only contain a line of your filter statement. Your program will read the filter expression from `filter.txt` and return the results properly. You can define your own filter syntax. For instance, a string `ICMP host1_IP host2_IP` could be used for 1), and a string `TCP 10 100` can be the second filter. In the example, the first word specifies the protocol, and the following are parameters for the filter. **In your report, please also include the contents of your** `filter.txt`.
3. Run command `telnet games.libreplanet.org` from your terminal to register a user with username & pswd chosen by you. Now run the script from Task 1.2, login the game server and show that the password can be captured by the sniffer in a **screenshot**.

> ### Task 1 Questions
>
> 1. Include the contents of your `filter.txt`.
> 2. Include your python code.
> 3. Include the screenshots.
> 4. Summarize your findings.

Task 2 - Spoofing

When a normal user sends out a packet, operating systems usually do not allow the user to set all the fields in the protocol headers (such as TCP, UDP, and IP headers). OSes will set most of the fields, while only allowing users to set a few fields, such as the destination IP address, the destination port number, etc. However, if users have the root privilege, they can set any arbitrary field in the packet headers (in theory). This can be exploited for packet spoofing, and it can be done through raw sockets.

Raw sockets give programmers the absolute control over the packet construction, allowing programmers to construct any arbitrary packet, including setting the header fields and the payload. Using raw sockets is quite straightforward; it involves four steps: (1) create a raw socket, (2) set socket option, (3) construct the packet, and (4) send out the packet through the raw socket. Please read the tutorial here: http://www.binarytides.com/raw-socket-programming-in-python-linux/, and learn how to write a packet spoofing program. Also, pay attention to the grammar in the examples. The examples use Python 2 grammar, e.g., `print`. Change it for Python 3.

1. **Write a spoofing program**. You can modify the tutorial example to get yours. You need to provide evidences (e.g., **screen captures** of a Wireshark packet trace) to show us that your program successfully sends out spoofed IP packets.
2. Spoof an ICMP Echo request. Spoof an ICMP echo request packet on behalf of another machine (i.e., using another machine's IP address in the same LAN as its source IP address). This packet should be sent to the host machine from Kali. You should turn on your Wireshark on the host, so if your spoofing is successful, you can see the echo reply to the spoofed address.
3. Spoof an Ethernet Frame. Set `01:02:03:04:05:06` as the source address.

Task 2 Questions

1. Include your python code.
2. Include the screenshots.
3. Summarize your findings.
4. Answer the following questions:
    - Can you set the IP packet length field to an arbitrary value, regardless of how big the actual packet is?
    - Using the raw socket programming, do you have to calculate the checksum for the IP header?