DIY Projects

NetworkTrafficAnalyser

Expected time to finish **7-8 Days**

By **Diya Agrawal**

Introduction

We would make a network traffic analyser, to parse and analyse the network traffic going through the targeted IPs and also track the traffic going to malicious sites known to us. This is a tool used extensively in the cybersecurity field and can be used in various cases.

You can go through this link to better understand the same: [Network Traffic Analyser for cyber security]

Tech Stack

- **Python**
- **Wireshark**
- **Ettercap**
- **MySQL**

Commands

1. We will learn about networks in depth so as to be able to make the analyzer. You can also play around with Cisco Packet Tracer to get hold of the same.
2. Then we would proceed to learn the fundamentals of Wireshark, the tool we would use to capture the packets and get their information files.
3. Now Ettercap would be used to determine which packets are going where and analyse the traffic.
4. MySQL is used to store all the files in an encrypted form.
5. Once we have completed understanding the individual components we will write a python program to make the network traffic analyzer.
6. To build upon the project, we can also use a visualizer like google earth API to give the output.

Resources

1. Network fundamentals: NetworkKing Playlist (Do till you get a good idea of how networks work and how you would approach the project)

2. Wireshark: What Is Wireshark and How to Use It | Cybersecurity | CompTIA
3. MySQL: SQL Tutorial - Full Database Course for Beginners
4. Ettercap: Ettercap and middle-attacks tutorial

Submission

The best projects will get featured in the next edition of **Debugged (Issue 3)**, our highly acclaimed club magazine, so don't forget to submit your projects upon completion!

After completing the project, fill out this form to submit your hard work.