UDP Spoofing

Purpose

The purpose of this assignment is to make you feel comfortable with using a VPN connection and working directly with raw sockets. You will learn how to create and use raw sockets, send raw IP packets with forged source IPs, and manually create UDP packets.

Objectives

Students will be able to:
- Program with raw sockets.
- Create UDP packets manually and programmatically.
- Send UDP packets with spoofed source IP addresses.

Technology Requirements

While students can use any programming language, Python is strongly recommended.

Note: The course team will not be able to help you if you choose any language that is not Python, Java, or C#; therefore, to create the best learning experience, Python is strongly recommended.

Project Description

A UDP service FlagServ is running at flagserv.cse543.rev.fish:13337. This UDP service receives a target IP address from the user, and if the user is authenticated, it will happily send a flag (a special string) via UDP to port 13337 of the target IP. Your job is to write a program that retrieves the flag.

FlagServ employs THE BEST AUTHENTICATION METHOD IN THE WORLD: Source-IP-based authentication, which means it authenticates all users based on their source IP addresses. If a user's source IP address is trusted, FlagServ will send out the flag to the specified destination (repeat: via UDP). Otherwise, it will send an error message back to the untrusted user (via UDP, too).

The only trusted IP is 10.2.4.10. Your task is to break or bypass this source-IP-based authentication scheme and steal the flag.

To keep the internet a secure place, flagserv.cse543.rev.fish points to a private IP that is only accessible through VPN. You will receive an OpenVPN configuration file. You will need to install OpenVPN and use it to connect to the VPN before talking to FlagServ.

Directions

See Project Description.

Evaluation

Your submission will be automatically graded. You will earn 100 if your stolen flag.txt is correct. Otherwise you will earn 0. Your code and readme.txt will be used as references. Partial credit will not be granted for this project.

Submission Directions for Project Deliverables

You will submit three files for this assignment:

- A txt file flag.txt with the stolen flag inside
- A txt file readme.txt describing your thought process or your solution to this problem
- Your code (a Python script or source code in any programming languages) that attacks the service and obtains the flag. Submit your code as a ZIP file.