driptables

Project Proposal - James Chi & Dan Reschke

Abstract

Our concept is centered around a late night Cyberlab struggle we encountered together when we were tasked with configuring Linux's built-in firewall, iptables. Using our "friends", we found several web-based firewall command generators, but we soon realized two things. Many gave the wrong output, giving us an incorrect firewall configuration. Also, going through the browser was inconvenient.

Problem to Solve

We intend to create a GUI version of iptables in order to simplify the process of creating rules on the linux-based firewall. Given that human error is a common factor in many preventable cyber incidents, improving what can seem to be a complicated task (especially if done across many systems) will likely reduce the amount of firewall misconfigurations in linux systems that utilize iptables.

Approach/Methods

To begin, we need to decide on a GUI framework/toolkit. We are still researching, and welcome any input or advice from instructors. The frontrunners are PyQt5 and Tkinter. The back end will be coded in Python and will use the input fields outlined below to generate, output, and append the iptables automatically when submitted by the end user.

Fields for user input (dropdown list):
- Rule Chain:
  1. Input
  2. Forward
  3. Output
  4. Prerouting
- Traffic Type (protocol):
  1. TCP
  2. UDP
  3. IP
  4. ICMP
- Action:
  1. Accept
  2. Drop
  3. Reject

Fields for user input (type):
- Source IP
- Source Port
- Destination IP
- Destination Port