Proof of Concept

Fullstack Academy - Cybersecurity Capstone
James Chi & Dan Reschke

Establishing Need

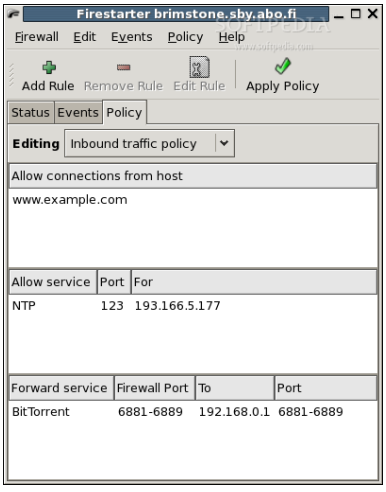
According to Gartner, through 2025, 99% of cloud security failures will be the customer's fault, largely due to misconfigurations [1]. Misconfigurations are often caused by human error, and are commonly remediated by shifting to security automation. We have heard from our classmates about how frustrating it can be to configure and manage iptables rules, and we have experienced how tedious it can be.

The Solution

A feasible solution based on our timeline would be similar to what we proposed, which is an automated iptables Python script in a GUI framework. Our goal is that by simplifying the iptables configuration and management process, user networks are less likely to suffer from a security incident due to a misconfiguration. We also hope that people who may have never used iptables previously are encouraged to use driptables, due to its ease of use.

EOL / Abandoned Solutions

Firestarter was a popular firewall configuration application. It also provided real-time networking information to the user. Unfortunately, development was abandoned in 2005, and Ubuntu removed it from all repositories by 2013. We are optimistic that if an application as robust as Firestarter was successful, our concept can come to life.



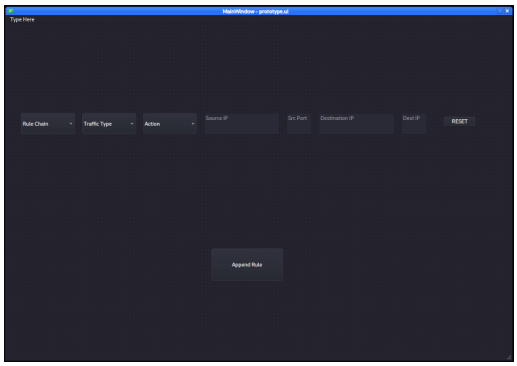
[1] https://www.gartner.com/smarterwithgartner/is-the-cloud-secure

Resources

We know our main programming languages will be Linux and Python. We intend on using PyQt5 for GUI design, along with Visual Studio Code for writing our code. We have also researched an IDE that may streamline the dev/testing process, but so far we have not needed to utilize it.

Deployment Overview

Our initial concepts include snippets of sample code, and a test GUI for our program.




```
#!/usr/bin/env python3
from PyQt5 import QtCore, QtGui, QtWidgets
import subprocess
import os
rule_table = []

class Ui_MainWindow(object):
```

```
boxes = {'chain':self.RuleChain,'protocol':self.TrafficType,'action':self.Action,'source':self.SrcIP,'src_port':self.SrcPort,'destination':self.DstIP,'dst_port':self.DstPort}
rule_table.append(boxes)
```

Key Schedule Constraints

Several key schedule constraints exist for the development, testing, and production of this project. They must be met by the deadlines[2] set by Fullstack Academy. Failure to comply with these deadlines will result in a product that does not meet our stakeholder goals and metrics—443

- Ability to code, test and deploy all components, and implement any stretch goals identified within the specified time frame.

- Ability to script, record, and produce the final project video within the specified time frame.

Metrics and Goals

KPIs will measure our on-time percentage for deliverables, NPS feedback from instructors and classmates, and teammate satisfaction/retention. The goals are to provide a polished end-product and presentation no later than the project deadline, and for both of us to be completely satisfied with the effort we put into it.

[2] https://files.slack.com/files-pri/T024FPYBQ-F03ABNPGZGB/deadlines.png