Ryan Schanzenbacher
rjs1877@rit.edu
2/16/23
Team Bravo
Red Team HW

Github Repo: https://github.com/ryan77627/xdp-packet-dropper

Question Answers

1. The goal of this tool is to simply distract the blue team. It is a tool meant to cause chaos, as the method is uses to disable any connectivity is fairly well hidden, unless you know what to look for. As such, the ability for the grey team servers to communicate will be in the red teams control (unless the module is found and removed.) This gives the red team the advantage of being able to cause blue team to lose points whenever we see fit.
2. No other tool really inspired this one. The inspiration was knowing that I was eventually going to take this class, and over winter break reading a really interesting Cloudflare engineering blog post that talked about XDP Driver usage within Cloudflare for preventing DDOS attacks. I figured they were an interesting concept I wanted to research further, especially due to their control in the network stack and how early they are run in relation to receiving packets. I figured it would be fairly easy to implement a simple toggle that recreated a `DROP ALL` iptables rule, but with the benefit of being very hidden.
3. The feasibility of another team member being able to use my tool? Very easy, it is a simple toggle with a premade script to send the packet. You just need to know the destination IP address. To contribute? A bit harder, as you need to have a basic understanding of C at the very least, but then you need to learn new concepts that are specific to XDP drivers, such as not having any global state, and doing many, ***many***, bounds checks as the XDP driver is preverified for any potential code that can perform a buffer overread and will reject the code if any is found.