BGP Attack and Protection Emulation Using the SEED Internet Emulator

ABSTRACT

The purpose of this research was to use the SEED Internet Emulator to learn about Border Gateway Protocol (BGP) as a beginner in the cybersecurity realm, with no prior knowledge of Virtual Machines, emulators, python programming, or cybersecurity. The SEED Internet Emulator is an open-source internet emulator developed by Wenliang Du and Honghao Zeng. The capabilities of the emulator make it an excellent tool for learning about BGP. Essentially, BGP determines what path packets take as they travel to their intended destination. This extremely important function makes it a common target of attacks. Attacks on BGP can disconnect the internet or redirect traffic from its intended destination, allowing the information to be intercepted. The most common BGP attack is called IP prefix hijacking, in which hackers announce the ownership of prefixes that do not belong to them. This causes packets to be rerouted from their intended destinations to a hackers BGP router. By modifying the code of components in the emulator, one can simulate an IP prefix attack, as well as defend against it. However, even with the reference materials provided by SEED Labs, it is difficult for someone with no prior experience with cybersecurity to complete the lab independently. I experienced this difficulty firsthand, so I developed an easy-to-follow guide which would allow students new to cybersecurity to complete the exercises in the lab and learn about BGP without close supervision. Using the internet emulator, I successfully simulated an IP prefix hijacking attack by configuring the code of a router to announce a false prefix, causing packets to be redirected. I then defended against this attack from within the impacted autonomous system (AS) by inserting code to announce longer prefixes, reclaiming the traffic. Lastly, I posed as an ISP and altered the code of an AS to reject any false IP prefix announcements. After completing these activities, I created a guide to walk students through the installation of the emulator and the completion of the lab. The guide will make introduction to cybersecurity much easier for students with no prior knowledge of the material.