Jonathan Ho

jlh5360@rit.edu

Team Bravo

CSEC 473.02

2235 Spring

HW4 Red Team Tool

1. **(8 points) What is the goal of this tool? What purpose does it bring to the competitions?**

   The goal of the port knocking tool is to provide a means for the red team to stealthily open ports on a target system by sending a sequence of connection attempts to specific ports. This allows the red team to access services behind the target's firewall without directly triggering alerts or detections. The tool enhances the red team's capabilities by providing a covert method of gaining access to restricted services during security competitions. By automating the port knocking process, the tool improves efficiency and reduces the likelihood of detection during reconnaissance and exploitation phases.

2. **(8 points) Did other tools influence your tool? If so, what are they? If not, what was your inspiration for the tool?**

   While the port knocking tool is primarily inspired by the concept of port knocking itself and not my other red team tools, its implementation and development is influenced by various resources. Commonly used libraries and modules in Python for network communication, such as the socket library, have guided the development of the tool. Additionally, the design principles of simplicity, reliability, and stealthiness, often emphasized in red teaming scenarios, have been considered in the development of the tool's functionality and approach. Although no specific red team tools were directly referenced, the development process drew insights from existing port knocking implementations and related network security tools with these resources I referenced and utilized to understand and develop a port knocking tool following common practices:

   - https://resources.infosecinstitute.com/topics/mitre-attck/mitre-attck-port-knocking/
   - https://www.youtube.com/watch?v=IBR3oLqGBj4
   - https://github.com/sidpalas/devops-directive/tree/master/2020-10-05-port-knocking
   - https://www.tecmint.com/port-knocking-to-secure-ssh/
   - https://goteleport.com/blog/ssh-port-knocking/

- https://www.howtogeek.com/442733/how-to-use-port-knocking-on-linux-and-why-you-shouldnt/

3. (8 points) What is the feasibility of another team member quickly learning to use or contribute to your tool? What makes it easy or difficult to learn?

Another team member can quickly learn to use or contribute to the port knocking tool due to several factors. Firstly, the tool is implemented in Python, a widely used and beginner-friendly programming language known for its readability and simplicity. The code is well-commented and structured, making it easy for team members to understand its logic and functionality. Additionally, the provided README.txt file that I wrote contains comprehensive installation and usage instructions, guiding users through the setup and execution process step by step. Moreover, the modular nature of the tool allows for easy customization or extension to adapt to different environments or requirements, further enhancing its usability for team members with varying levels of expertise. Overall, the combination of clear documentation, readable code, and flexibility ensures that other team members can quickly grasp and utilize the port knocking tool effectively in red teaming exercises.