Mitigating SYN Attacks with NGFWs

Jesse Leonard and Cameron McDuffie
Advisors: Jorge Crichigno, Ali Mazloum, Jose Gomez

Department of Integrated Information Technology
University of South Carolina

December 2nd, 2021

Agenda

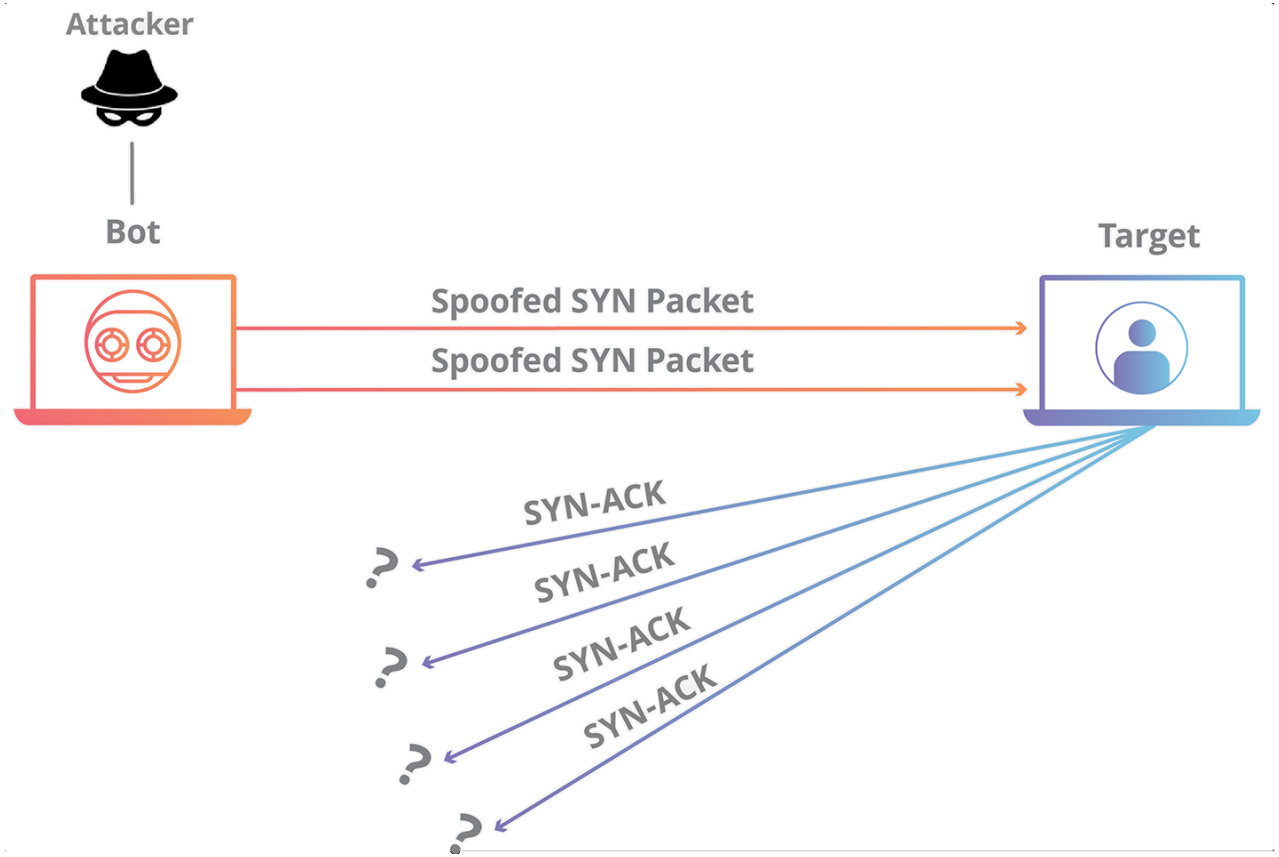
- Purpose
- Introduction
- Problem Description
- Background Information
- Proposed Solution
- Analyzing SYN Packets
- Conclusion

Purpose

- Understand the TCP handshake
- Understand SYN flood attacks
- Understand NGFW's abilities and configurations
- Mitigate Denial of Service (via SYN flood) using a NGFW
- Find a balanced solution between protection and resource allocation

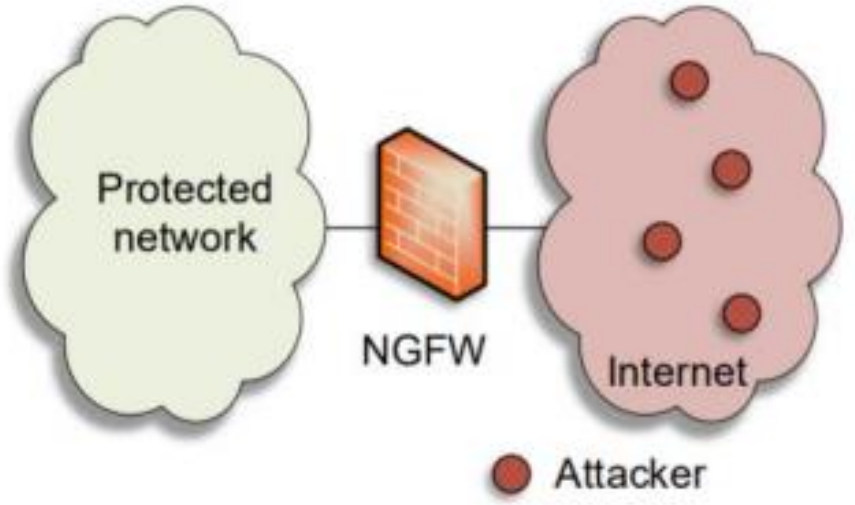
Introduction

- SYN Flood – Type of DDoS (Denial of Service) Attack
- Utilizes TCP three-way handshake
- Three types of attacks
  I. Direct
  II. Spoof
  III. Distributed



Problem Description

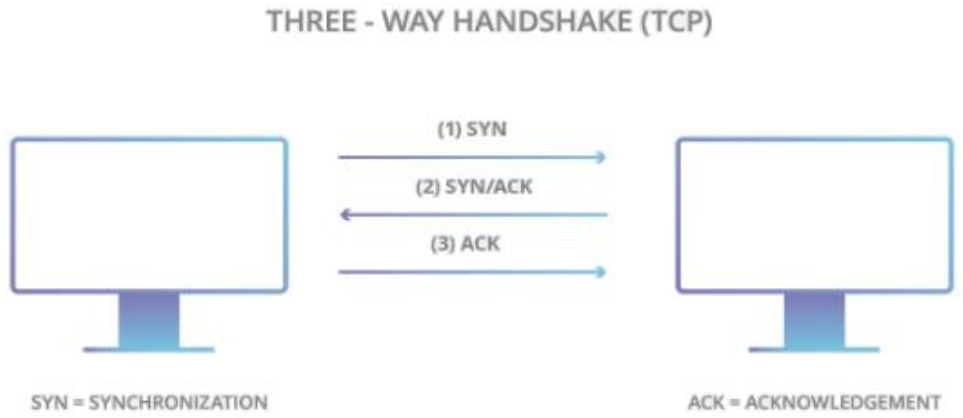
- Protect a network against SYN attacks using a NGFW
- Implement a protection policy
- Server is unable to respond to legitimate traffic, policy prevents this



Background Information

- Traditional Firewalls
  I. Identify traffic based on protocol, IP address, and port number
  II. Attacks pass through open firewall ports intended for legitimate traffic

- TCP
  I. Main transport-layer protocol used on the internet
  II. Establishes connections to take place between devices

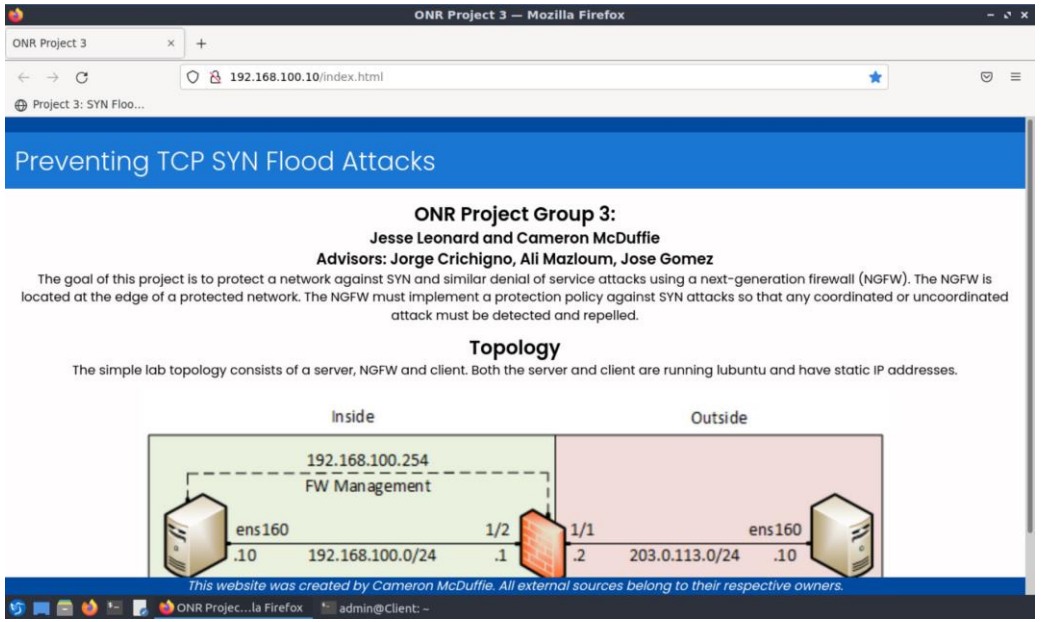


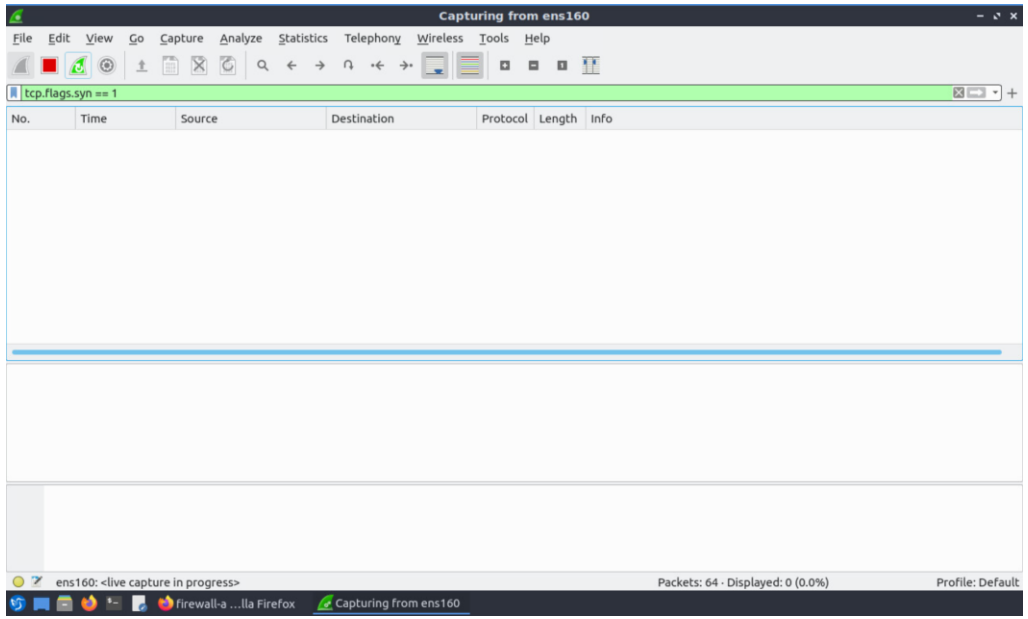
Proposed Solution

- Filtered traffic is monitored via wireshark, only TCP SYN packets will show
- DoS protection profile allows the firewall to block illegitimate traffic
- Firewall generates SYN cookies to understand what traffic is legitimate
- If a client does not return a cookie with the ACK packet, it is dropped

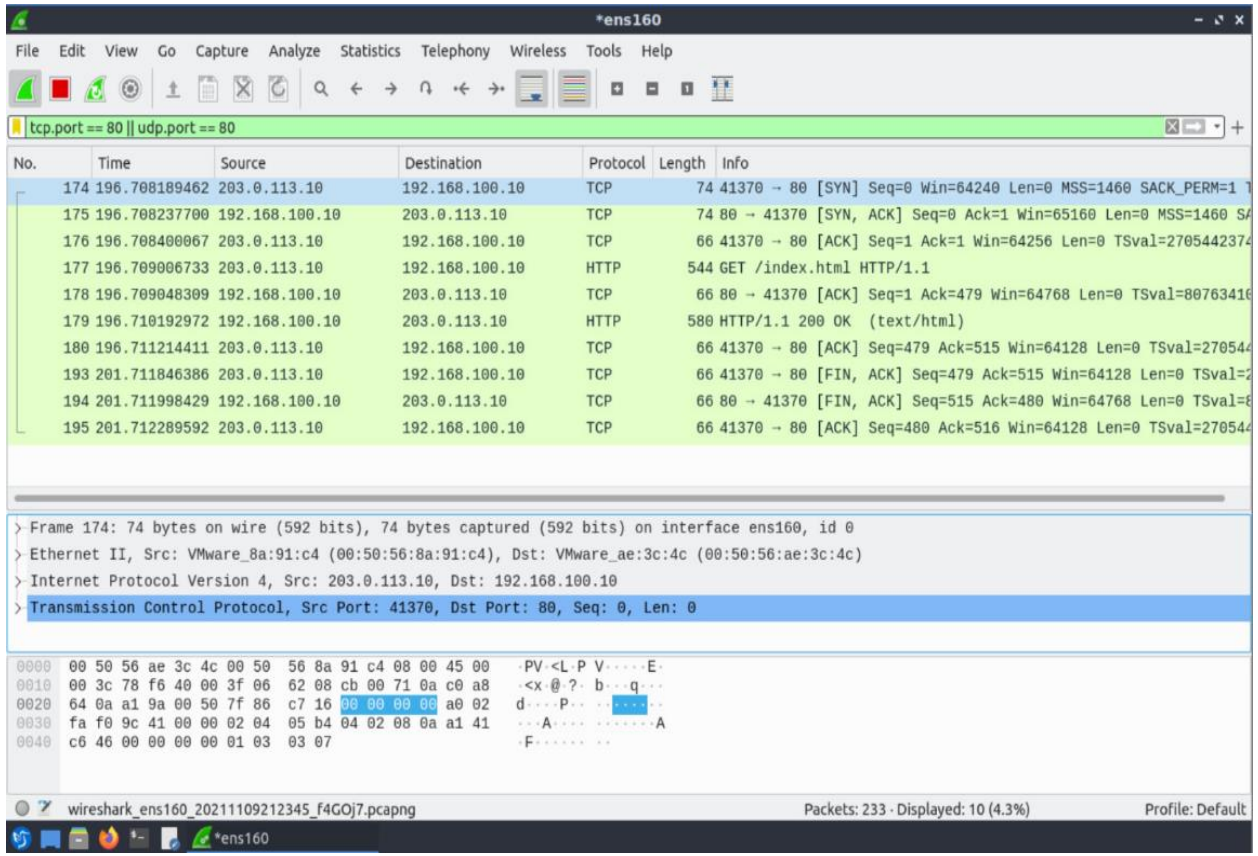
Solution Results

- A website is hosted on port 80 of the server to test availability during an attack
- DoS protection profile is enabled
- When accessing the website during an attack, it is still available

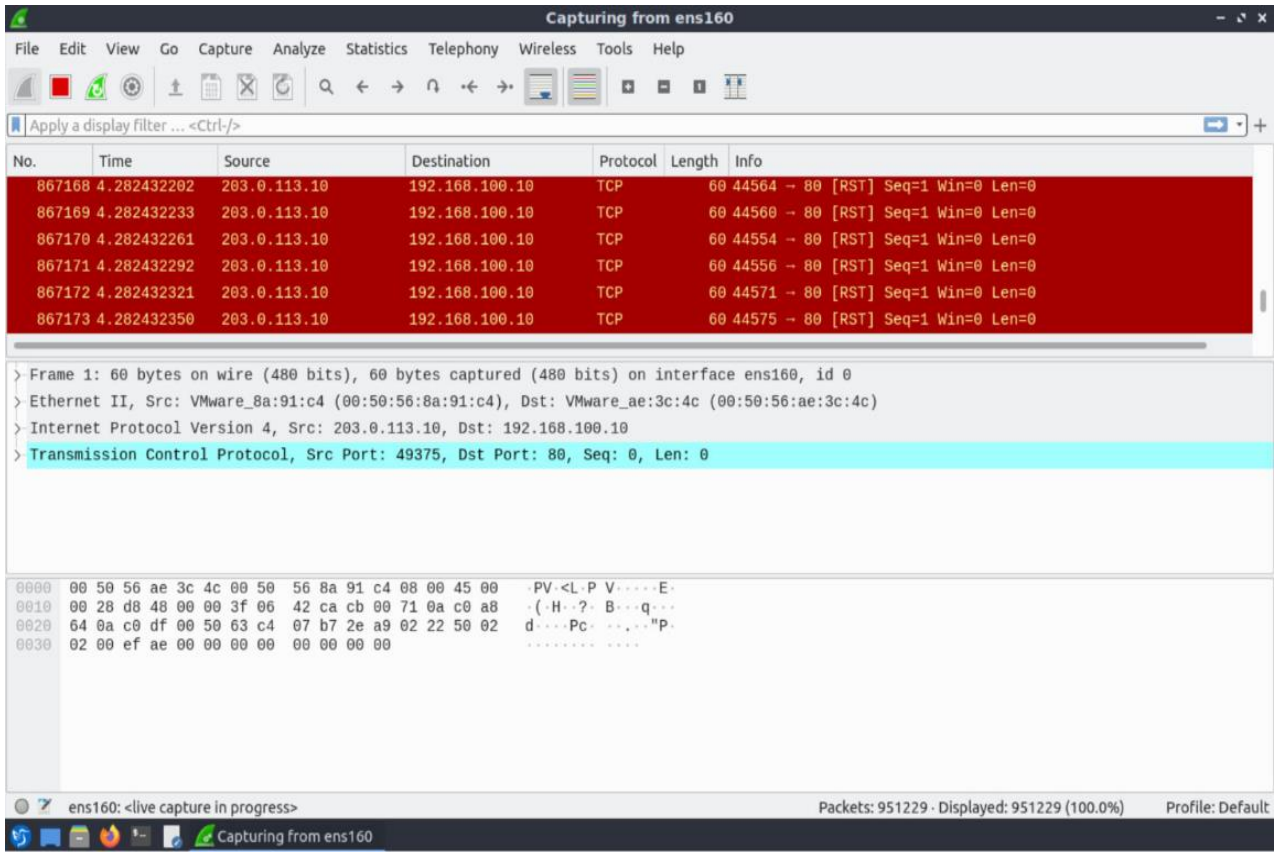




Analyzing SYN Packets



Normal Traffic



SYN Attack Traffic

Conclusion

- Why is this work important?
- Future projects/concepts with this knowledge
- Questions?
- Thank you for listening and watching